Oracle® Enterprise Manager

Cloud Control Administrator’s Guide

12*c* Release 4 (12.1.0.4)

E24473-35

January 2015

Oracle Enterprise Manager Cloud Control Administrator's Guide, 12*c* Release 4 (12.1.0.4)

E24473-35

Contents

3 Using Incident Management

4 Using Notifications

5 Using Blackouts

6 Managing Groups

7 Using Administration Groups

8 Using Monitoring Templates

9 Using Metric Extensions

10 Advanced Threshold Management

11 Utilizing the Job System and Corrective Actions

Part II Administering Cloud Control

12 Maintaining Enterprise Manager

13 Maintaining and Troubleshooting the Management Repository

14 Updating Cloud Control

15 Configuring a Software Library

16 Managing Plug-Ins

17 Patching Oracle Management Service and the Repository

18 Patching Oracle Management Agents

19 Personalizing Cloud Control

20 Starting and Stopping Enterprise Manager Components

23 Configuring and Using Services

24 Introducing Enterprise Manager Support for SNMP

Part III Security

25 Configuring Security

Part IV Generating Reports

26 Using Information Publisher

27 Creating Usage Tracking Reports

Part V Accessing Enterprise Manager via Mobile Devices

28 Remote Access To Enterprise Manager

Part VI Configuring Enterprise Manager for High Availability

Part VII Appendixes

Preface

This guide describes how to use Oracle Enterprise Manager Cloud Control 12*c* core functionality.

The preface covers the following:

- Audience
- Documentation Accessibility
- Related Documents
- Conventions

Audience

This document is intended for Enterprise Manager administrators and developers who want to manage their Enterprise Manager infrastructure.

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 that have purchased support 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 the latest releases of these and other Oracle documentation, check the Oracle Technology Network at:

http://docs.oracle.com/en/enterprise-manager/

Oracle Enterprise Manager also provides extensive Online Help. From the *user* menu at the top of any Enterprise Manager page, select **Help** to display the online help window.

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.

What's Changed in this Guide?

The revisions listed below identify information updates, structural changes, as well as relocation of information to other guides.

Since the last revision, the following changes have been made:

- **Added**: Applying adaptive thresholds using monitoring templates
- **Modified**: Various technical and procedural updates.

Part I

Monitoring and Managing Targets

This section contains the following chapters:

1 Enterprise Monitoring

This chapter covers the following topics:

1.1 Monitoring Overview

Enterprise Manager Cloud Control monitoring functionality permits unattended monitoring of your IT environment. Enterprise Manager comes with a comprehensive set of performance and health metrics that allows monitoring of key components in your environment, such as applications, application servers, databases, as well as the back-end components on which they rely (such as hosts, operating systems, storage).

The Management Agent on each monitored host monitors the status, health, and performance of all managed components (targets) on that host. If a target goes down, or if a performance metric crosses a warning or critical threshold, an event is triggered and sent to Enterprise Manager. Administrators or any interested party can be notified of the triggered event through the Enterprise Manager notification system.

Adding targets to monitor is simple. Enterprise Manager provides you with the option of either adding targets manually or automatically discovering all targets on a host. Enterprise Manager can also automatically and intelligently apply monitoring settings for newly added targets. For more information, see Section 1.4.2, "Administration Groups and Template Collections"). While Enterprise Manager provides a comprehensive set of metrics used for monitoring, you can also use metric extensions (see Section 1.3.6, "Metric Extensions: Customizing Monitoring") to monitor conditions that are specific to your environment. As your data center grows, it will become more challenging to manage individual targets separately, thus you can use Enterprise Manager's group management functionality to organize large sets of targets into groups, allowing you to monitor and manage many targets as one.

1.2 Comprehensive Out-of-Box Monitoring

Monitoring begins as soon as you install Enterprise Manager Cloud Control 12*c*. Enterprise Manager's Management Agents automatically start monitoring their host's systems (including hardware and software configuration data on these hosts) as soon as they are deployed and started. Enterprise Manager provides auto-discovery scripts that enable these Agents to automatically discover all Oracle components and start monitoring them using a comprehensive set of metrics at Oracle-recommended thresholds.

This monitoring functionality includes other components of the Oracle ecosystem such as NetApp Filer, BIG-IP load balancers, Checkpoint Firewall, and IBM WebSphere. Metrics from all monitored components are stored and aggregated in the Management Repository, providing administrators with a rich source of diagnostic information and trend analysis data. When critical alerts are detected, notifications are sent to administrators for rapid resolution.

Out-of-box, Enterprise Manager monitoring functionality provides:

- In-depth monitoring with Oracle-recommended metrics and thresholds.
- Monitoring of all components of your IT infrastructure (Oracle and non-Oracle) as well as the applications and services that are running on them.
- Access to real-time performance charts.
- Collection, storage, and aggregation of metric data in the Management Repository. This allows you to perform strategic tasks such as trend analysis and reporting.
- E-mail and pager notifications for detected critical events.

Enterprise Manager can monitor a wide variety of components (such as databases, hosts, and routers) within your IT infrastructure.

Some examples of monitored metrics are:

- Archive Area Used (Database)
- Component Memory Usage (Application Server)
- Segments Approaching Maximum Extents Count (Database)
- Network Interface Total I/O Rate (Host)

Monitoring Without Management Agents

When it is not practical to have a Management Agent present to monitor specific components of your IT infrastructure, as might be the case with an IP traffic controller or remote Web application, Enterprise Manager provides Extended Network and Critical URL Monitoring functionality. This feature allows the Beacon functionality of the Agent to monitor remote network devices and URLs for availability and responsiveness without requiring an Agent to be physically present on that device. You simply select a specific Beacon, and add key network components and URLs to the *Network and URL Watch Lists*. More information about using this feature is available in the Enterprise Manager online help and from the Oracle Technology Network Web site. Enterprise Manager monitoring concepts and the underlying subsystems that support this functionality are discussed in the following sections.

1.3 Monitoring: Basics

Enterprise Manager Cloud Control 12c comes with a comprehensive set of predefined performance and health metrics that enables automated monitoring of key components in your environment, such as applications, application servers, databases, as well as the back-end components on which they rely, such as hosts, operating systems, storage. While Enterprise Manager can monitor for many types of conditions (events), the most common use of its monitoring capability centers around the basics of monitoring for violation of acceptable performance boundaries defined by metric values. The following sections discuss the basic concepts and Enterprise Manger functionality that supports monitoring of targets.

1.3.1 Metric Thresholds: Determining When a Monitored Condition is an Issue

Some metrics have associated predefined limiting parameters called thresholds that cause metric alerts (specific type of event) to be triggered when collected metric values exceed these limits. Enterprise Manager allows you to set metric threshold values for two levels of alert severity:

- **Warning** - Attention is required in a particular area, but the area is still functional.
- **Critical** - Immediate action is required in a particular area. The area is either not functional or indicative of imminent problems.

Hence, thresholds are boundary values against which monitored metric values are compared. For example, for each disk device associated with the Disk Utilization (%) metric, you might define a warning threshold at 80% disk space used and critical threshold at 95%.

Note: Not all metrics need a threshold: If the values do not make sense, or are not needed in a particular environment, they can be removed or simply not set.

While the out-of-box predefined metric threshold values will work for most monitoring conditions, your environment may require that you customize threshold values to more accurately reflect the operational norms of your environment. Setting accurate threshold values, however, may be more challenging for certain categories of metrics such as performance metrics.

For example, what are appropriate warning and critical thresholds for the *Response Time Per Transaction* database metric? For such metrics, it might make more sense to be alerted when the monitored values for the performance metric deviates from normal behavior. Enterprise Manager provides features to enable you to capture normal performance behavior for a target and determine thresholds that are deviations from that performance norm.

Note: Enterprise Manager administrators must be granted *Manage Target Metrics* or greater privilege on a target in order to perform any metric threshold changes.

1.3.2 Metric Baselines: Determining Valid Metric Thresholds

Determining what metric threshold values accurately reflect the performance monitoring needs of your environment is not trivial. Rather than relying on trial and error to determine the correct values, Enterprise Manager provides metric baselines. Metric baselines are well-defined time intervals (baseline periods) over which Enterprise Manager has captured system performance metrics, creating statistical characterizations of system performance over specific time periods. This historical data greatly simplifies the task of determining valid metric threshold values by providing normalized views of system performance. Baseline normalized views of metric behavior help administrators explain and understand event occurrences.

The underlying assumption of metric baselines is that systems with relatively stable performance should exhibit similar metric observations (values) over times of comparable workload. Two types of baseline periods are supported:

- **Moving Window Baseline Periods**: Moving window baseline periods are defined as some number of days prior to the current date (Example: Last 7 days). This allows comparison of current metric values with recently observed history. Moving window baselines are useful for operational systems with predictable workload cycles (Example: OLTP days and batch nights).
- **Static Baseline Periods**: Static baselines are periods of time you define that are of particular interest to you (Example: End of the fiscal year). These baselines can be used to characterize workload periods for comparison against future occurrences of that workload (Example: Compare the end of the fiscal year from one calendar year to the next).

1.3.3 Advanced Threshold Management

While metric baselines are generally useful for determining valid target alert thresholds, these thresholds are static and are not able to account for expected performance variation. There are monitoring situations in which different work loads for a target occur at regular (expected) intervals. Here, a static alert threshold would prove to be inaccurate. For example, the alert thresholds for a database performing Online Transaction Process (OLTP) during the day and batch processing at night would be different. Similarly, database workloads can change based purely on different time periods, such as weekday versus weekend. Thus, fixed static values for thresholds might result in false alert reporting, and with excessive alerting could generate excessive overhead with regard to performance management. For this OLTP example, using static baselines to determine accurate alert thresholds fails to account for expected cyclic variations in performance, adversely affecting problem detection. Static baselines introduce the following configuration issues:

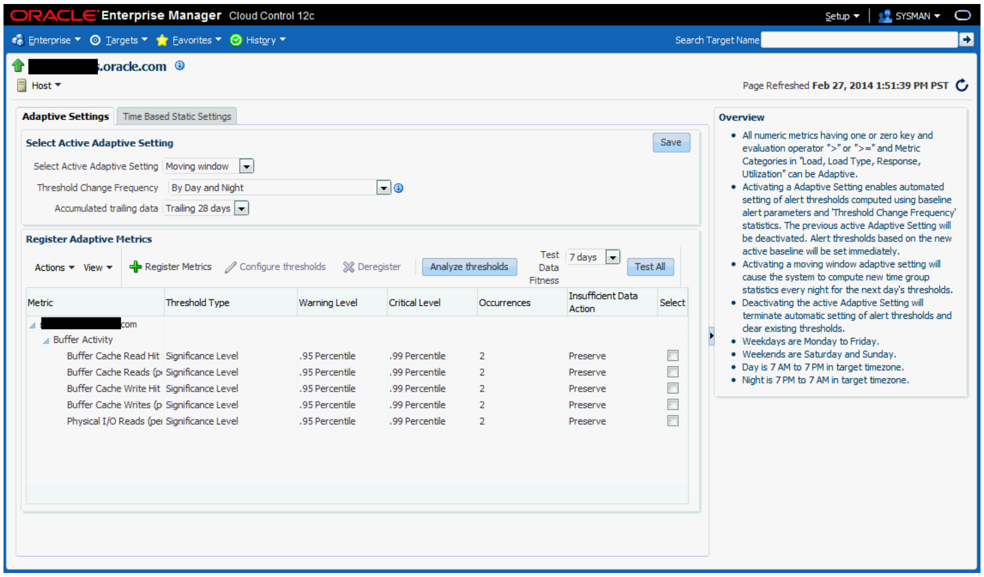
- Baselines configured for Batch performance may fail to detect OLTP performance degradation.
- Baselines configured for OLTP performance may generate excessive alerts during Batch cycles

Beginning with Enterprise Manager Release 12.1.0.4, Advanced Threshold Management can be used to compute thresholds using baselines that are either adaptive (self-adjusting) or time-based (user-defined).

- *Adaptive Thresholds*: Allows Enterprise Manager to statistically compute threshold that are adaptive in nature. Adaptive thresholds apply to all targets (both Agent and repository monitored).
- *Time-based Thresholds*: Allows you to define a specific threshold values to be used at different times to account for changing workloads over time.

A convenient UI allows you to create time-based and adaptive thresholds. From a target home page (a host, for example), navigate to the Metric Collection and Settings page. Click **Advanced Threshold Management** in the *Related Links* region.

Figure 1–1 Advanced Threshold Management Page



[redacted].oracle.com

Page Refreshed **Feb 27, 2014 1:51:39 PM PST**

Select Active Adaptive Setting

Select Active Adaptive Setting: Moving window

Threshold Change Frequency: By Day and Night

Accumulated trailing data: Trailing 28 days

Register Adaptive Metrics

Test Data Fitness: 7 days

Metric	Threshold Type	Warning Level	Critical Level	Occurrences	Insufficient Data Action	Select
[redacted]com						
Buffer Activity						
Buffer Cache Read Hit	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Buffer Cache Reads (p	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Buffer Cache Write Hit	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Buffer Cache Writes (p	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Physical I/O Reads (pe	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□

Overview

- All numeric metrics having one or zero key and evaluation operator ">" or ">=" and Metric Categories in "Load, Load Type, Response, Utilization" can be Adaptive.
- Activating a Adaptive Setting enables automated setting of alert thresholds computed using baseline alert parameters and 'Threshold Change Frequency' statistics. The previous active Adaptive Setting will be deactivated. Alert thresholds based on the new active baseline will be set immediately.
- Activating a moving window adaptive setting will cause the system to compute new time group statistics every night for the next day's thresholds.
- Deactivating the active Adaptive Setting will terminate automatic setting of alert thresholds and clear existing thresholds.
- Weekdays are Monday to Friday.
- Weekends are Saturday and Sunday.
- Day is 7 AM to 7 PM in target timezone.
- Night is 7 PM to 7 AM in target timezone.

Only numeric and View Collect metrics can be registered as adaptive thresholds. In addition, only the following types of metrics are permitted:

- Load
- Load Type
- Utilization and Response

1.3.4 Events: Defining What Conditions are of Interest

When a metric threshold value is reached, a metric alert is raised. A metric alert is a type of event. An event is a significant occurrence that indicates a potential problem; for example, either a warning or critical threshold for a monitored metric has been crossed. Other examples of events include: database instance is down, a configuration file has been changed, job executions ended in failure, or a host exceeded a specified percentage CPU utilization. Two of the most important event types used in enterprise monitoring are:

- Metric Alert
- Target Availability

For more information on events and available event types for which you can monitor, see Chapter 3, "Using Incident Management".

1.3.5 Corrective Actions: Resolving Issues Automatically

Corrective actions allow you to specify automated responses to metric alerts, saving administrator time and ensuring issues are dealt with before they noticeably impact users. For example, if Enterprise Manager detects that a component, such as the SQL*Net listener is down, a corrective action can be specified to automatically start it back up. A corrective action is, therefore, any task you specify that will be executed when a metric triggers a warning or critical alert severity. In addition to performing a corrective task, a corrective action can be used to gather more diagnostic information, if needed. By default, the corrective action runs on the target on which the event has been raised.

A corrective action can also consist of multiple tasks, with each task running on a different target. Administrators can also receive notifications for the success or failure of corrective actions. A corrective action can also consist of multiple tasks, with each task running on a different target.

Corrective actions for a target can be defined by all Enterprise Manager administrators who have been granted *Manage Target Metrics* or greater privilege on the target. For any metric, you can define different corrective actions when the metric triggers at warning severity or at critical severity.

Corrective actions must run using the credentials of a specific Enterprise Manager administrator. For this reason, whenever a corrective action is created or modified, the credentials that the modified action will run with must be specified.

1.3.6 Metric Extensions: Customizing Monitoring

Metric Extensions let you extend Enterprise Manager's monitoring capabilities to cover conditions specific to your IT environment, thus providing you with a complete and comprehensive view of your monitored environment.

Metric extensions allow you to define new metrics on any target type that utilize the same full set of data collection mechanisms used by Oracle provided metrics. For example, some target types you can create metrics on are:

- Hosts
- Databases
- IBM Websphere
- Oracle Exadata Databases and Storage Servers
- Oracle Business Intelligence Components

Once these new metrics are defined, they are used like any other Enterprise Manager metric. For more information about metric extensions, see Chapter 9, "Using Metric Extensions".

User-Defined Metrics (Pre-12*c*)

If you upgraded your Enterprise Manager 12*c* site from an older version of Enterprise Manager, then all user-defined metrics defined in the older version will also be migrated to Enterprise Manager 12*c*. These user-defined metrics will continue to work, however they will no longer be supported a future release. If you have existing user-defined metrics, it is recommended that you migrate them to metric extensions as soon as possible to prevent potential monitoring disruptions in your managed environment. For information about the migration process, see *Converting User-defined Metrics to Metric Extensions* in Chapter 9, "Using Metric Extensions"

1.3.7 Blackouts

Blackouts allow you to support planned outage periods to perform scheduled or emergency maintenance. When a target is put under blackout, monitoring is suspended, thus preventing unnecessary alerts from being sent when you bring down a target for scheduled maintenance operations such as database backup or hardware upgrade. Blackout periods are automatically excluded when calculating a target's overall availability.

A blackout period can be defined for individual targets, a group of targets or for all targets on a host. The blackout can be scheduled to run immediately or in the future, and to run indefinitely or stop after a specific duration. Blackouts can be created on an as-needed basis, or scheduled to run at regular intervals. If, during the maintenance period, you discover that you need more (or less) time to complete maintenance tasks, you can easily extend (or stop) the blackout that is currently in effect. Blackout functionality is available from both the Enterprise Manager console as well as via the Enterprise Manager command-line interface (EM CLI). EM CLI is often useful for administrators who would like to incorporate the blacking out of a target within their maintenance scripts. When a blackout ends, the Management Agent automatically re-evaluates all metrics for the target to provide current status of the target post-blackout.

If an administrator inadvertently performs scheduled maintenance on a target without first putting the target under blackout, these periods would be reflected as target downtime instead of planned blackout periods. This has an adverse impact on the target's availability records. In such cases, Enterprise Manager allows Super Administrators to go back and define the blackout period that should have happened at that time. The ability to create these retroactive blackouts provides Super Administrators with the flexibility to define a more accurate picture of target availability.

1.4 Monitoring: Advanced Setup

Enterprise Manager greatly simplifies managing your monitored environment and also allows you to customize and extend Enterprise Manager monitoring capabilities. However, the primary advantage Enterprise Manager monitoring provides is the ability to monitor and manage large-scale, heterogeneous environments. Whether you are monitoring an environment with 10 targets or 10,000 targets, the following Enterprise Manager advanced features allow you to implement and maintain your monitored environment with the equal levels of convenience and simplicity.

1.4.1 Monitoring Templates

Monitoring Templates simplify the task of standardizing monitoring settings across your enterprise by allowing you to specify your standards for monitoring in a template once and apply them to monitored targets across your organization. This makes it easy for you to apply specific monitoring settings to specific classes of targets throughout your enterprise. For example, you can define one monitoring template for test databases and another monitoring template for production databases.

A monitoring template defines all Enterprise Manager parameters you would normally set to monitor a 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 affected targets in order to propagate the new changes. The apply operation can be automated using Administration Groups and Template Collections. For any target, you can preserve custom monitoring settings by specifying metric settings that can never be overwritten by a template.

Enterprise Manager comes with an array of Oracle-certified templates that provide recommended metric settings for various Oracle target types.

For more information about monitoring templates, see Chapter 8, "Using Monitoring Templates".

1.4.2 Administration Groups and Template Collections

Monitored environments are rarely static—new targets are constantly being added from across your ecosystem. Enterprise Manager allows you to maintain control of this dynamic environment through administration groups. Administration groups automate the process of setting up targets for management in Enterprise Manager by automatically applying management settings such as monitoring settings or compliance standards. Typically, these settings are manually applied to individual targets, or perhaps semi-automatically using monitoring templates (see Section 1.4.1, "Monitoring Templates") or custom scripts. Administration groups combine the convenience of applying monitoring settings using monitoring templates with the power of automation.

Template collections contain the monitoring settings and other management settings that are meant to be applied to targets as they join the administration group. Monitoring settings for targets are defined in monitoring templates. Monitoring templates are defined on a per target type basis, so you will need to create monitoring templates for each of the different target types in your administration group. You will most likely create multiple monitoring templates to define the appropriate monitoring settings for an administration group.

Every target added to Enterprise Manager possesses innate attributes called *target properties*. Enterprise Manager uses these target properties to add targets to the correct administration group. Administration group membership is based on target properties as membership criteria so target membership is dynamic. Once added to the administration group, Enterprise Manager automatically applies the requisite monitoring settings using monitoring templates that are part of the associated template collection .

Administration groups use the following target properties to define membership criteria:

- Contact
- Cost Center
- Customer Support Identifier
- Department
- Lifecycle Status
- Line of Business
- Location
- Target Version
- Target Type

1.4.3 Customizing Alert Messages

Whenever a metric threshold is reached, an alert is raised along with a metric-specific message. These messages are written to address generic metric alert conditions. Beginning with Enterprise Manager Release 12.1.0.4, you can customize these messages to suit the specific requirements of your monitored environment.

Customizing an alert message allows you to tailor the message to suit your monitoring needs. You can tailor the message to include their operational context specific to your environment such as IT error codes used in your data center, or add additional information collected by Enterprise Manager such as:

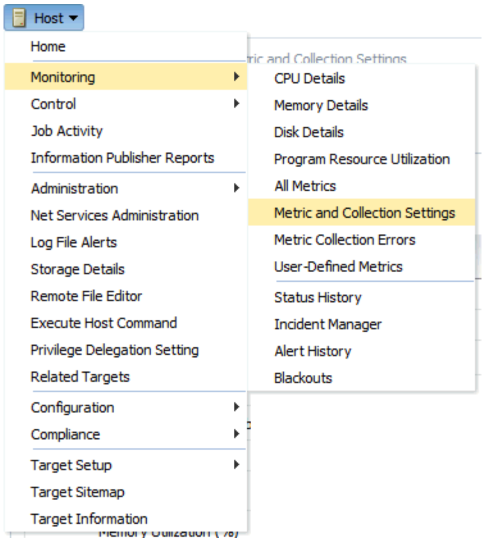
- Metric name for which the alert has been triggered

- Severity level of the alert or violation
- Threshold value for which warning or critical violation has been triggered
- Number of Occurrences after which alert has been triggered

Alert message customization allows for more efficient alert management by increasing message usability.

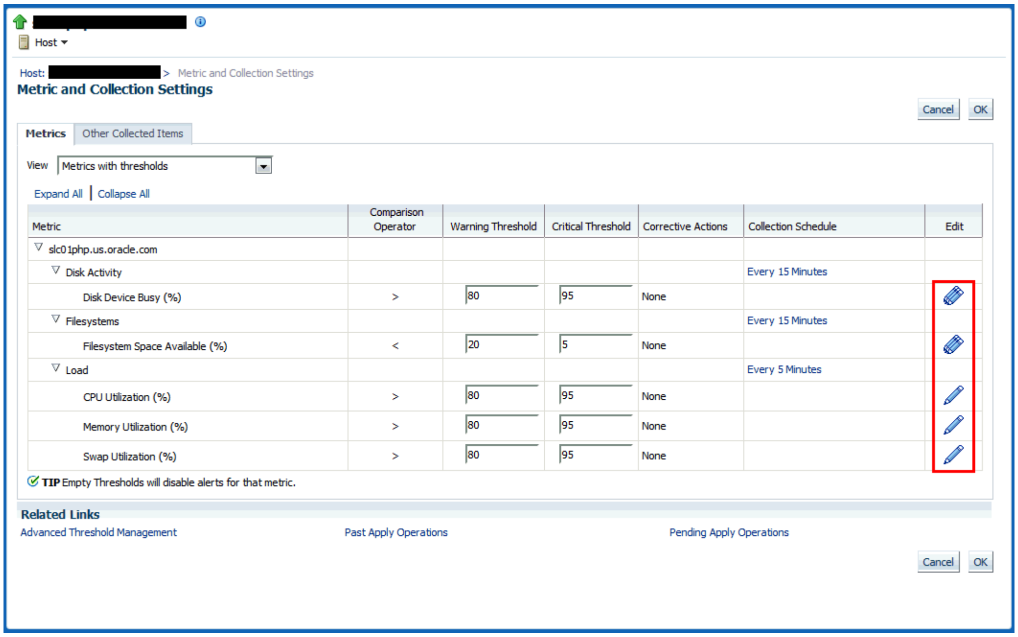
To customize a metric alert message:

1. Navigate to a target homepage.
2. From the *target* menu (host target type is shows in the graphic), select **Monitoring** and then **Metric and Collection Settings**.



The *Metric and Collection Settings* page displays.

3. In the metric table, find the specific metric whose message you want to change and click the edit icon (pencil).


[redacted]

Host ▾

Host: [redacted] > Metric and Collection Settings

Metric and Collection Settings

Cancel OK

Metrics | Other Collected Items

View: Metrics with thresholds

Expand All | Collapse All

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
▽ slc01php.us.oracle.com						
▽ Disk Activity					Every 15 Minutes	
Disk Device Busy (%)	>	80	95	None		✎
▽ Filesystems					Every 15 Minutes	
Filesystem Space Available (%)	<	20	5	None		✎
▽ Load					Every 5 Minutes	
CPU Utilization (%)	>	80	95	None		✎
Memory Utilization (%)	>	80	95	None		✎
Swap Utilization (%)	>	80	95	None		✎

✓ **TIP** Empty Thresholds will disable alerts for that metric.

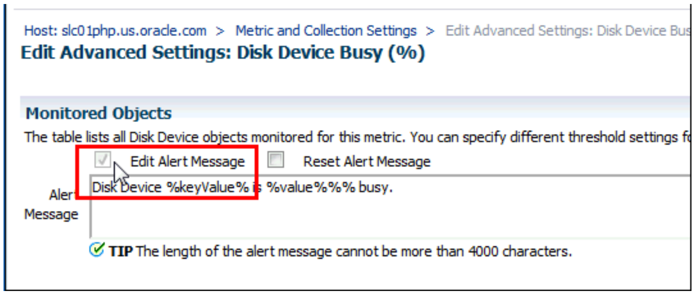
Related Links

Advanced Threshold Management   Past Apply Operations   Pending Apply Operations

Cancel OK

The *Edit Advanced Settings* page displays.

4. In the *Monitored Objects* region, click **Edit Alert Message**.



Host: slc01php.us.oracle.com > Metric and Collection Settings > Edit Advanced Settings: Disk Device Bus
☑ Edit Alert Message
☐ Reset Alert Message

Edit Advanced Settings: Disk Device Busy (%)

Monitored Objects

The table lists all Disk Device objects monitored for this metric. You can specify different threshold settings fo

Alert Message: Disk Device %keyValue% is %value%%% busy.

✓ TIP The length of the alert message cannot be more than 4000 characters.

5. Modify the alert message as appropriate.

> **Note:** To change your revised message back to the original Oracle-defined message at any time, click **Reset Alert Message**.

6. Click **Continue** to return to the *Metric and Collection Settings* page.
7. To modify additional metric alert messages, repeat steps three through six.
8. Once you are finished, click **OK** to save all changes to the Enterprise Manager Repository. Enterprise Manager will display a message indicating the updates have succeeded.
9. Click **OK** to dismiss the message and return to the target homepage.

1.5 Notifications

For a typical monitoring scenario, when a target becomes unavailable or if thresholds for performance are crossed, events are raised and notifications are sent to the appropriate administrators. Enterprise Manager supports notifications via email, pager, SNMP traps, or by running custom scripts and allows administrators to control these notification mechanisms through:

- Notification Methods
- Rules and Rule Sets

Notification Methods

A notification method represents a specific way to send notifications. Besides e-mail, there are three types of notification methods: OS Command, PL/SQL, SNMP Traps. When configuring a notification method, you need to specify the particulars associated with a specific notification mechanism such as which SMTP gateway(s) to use for e-mail or which custom OS script to run. Super Administrators perform a one-time setup of the various types of notification methods available for use.

Rules

A rule instructs Enterprise Manager to take specific action when events or incidents (entity containing one important event or related events) occur, such as notifying an administrator or opening a helpdesk ticket (see Section 1.6, "Managing Events, Incidents, and Problems"). For example, you can define a rule that specifies e-mail should be sent to you when CPU Utilization on any host target is at critical severity, or another rule that notifies an administrator’s supervisor if an incident is not acknowledged within 24 hours.

1.5.1 Customizing Notifications

Notifications that are sent to Administrators can be customized based on message type and on-call schedule. Message customization is useful for administrators who rely on both e-mail and paging systems as a means for receiving notifications. The message formats for these systems typically vary—messages sent to e-mail can be lengthy and can contain URLs, and messages sent to a pager are brief and limited to a finite number of characters. To support these types of mechanisms, Enterprise Manager allows administrators to associate a long or short message format with each e-mail address. E-mail addresses that are used to send regular e-mails can be associated with the *long* format; pages can be associated with the *short* format. The *long* format contains full details about the event/incident; the *short* format contains the most critical pieces of information.

Notifications can also be customized based on an administrator's on-call schedule. An administrator who is on-call might want to be contacted by both his pager and work email address during business hours and only by his pager address during off hours. Enterprise Manager offers a flexible notification schedule to support the wide variety of on-call schedules. Using this schedule, an administrator defines his on-call schedule by specifying the email addresses by which they should be contacted when they are on-call. For periods where they are not on-call, or do not wish to receive notifications for incidents, they simply leave that part of the schedule blank. All alerts that are sent to an administrator automatically adhere to his specified schedule.

1.6 Managing Events, Incidents, and Problems

Enterprise Manager's monitoring functionality is built upon the precept of monitoring by exception. This means it monitors and raises events when exception conditions exist in your IT environment and allowing administrators to address them in a timely manner. As discussed earlier, the two most commonly used event types to monitor for are metric alert and target availability. Although these are the most common event types for which Enterprise Manager monitors, there are many others. Available event types include:

- Target Availability
- Metric Alert
- Metric Evaluation Errors
- Job Status Changes
- Compliance Standard Rule Violations
- Compliance Standard Score Violations
- High Availability
- Service Level Agreement Alerts
- User-reported
- Application Dependency and Performance Alert
- JVM Diagnostics Threshold Violation

By definition, an incident is a unit containing a single, or closely correlated set of events that identify an issue that needs administrator attention within your managed environment. So an incident might be as simple as a single event indicating available space in a tablespace has fallen below a specified limit, or more complex such as an incident consisting of multiple events relating to potential performance issue when a server is running out of resources. Such an incident would contain events relating to the usage of CPU, I/O , and memory resources. Managing by incident gives you the ability to address issues that may consist of any number of causal factors. For an in-depth discussion on incidents and events, see Chapter 3, "Using Incident Management".

Although incidents can correspond to a single events, incidents more commonly correspond to groups of related events. A large number of discrete events can quickly become unmanageable, but handled as an assemblage of related events, incidents allow you to manage large numbers of event occurrences more effectively.

Once an incident is created, Enterprise Manager makes available a rich set of incident management workflow features that let you to manage and track the incident through its complete lifecycle. Incident management features include:

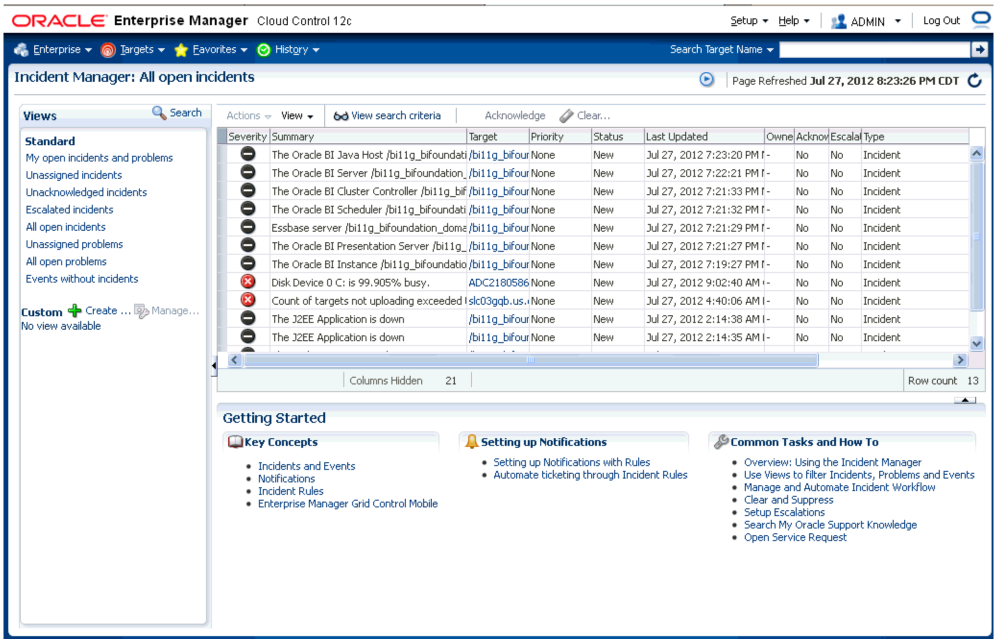
- Assign incident ownership.
- Track the incident resolution status.
- Set incident priority.
- Set incident escalation level.
- Ability to provide a manual summary.
- Ability to add user comments.
- Ability to suppress/unsuppress
- Ability to manually clear the incident.
- Ability to create a ticket manually.

Problems pertain to the diagnostic incidents and problems stored in Automatic Diagnostic Repository (ADR), which are automatically raised by Oracle software when it encounters critical errors in the software. When problems are raised for Oracle software, Oracle has determined that the recommended recourse is to open a Service Request (SR), send support the diagnostic logs, and eventually provide a solution from Oracle. A problem represents the underlying root cause of a set of incidents. Enterprise Manager provides features to track and manage the lifecycle of a problem.

1.6.1 Incident Manager

Enterprise Manager Cloud Control simplifies managing incidents through an intuitive UI called Incident Manager. Incident Manager provides and easy-to-use interface that allows you to search, view, manage, and resolve incidents and problems impacting your environment. To access Incident Manager, from the **Enterprise** menu, select **Monitoring**, and then **Incident Manager**.

Figure 1–2 Incident Manager



Incident Manager: All open incidents

Page Refreshed **Jul 27, 2012 8:23:26 PM CDT**

Views

Standard

- My open incidents and problems
- Unassigned incidents
- Unacknowledged incidents
- Escalated incidents
- All open incidents
- Unassigned problems
- All open problems
- Events without incidents

Custom

No view available

Severity	Summary	Target	Priority	Status	Last Updated	Owne	Acknov	Escalat	Type
⊖	The Oracle BI Java Host /bi11g_bifoundati	/bi11g_bifour	None	New	Jul 27, 2012 7:23:20 PM	-	No	No	Incident
⊖	The Oracle BI Server /bi11g_bifoundation_	/bi11g_bifour	None	New	Jul 27, 2012 7:22:21 PM	-	No	No	Incident
⊖	The Oracle BI Cluster Controller /bi11g_bif	/bi11g_bifour	None	New	Jul 27, 2012 7:21:33 PM	-	No	No	Incident
⊖	The Oracle BI Scheduler /bi11g_bifoundati	/bi11g_bifour	None	New	Jul 27, 2012 7:21:32 PM	-	No	No	Incident
⊖	Essbase server /bi11g_bifoundation_dome	/bi11g_bifour	None	New	Jul 27, 2012 7:21:29 PM	-	No	No	Incident
⊖	The Oracle BI Presentation Server /bi11g_	/bi11g_bifour	None	New	Jul 27, 2012 7:21:27 PM	-	No	No	Incident
⊖	The Oracle BI Instance /bi11g_bifoundatio	/bi11g_bifour	None	New	Jul 27, 2012 7:19:27 PM	-	No	No	Incident
⊗	Disk Device 0 C: is 99.905% busy.	ADC2180586	None	New	Jul 27, 2012 9:02:40 AM	-	No	No	Incident
⊗	Count of targets not uploading exceeded	slc03gqb.us.	None	New	Jul 27, 2012 4:40:06 AM	-	No	No	Incident
⊖	The J2EE Application is down	/bi11g_bifour	None	New	Jul 27, 2012 2:14:38 AM	-	No	No	Incident
⊖	The J2EE Application is down	/bi11g_bifour	None	New	Jul 27, 2012 2:14:35 AM	-	No	No	Incident

Columns Hidden 21

Row count 13

Getting Started

Key Concepts

- Incidents and Events
- Notifications
- Incident Rules
- Enterprise Manager Grid Control Mobile

Setting up Notifications

- Setting up Notifications with Rules
- Automate ticketing through Incident Rules

Common Tasks and How To

- Overview: Using the Incident Manager
- Use Views to filter Incidents, Problems and Events
- Manage and Automate Incident Workflow
- Clear and Suppress
- Setup Escalations
- Search My Oracle Support Knowledge
- Open Service Request

From the Incident Manager UI, you can:

- Filter incidents, problems, and events by using custom views
- Respond and work on an incident
- Manage incident lifecycle including assigning, acknowledging, tracking its status, prioritization, and escalation
- Access (in context) My Oracle Support knowledge base articles and other Oracle documentation to help resolve the incident.
- Access direct in-context diagnostic/action links to relevant Enterprise Manager functionality allowing you to quickly diagnose or resolve the incident.

1.6.2 Incident Rules and Rule Sets

An *incident rule* specifies criteria and actions that determine when a notification should be sent and how it should be sent whenever an event or incident is raised. The criteria defined within a rule can apply to attributes such as the target type, events and severity states (clear, warning or critical) and the notification method that should be used when an incident is raised that matches the rule criteria. Rule actions can be conditional in nature. For example, a rule action can be defined to page a user when an incident severity is critical or just send e-mail if it is warning.

A *rule set* is a collection of rules that apply to a common set of targets such as hosts, databases, groups, jobs, metric extensions, or self updates and take appropriate actions to automate the business processes underlying incident. Incident rule sets can be made public for sharing across administrators. For example, administrators can subscribe to the same rule set if they are interested in receiving notifications for the same criteria defined in the rule. Alternatively, an Enterprise Manager Super Administrator can assign incident rule sets to other administrators so that they receive notifications for incidents as defined in the rule.

In addition to being used by the notification system (see *Rules* in Section 1.5, "Notifications"), rule sets can also instruct Enterprise Manager to perform other actions, such as creating incidents, updating incidents, or call into a trouble ticketing system as discussed in Section 1.6.3, "Connectors".

1.6.3 Connectors

An Oracle Management Connector integrates third-party management systems with Enterprise Manager. There are two types of connectors: Event connectors and helpdesk connectors.

Using the event connector, you can configure Enterprise Manager to share events with non-Oracle management systems. The connector monitors all events sent from Oracle Enterprise Manager and automatically updates alert information in the third-party management system. Event connectors support the following functions:

- Sharing of event information from Oracle Enterprise Manager to the third-party management system.
- Customization of event to alert mappings between Oracle Enterprise Manager and the third-party management system.
- Synchronization of event changes in Oracle Enterprise Manager with the alerts in the third-party management system.

Using the helpdesk connector, you can configure Enterprise Manager to create, update, or close a ticket for any event created in Enterprise Manager. The ticket generated by the connector contains the relevant information about the Enterprise Manager incident, including a link to the Enterprise Manager console to enable helpdesk analysts leverage Enterprise Manager's diagnostic and resolution features to resolve the incident. In Enterprise Manger, the ticket ID, ticket status, and link to the third-party ticketing system is the shown in the context of the incident. This provides Enterprise Manager administrators with ticket status information and an easy way to quickly access the ticket.

Available connectors include:

- BMC Remedy Service Desk Connector
- HP Service Manager Connector
- CA Service Desk Connector
- HP Operations Manager Connector
- Microsoft Systems Center Operations Manager Connector
- IBM Tivoli Enterprise Console Connector
- IBM Tivoli Netcool/OMNIbus Connector

For more information about Oracle-built connectors, see the Enterprise Manager Plug-ins Exchange.

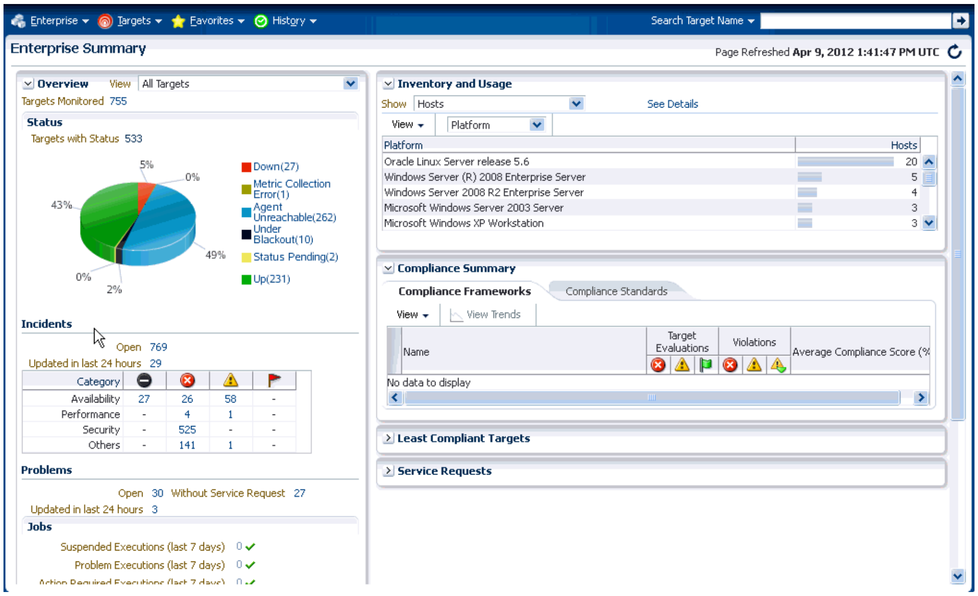
http://www.oracle.com/goto/emextensibility

1.7 Accessing Monitoring Information

Enterprise Manager provides multiple ways to access monitoring information. The primary focal point for incident management is the Incident Manager console, however Enterprise Manager also provides other ways to access monitoring information. The following figures show the various locations within Enterprise Manager that display target monitoring information. The following figure shows the

Enterprise Manager Overview page that conveniently displays target status rollup and rollup of incidents.

Figure 1–3 Enterprise Manager Console



Enterprise Summary

Page Refreshed **Apr 9, 2012 1:41:47 PM UTC**

Overview View All Targets

Targets Monitored 755

Status

Targets with Status 533

Incidents

Open 769

Updated in last 24 hours 29

Category	⊖	⊗	⚠	🚩
Availability	27	26	58	-
Performance	-	4	1	-
Security	-	525	-	-
Others	-	141	1	-

Problems

Open 30 Without Service Request 27

Updated in last 24 hours 3

Jobs

Suspended Executions (last 7 days) 0 ✓

Problem Executions (last 7 days) 0 ✓

Action Required Executions (last 7 days) 0 ✓

Inventory and Usage

Show Hosts

View Platform

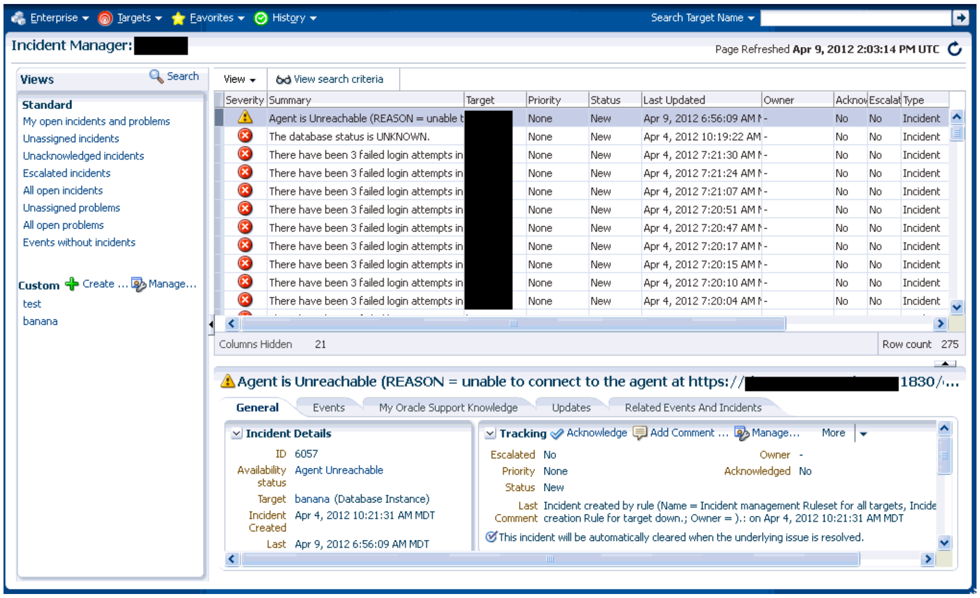
Platform	Hosts
Oracle Linux Server release 5.6	20
Windows Server (R) 2008 Enterprise Server	5
Windows Server 2008 R2 Enterprise Server	4
Microsoft Windows Server 2003 Server	3
Microsoft Windows XP Workstation	3

Compliance Summary

Name	Target Evaluations			Violations			Average Compliance Score (%
	⊗	⚠	🚩	⊗	⚠	⚠	
No data to display							

The next figure shows the Incident Manager home page which displays incidents for a system or target.

Figure 1–4 Incident Manager (in context of a system or target)



Incident Manager: [redacted]

Page Refreshed **Apr 9, 2012 2:03:14 PM UTC**

Views

Standard

My open incidents and problems
Unassigned incidents
Unacknowledged incidents
Escalated incidents
All open incidents
Unassigned problems
All open problems
Events without incidents

Custom

test
banana

Severity	Summary	Target	Priority	Status	Last Updated	Owner	Acknov	Escalat	Type
⚠	Agent is Unreachable (REASON = unable t	[redacted]	None	New	Apr 9, 2012 6:56:09 AM I	-	No	No	Incident
⊗	The database status is UNKNOWN.	[redacted]	None	New	Apr 4, 2012 10:19:22 AM	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:21:30 AM I	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:21:24 AM I	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:21:07 AM I	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:51 AM I	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:47 AM I	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:17 AM I	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:15 AM I	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:10 AM I	-	No	No	Incident
⊗	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:04 AM I	-	No	No	Incident

Columns Hidden 21 Row count 275

⚠ Agent is Unreachable (REASON = unable to connect to the agent at https://[redacted]1830/...

Incident Details

ID 6057
Availability status Agent Unreachable
Target banana (Database Instance)
Incident Created Apr 4, 2012 10:21:31 AM MDT
Last Apr 9, 2012 6:56:09 AM MDT

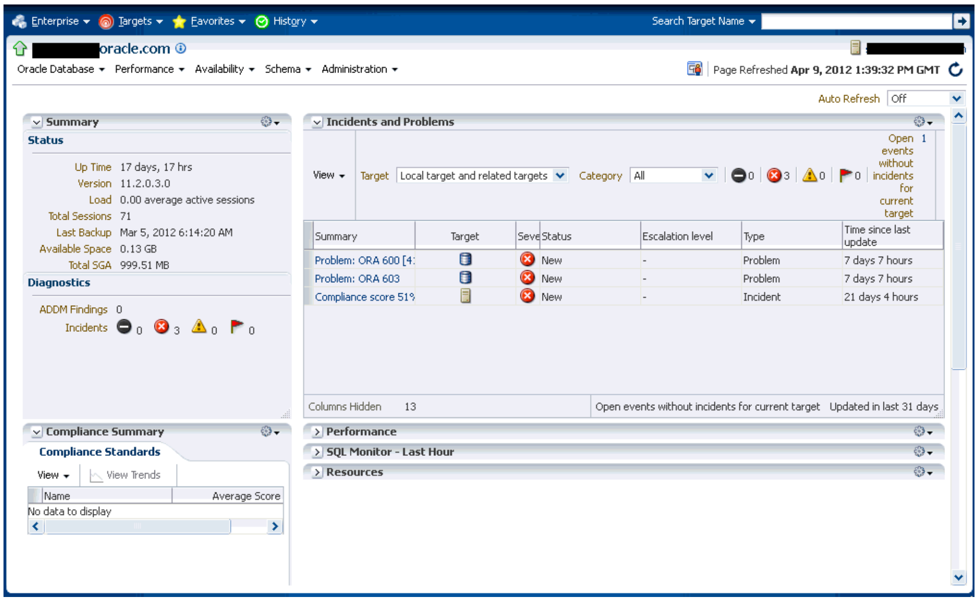
Tracking

Escalated No
Priority None
Status New
Owner -
Acknowledged No
Last Comment Incident created by rule (Name = Incident management Ruleset for all targets, Incide creation Rule for target down.; Owner =).: on Apr 4, 2012 10:21:31 AM MDT

✓ This incident will be automatically cleared when the underlying issue is resolved.

Monitoring information is also displayed on target home pages. In the following figure, you can see target status as well as a rollup of incidents.

Figure 1–5 Target Home Pages



Page Refreshed **Apr 9, 2012 1:39:32 PM GMT**

Auto Refresh: Off

Status

Up Time	17 days, 17 hrs
Version	11.2.0.3.0
Load	0.00 average active sessions
Total Sessions	71
Last Backup	Mar 5, 2012 6:14:20 AM
Available Space	0.13 GB
Total SGA	999.51 MB

Diagnostics

ADDM Findings	0
Incidents	⊖ 0 ✖ 3 ⚠ 0 ⚑ 0

Target: Local target and related targets Category: All ⊖ 0 ✖ 3 ⚠ 0 ⚑ 0 Open events without incidents for current target: 1

Summary	Target	Seve	Status	Escalation level	Type	Time since last update
Problem: ORA 600 [4:		✖	New	-	Problem	7 days 7 hours
Problem: ORA 603		✖	New	-	Problem	7 days 7 hours
Compliance score 51%		✖	New	-	Incident	21 days 4 hours

Columns Hidden 13 Open events without incidents for current target Updated in last 31 days

Name	Average Score
No data to display	

2 Discovering, Promoting, and Adding Targets

Enterprise Manager Cloud Control (Cloud Control) enables you to discover, promote, add, and then monitor software deployments across your network, using a single GUI-rich console. This chapter introduces you to the concepts of discovery, promotion, and monitoring, and describes how you can perform these tasks using Cloud Control.

In particular, this chapter covers the following:

- About Discovering, Promoting, and Adding Targets
- Discovering and Promoting All Target Types
- Discovering and Promoting Oracle Homes
- Discovering, Promoting, and Adding Database Targets
- Discovering, Promoting, and Adding Middleware Targets

2.1 About Discovering, Promoting, and Adding Targets

- About Discovering, Promoting, and Monitoring Hosts and Targets
- Discovery and Monitoring in Enterprise Manager Lifecycle
- Discovery and Monitoring Process

2.1.1 About Discovering, Promoting, and Monitoring Hosts and Targets

This section describes the following:

- What are Targets and Managed Targets?
- What is Discovery?
- What is Promotion?
- What is Monitoring?

2.1.1.1 What are Targets and Managed Targets?

Targets are entities such as host machines, databases, Fusion Middleware components, that can be managed and monitored in Cloud Control.

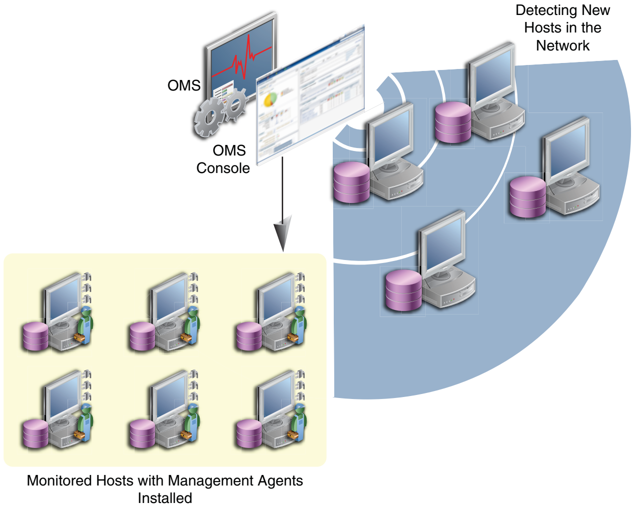
Managed targets are entities that are actively being monitored and managed by Cloud Control.

2.1.1.2 What is Discovery?

Discovery refers to the process of identifying unmanaged hosts and targets in your environment. You can discover hosts and targets automatically or manually.

Figure 2–1 illustrates the discovery process.

Figure 2–1 Discovery


Detecting New Hosts in the Network
OMS
OMS Console
Monitored Hosts with Management Agents Installed

You can discover targets using either of the following methods:

Autodiscovery Process

For discovery of a host, the autodiscovery process enables a Management Agent running on the host to run an Enterprise Manager job that scans for unmanaged hosts. You then convert these unmanaged hosts to managed hosts by deploying Management Agents on these hosts. Next, you search for targets such as databases or other deployed components or applications on these managed hosts, and finally you promote these targets to managed status.

For discovery of targets, the autodiscovery process enables you to search for targets on the host and then add these targets using Enterprise Manager.

The benefit of using this process is that as new components are added to your infrastructure, they can be found and brought under management on a regularly-scheduled basis.

Guided Discovery Process

The guided discovery process enables you to explicitly add a specific database target as a target to bring under management. The discovery wizard guides you through the process and most of the specifications required are filled by default.

The benefits of using this process are as follows:

- You can find targets with less effort.
- You can find a new database that has been added recently even if autodiscovery has not been run.
- You can find a non-promoted database that already exists in autodiscovery results, but has a change in details. For example, the port.
- You eliminate unnecessary consumption of resources on the Management Agent when discovery is not needed.

Specifying Target Monitoring Properties

Specifying target monitoring properties enables you to manually specify all the details required to discover the database target, such as the host name and location, target name and location, and other specific information. This process is generally used when the autodiscovery process and guided discovery process fails to discover the target that you want to add.

For more information on how to discover unmanaged hosts refer to Step 1: Discovering Unmanaged Hosts Using Network Scan.

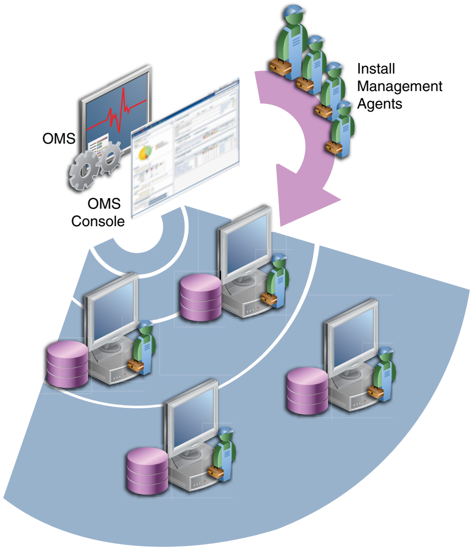
For more information on how to discover targets on managed hosts refer to Step 3: Discovering Targets on Managed Hosts

2.1.1.3 What is Promotion?

Promotion refers to the process of converting unmanaged hosts and targets, which have been discovered in your network, to managed hosts and targets in Cloud Control so that they can be monitored and managed efficiently. While conversion of unmanaged hosts to managed hosts involves deployment of a Management Agent on those hosts, conversion of unmanaged targets running on those hosts to managed targets involves only adding the targets as manageable entities in Cloud Control without deploying any additional component on the hosts.

Figure 2–2 illustrates the promotion process.

Figure 2–2 Promotion



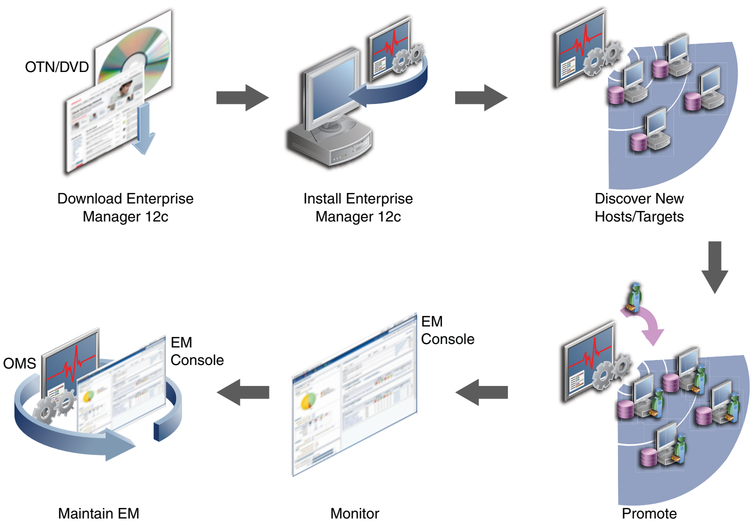
2.1.1.4 What is Monitoring?

Monitoring refers to the process of gathering information and keeping track of activity, status, performance, and health of targets managed by Cloud Control on your host. A Management Agent deployed on the host in conjunction with plug-ins monitors every managed target on the host.

2.1.2 Discovery and Monitoring in Enterprise Manager Lifecycle

Figure 2–3 illustrates the lifecycle process of discovering and monitoring targets in Cloud Control.

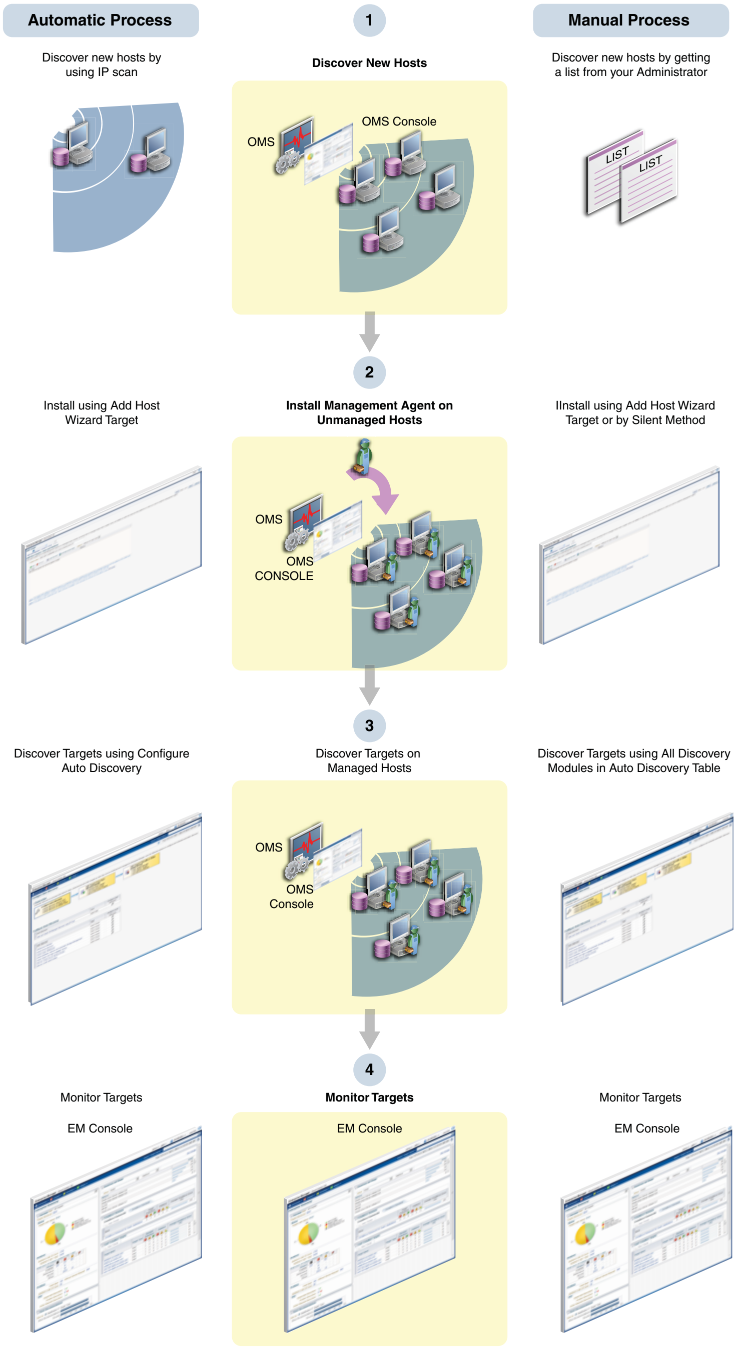
Figure 2–3 Discovery and Monitoring in Enterprise Manager Lifecycle


OTN/DVD
Download Enterprise Manager 12c
Install Enterprise Manager 12c
Discover New Hosts/Targets
OMS
EM Console
EM Console
Maintain EM
Monitor
Promote

2.1.3 Discovery and Monitoring Process

Figure 2–4 illustrates the high level process of discovering and monitoring targets:

Figure 2–4 Discovery and Monitoring Process


Automatic Process
1
Manual Process
Discover new hosts by using IP scan
Discover New Hosts
Discover new hosts by getting a list from your Administrator
OMS
OMS Console
LIST
LIST
2
Install using Add Host Wizard Target
Install Management Agent on Unmanaged Hosts
IInstall using Add Host Wizard Target or by Silent Method
OMS
OMS CONSOLE
3
Discover Targets using Configure Auto Discovery
Discover Targets on Managed Hosts
Discover Targets using All Discovery Modules in Auto Discovery Table
OMS
OMS Console
4
Monitor Targets
Monitor Targets
Monitor Targets
EM Console
EM Console
EM Console

2.2 Discovering and Promoting All Target Types

This section covers the following:

- Discovering and Promoting All Target Types Using the Autodiscovery Process
- Discovering and Adding All Target Types Using the Guided Discovery Process
- Discovering and Adding All Target Types By Specifying Target Monitoring Properties

- Retrieving Deleted Targets

2.2.1 Discovering and Promoting All Target Types Using the Autodiscovery Process

This section covers the following:

- Meeting the Prerequisites
- Discovering and Promoting All Target Types

2.2.1.1 Meeting the Prerequisites

Before you discover targets using the autodiscovery process, meet these prerequisites:

- To run automatic host discovery (Nmap binary) on a Management Agent installed on a Solaris system, follow these steps:
  1. Install Cloud Control 3.4.3 or higher on the Solaris system.
  2. Stop the Management Agent from the running.
  3. Execute the following commands on the terminal session which you will use to start the Management Agent:

     ```
     bash-2.03$ LD_LIBRARY_PATH=<directory path of Cloud ControlCloud
     Control libraries>:$LD_LIBRARY_PATH
     ```

     ```
     bash-2.03$ export LD_LIBRARY_PATH
     ```

     Note: These steps ensure that Nmap refers to the Cloud Control libraries while the Management Agent is running.

  4. Start the Management Agent using the terminal session used for the previous step.

     Note: Add `LD_LIBRARY_PATH` to your start up scripts so that this setting is retained after you reboot your system.

- To discover hosts from a Management Agent running on the following systems, follow the prerequisites stated in Table 2–1.

Table 2–1 Prerequisites for discovering hosts

System	Prerequisites

Solaris 11 cluster (SPARC or x86-64)	Create a static IPv4 address on interface `net0`:
	`ipadm create-addr -T static -a local=X.X.X.X/YY net0/ZZ`
	Here, `X.X.X.X` is a static IPv4 address, `YY` is the sub network mask, and `ZZ` is the specific identity for the `net0` interface. The created static address will subsequently be identified by `net0/ZZ`.
	For example:
	`ipadm create-addr -T static -a local=10.134.108.101/24 net0/hh`

Table 2–1 (Cont.) Prerequisites for discovering hosts

System	Prerequisites
SUSE Linux for System z™	**1.** Run the `QETH_OPTIONS='fake_ll=1'` option by adding it to the configuration file for the NIC present in the `/etc/sysconfig/hardware directory.` The name of the configuration file changes according to the NIC used. Contact your system administration for the name of the configuration file that your system uses. **2.** Restart your system for the changes to take effect.
RedHat Linux for System z	**1.** Run the `OPTIONS='fake_ll=1'` option by adding it to the configuration file for the NIC present in the `/etc/sysconfig/network-scripts` directory. The name of the configuration file changes according to the NIC used. Contact your system administration for the name of the configuration file that your system uses. **2.** Verify that the alias in the `/etc/modprobe.conf` file includes the following command: `alias eth0 geth` **3.** Restart the system for the changes to take effect.

2.2.1.2 Discovering and Promoting All Target Types

To discover and promote all target types using autodiscovery process, follow these steps:

- Step 1: Discovering Unmanaged Hosts Using Network Scan
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Discovering Targets on Managed Hosts
- Step 4: Promoting Targets to Managed Status

2.2.1.2.1 Step 1: Discovering Unmanaged Hosts Using Network Scan

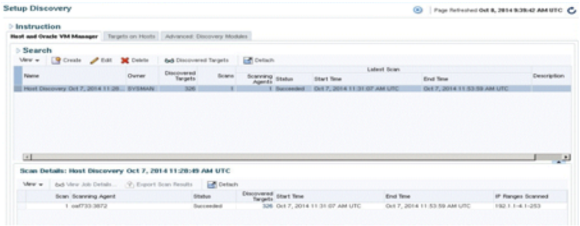
> **Note:** Skip this step if host is already managed in Enterprise Manager.

To discover and configure hosts using IP scan, follow these steps:

> **Note:** If automatic host discovery is not available for your platform, deploy the Management Agent manually. To deploy the Management Agent, refer to following URL:
>
> http://docs.oracle.com/cd/E24628_01/install.121/e24089/install_agent_usng_rsp.htm

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

2. On the Setup Discovery page, in the Host and Oracle VM Manager tab, click **Create.** You will now create the discover job. By default, the Name field will be populated with a title including that date and time the job was created. Note that you can edit the discovery jobs and schedule discovery to run immediately or later.

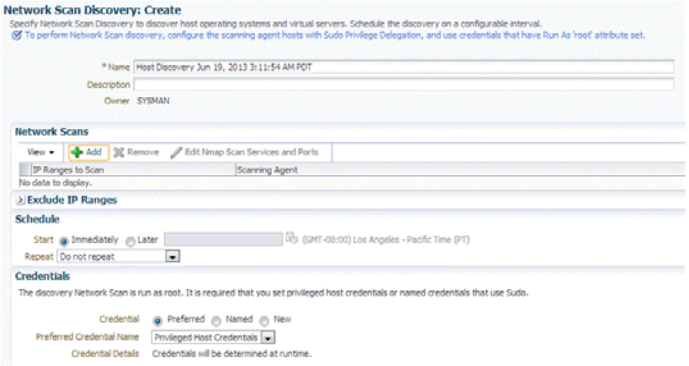

Setup Discovery
Page Refreshed Oct 8, 2014 9:39:42 AM UTC
Instruction
Host and Oracle VM Manager
Targets on Hosts
Advanced Discovery Modules
Search
View
Create
Edit
Delete
Discovered Targets
Detach

Name	Owner	Discovered Targets	Scans	Latest Scan Scanning Agents	Status	Start Time	End Time	Description
Host Discovery Oct 7, 2014 11:28...	SYSMAN	326	1	1	Succeeded	Oct 7, 2014 11:31:07 AM UTC	Oct 7, 2014 11:53:59 AM UTC	

Scan Details: Host Discovery Oct 7, 2014 11:28:49 AM UTC

Scan	Scanning Agent	Status	Discovered Targets	Start Time	End Time	IP Ranges Scanned
1	oaf733:3872	Succeeded	326	Oct 7, 2014 11:31:07 AM UTC	Oct 7, 2014 11:53:59 AM UTC	192.1.1-4.1-253

3. On the Network Scan Discovery: Create page, click **Add**. You will now select the Management Agent that will perform the network scan. You can select the Management Agent that is installed by default on the Oracle Management Service host, or can select another Agent if desired.



Network Scan Discovery: Create

Specify Network Scan Discovery to discover host operating systems and virtual servers. Schedule the discovery on a configurable interval.

To perform Network Scan discovery, configure the scanning agent hosts with Sudo Privilege Delegation, and use credentials that have Run As 'root' attribute set.

* Name: Host Discovery Jun 19, 2013 3:11:54 AM PDT

Description:

Owner: SYSMAN

Network Scans

IP Ranges to Scan	Scanning Agent

No data to display.

Exclude IP Ranges

Schedule

Start ● Immediately ○ Later (GMT-08:00) Los Angeles - Pacific Time (PT)

Repeat: Do not repeat

Credentials

The discovery Network Scan is run as root. It is required that you set privileged host credentials or named credentials that use Sudo.

Credential ● Preferred ○ Named ○ New

Preferred Credential Name: Privileged Host Credentials

Credential Details: Credentials will be determined at runtime.

Note that because the entire network will be scanned, the Sudo Privilege Delegation must be set on the Management Agent host that will perform the scan.

4. Select the agent in the IP Ranges for scan table, and enter the IP ranges to scan. You can specify any or even all of the following:

   - One or more absolute hostnames, each separated by a space; for example: `host1.example.com host3.example.com`
   - One or more IP addresses, each separated by a space
   - A range of addresses; for example: `10.0.0-255.1-250`. Note that IP addresses and IP ranges must be separated by a comma; for example: `10.0.0-255.1-250`
   - Classless Inter-Domain Routing (CIDR) notations; for example: `128.16.10.0/24`

   Separate each value with a space; for example:

   ```
   host1.example.com 192.168.0.1 128.16.10.0/24 10.0.0-255.1-250,254
   ```

5. A default list of ports to scan within the IP ranges you specified is listed in the Configure Ports table. These are default ports typically used by the listed Oracle components.

To modify the port values for a component, select the component in the table and change the values accordingly. Up to 10 ports and/or port ranges can be specified.

6. If you want to add more component ports to the list, click **Add**. Enter the name of the service to include, and specify the port(s) or port range to scan.

7. Specify the following:

   - The schedule at which the discovery job will run. Note that you can start the job immediately.

   - The credentials set on the Management Agent that will perform the scan.

     As noted, the Sudo Privilege Delegation must be set on the Management Agent host that will perform the scan. The named credential that will be used must be configured to run as root.

   Click **Save and Submit Scan.**

8. After the discovery job executes, you can check for discovered hosts that may contain potential targets. You can do this two ways:

   - Select the job in the Host Discovery page, then click **View Discovered Targets**;

     or:

   - From the **Setup** menu, select **Add Target**, then select **Auto Discovery Results**.

2.2.1.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

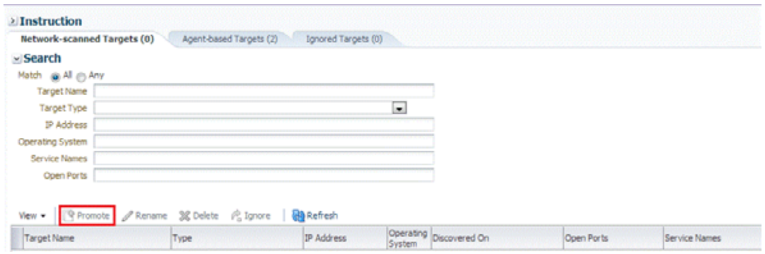
> **Note:** Skip this step if host is already managed in Enterprise Manager.

To convert unmanaged hosts to managed hosts, follow these steps:

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

2. On the Auto Discovery Results page, select the **Network-scanned Targets** tab. All discovered hosts are listed, with the open ports and identifiable service names shown. Based on your understanding of the Oracle components deployed on your network, you should be able to determine the types of potential targets that have been discovered.

3. Select a host from the table, then click **Promote** to promote the host to managed target status. The Add Host Targets wizard opens. You will use this wizard to install a Management Agent on the host.



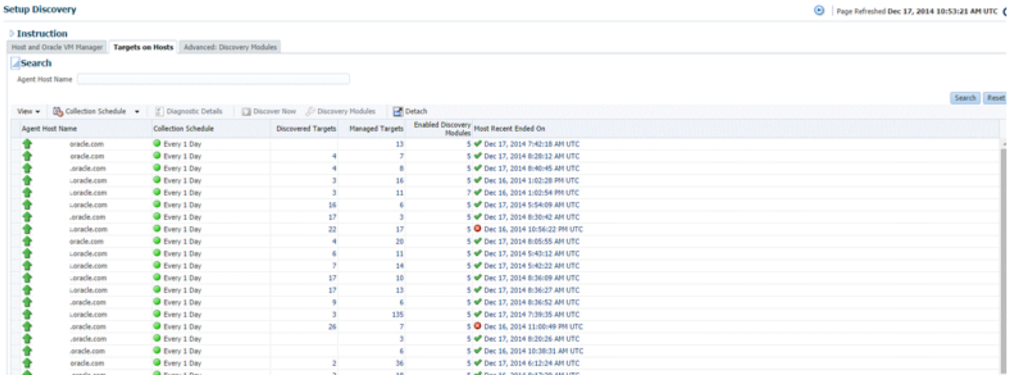
Installing a Management Agent on an unmanaged host promotes the unmanaged host to managed target status, thereby converting the host to a managed host.

2.2.1.2.3 Step 3: Discovering Targets on Managed Hosts

To discover targets on managed hosts, follow these steps:

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

2. On the Setup Discovery page, in the **Targets on Hosts** tab, expand **Search,** then enter the hostname for the host you want to check for targets in the Agent Host Name field. The host must have a Management Agent installed on it.



Agent Host Name	Collection Schedule	Discovered Targets	Managed Targets	Enabled Discovery Modules	Most Recent Ended On
oracle.com	● Every 1 Day		13	5	✓ Dec 17, 2014 7:42:18 AM UTC
oracle.com	● Every 1 Day	4	7	5	✓ Dec 17, 2014 8:28:12 AM UTC
.oracle.com	● Every 1 Day	4	8	5	✓ Dec 17, 2014 8:40:45 AM UTC
.oracle.com	● Every 1 Day	3	16	5	✓ Dec 16, 2014 1:02:28 PM UTC
.oracle.com	● Every 1 Day	3	11	7	✓ Dec 16, 2014 1:02:54 PM UTC
.oracle.com	● Every 1 Day	16	6	5	✓ Dec 17, 2014 5:54:09 AM UTC
.oracle.com	● Every 1 Day	17	3	5	✓ Dec 17, 2014 8:30:42 AM UTC
.oracle.com	● Every 1 Day	22	17	5	⊗ Dec 16, 2014 10:56:22 PM UTC
oracle.com	● Every 1 Day	4	20	5	✓ Dec 17, 2014 8:05:55 AM UTC
.oracle.com	● Every 1 Day	6	11	5	✓ Dec 17, 2014 5:43:12 AM UTC
.oracle.com	● Every 1 Day	7	14	5	✓ Dec 17, 2014 5:42:22 AM UTC
.oracle.com	● Every 1 Day	17	10	5	✓ Dec 17, 2014 8:36:09 AM UTC
.oracle.com	● Every 1 Day	17	13	5	✓ Dec 17, 2014 8:36:27 AM UTC
.oracle.com	● Every 1 Day	9	6	5	✓ Dec 17, 2014 8:36:52 AM UTC
.oracle.com	● Every 1 Day	3	135	5	✓ Dec 17, 2014 7:39:35 AM UTC
.oracle.com	● Every 1 Day	26	7	5	⊗ Dec 16, 2014 11:00:49 PM UTC
.oracle.com	● Every 1 Day		3	5	✓ Dec 17, 2014 8:20:26 AM UTC
.oracle.com	● Every 1 Day		6	5	✓ Dec 16, 2014 10:38:31 AM UTC
oracle.com	● Every 1 Day	2	36	5	✓ Dec 17, 2014 6:12:24 AM UTC

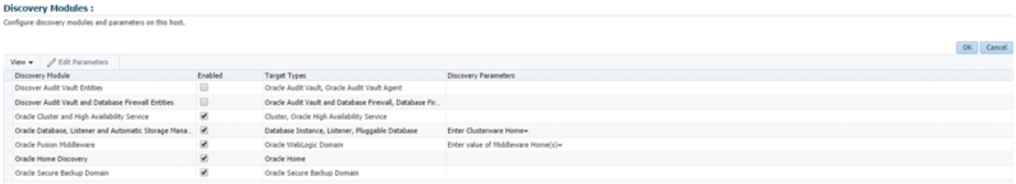
3. On the Target Discovery (Agent-based) page, expand **Search,** then enter the hostname for the host you want to check for targets in the Agent Host Name field. The host must have a Management Agent installed on it.

4. To search for a specific Management Agent, click **Search.** The table lists all the Management Agents and filters the list based on what you search for.

5. Select the host in the table and click **Discovery Modules.**

6. On the Discovery Modules page, select the target types that you want to discover on the host. Select the target types you want to discover on the host. Note that you must supply search parameters for some target types. To specify a parameter, select the target type in the Discovery Module column and click **Edit Parameters.**

   - Oracle Cluster and High Availability Service: No parameters required.
   - Oracle Database, Listener and Automatic Storage Management: Specify the path to the Clusterware Home.
   - Oracle Home Discovery: No parameters required.
   - Oracle Secure Backup Domain: No parameters required.
   - Oracle Fusion Middleware: Specify * (the "star" character) to search all Middleware Homes, or specify the path to one or more Middleware Homes on the host, each separated by a comma.



Discovery Modules :

Configure discovery modules and parameters on this host.

Discovery Module	Enabled	Target Types	Discovery Parameters
Discover Audit Vault Entities	□	Oracle Audit Vault, Oracle Audit Vault Agent	
Discover Audit Vault and Database Firewall Entities	□	Oracle Audit Vault and Database Firewall, Database Fir...	
Oracle Cluster and High Availability Service	☑	Cluster, Oracle High Availability Service	
Oracle Database, Listener and Automatic Storage Mana...	☑	Database Instance, Listener, Pluggable Database	Enter Clusterware Home=
Oracle Fusion Middleware	☑	Oracle WebLogic Domain	Enter value of Middleware Home(s)=
Oracle Home Discovery	☑	Oracle Home	
Oracle Secure Backup Domain	☑	Oracle Secure Backup Domain	

Click **OK** when finished. Target discovery has been configured on this host.

7. On the Setup Discovery page, in the Targets on Host tab, select the hosts you want to set the schedule at which discovery will be run. Click **Collection Schedule,** and then select **For all hosts,** or **For selected hosts.** In the Collection Schedule dialog box, enable or disable collection for the hosts that you have selected. If you have enabled collection, then select the frequency of collection. This schedule will be applied to all selected hosts. By default the discovery will run every 24 hours. Click **OK.**

8. Repeat these steps for each additional host on which you want to configure discovery.

9. Click **Discover Now** to discover targets immediately. The discovery will also run at the scheduled interval.

2.2.1.2.4 Step 4: Promoting Targets to Managed Status

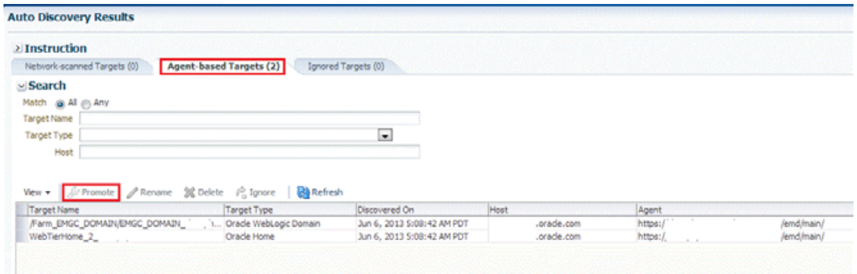
To promote discovered targets to managed status, follow these steps:

1. After the discovery job executes, you can check for discovered hosts that may contain potential targets. You can do this two ways:

   - Select the job in the Host Discovery page, then click **View Discovered Targets**; or

   - From the **Setup** menu, select **Add Target**, then select **Auto Discovery Results**.

2. Select a target to promote, then click **Promote**. A wizard specific to the target type you are promoting opens. Supply the required values.



Auto Discovery Results

Instruction

Network-scanned Targets (0) | Agent-based Targets (2) | Ignored Targets (0)

Search

Match ● All ○ Any

Target Name

Target Type

Host

Target Name	Target Type	Discovered On	Host	Agent
/Farm_EMGC_DOMAIN/EMGC_DOMAIN_ ...	Oracle WebLogic Domain	Jun 6, 2013 5:08:42 AM PDT	.oracle.com	https:/ /emd/main/
WebTierHome_2_	Oracle Home	Jun 6, 2013 5:08:42 AM PDT	.oracle.com	https:/ /emd/main/

3. Click the **Agent-based Targets** tab.You can choose one or several targets to promote.

4. Note that you can optionally click **Ignore** for a discovered target. Ignoring a target puts it into a list of targets that you do not want to manage.

   Ignored targets will be displayed in the Ignored Targets tab, and will remain in Cloud Control as un-managed targets until you decide to either promote or remove them. If you delete a target, it would be rediscovered the next time discovery runs.

5. Check the target type home page to verify that the target is promoted as an Cloud Control target. Once a target is successfully promoted, the Management Agent installed on the target host will begin collecting metric data on the target.

Note:

- When you promote a discovered target to managed status, the plug-in required for the target is automatically deployed to the Management Agent, which monitors the host where the target has been discovered. For the plug-in to be deployed, the Management Agent must be secure. Therefore, before promoting the discovered targets to managed status, ensure that the Management Agent is secure. You can always unsecure it after the discovered target is promoted to managed status, that is, after the required plug-in is deployed.

  To verify the secure status of a Management Agent, and to secure it if required, use any one of the following methods:

  - From the **Setup** menu, select **Manage Cloud Control,** and then click **Agents**. Click the required Management Agent. Verify whether the Management Agent is secure. If it is not secure, from the **Agent** menu, click **Secure** to secure it.
  - Run the following command to verify if the Management Agent is secure:

    ```
    <EMSTATE>/bin/emctl status agent
    ```

    If the Management Agent is secure, the Management Agent URL displayed in the output of the previous command is an HTTPS URL. However, if the Management Agent URL displayed is an HTTP URL, secure the Management Agent by running the following command:

    ```
    <EMSTATE>/bin/emctl secure agent
    ```

- Cloud Control supports simultaneous promotion of multiple targets only for some target types. Additionally, multiple selection of database targets has been disabled to avoid a user selecting RAC databases across clusters. This is similar to the user-guided discovery feature where a user cannot discover targets across a cluster in the same session.

2.2.2 Discovering and Adding All Target Types Using the Guided Discovery Process

To discover and add all target types using the guided process, follow these steps:

- Step 1: Identifying Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Targets

2.2.2.1 Step 1: Identifying Unmanaged Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Identify the unmanaged hosts by getting the list of hosts from your administrator or by checking the Auto Discovery Results page by selecting the **Setup** menu, **Add Targets,** and then **Auto Discovery Results.**

2.2.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

To convert unmanaged hosts to managed hosts manually, you should manually install a Management Agent on each host. You can install a Management Agent in graphical or in silent mode.

For instructions to install in graphical mode, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.* For instructions to install in silent mode, see *Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

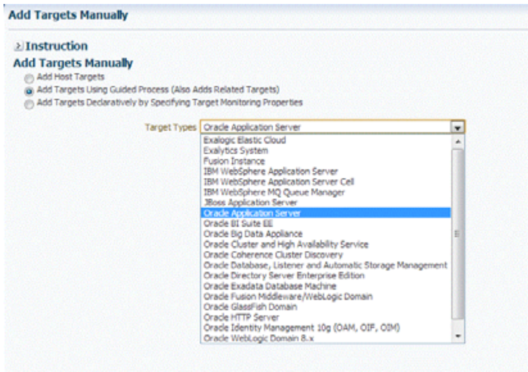
2.2.2.3 Step 3: Adding Targets

To add targets using the guided process, follow these steps:

Note: When you add a target using the guided process, some scripts and automated processes are run that are particular for the target type that you select. You may have to input credentials in order to run the guided process.

---

1. From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**. Cloud Control displays the Add Targets Manually page.
2. On the Add Targets Manually page, select **Add Targets Using Guided Process (Also Adds Related Targets)**.
3. Choose one of the target types to add from the Target Types list, such as **Exalogic Elastic Cloud, Oracle Cluster and High Availability Service,** or **Oracle WebLogic Domain.** Click **Add Using Guided Process...**



Add Targets Manually

Instruction

Add Targets Manually

○ Add Host Targets
● Add Targets Using Guided Process (Also Adds Related Targets)
○ Add Targets Declaratively by Specifying Target Monitoring Properties

Target Types: Oracle Application Server

Exalogic Elastic Cloud
Exalytics System
Fusion Instance
IBM WebSphere Application Server
IBM WebSphere Application Server Cell
IBM WebSphere MQ Queue Manager
JBoss Application Server
Oracle Application Server
Oracle BI Suite EE
Oracle Big Data Appliance
Oracle Cluster and High Availability Service
Oracle Coherence Cluster Discovery
Oracle Database, Listener and Automatic Storage Management
Oracle Directory Server Enterprise Edition
Oracle Exadata Database Machine
Oracle Fusion Middleware/WebLogic Domain
Oracle GlassFish Domain
Oracle HTTP Server
Oracle Identity Management 10g (OAM, OIF, OIM)
Oracle WebLogic Domain 8.x

4. After you select the target type, a wizard specific to the target type guides you through the process of manually adding the target.

Upon confirmation, the target becomes a managed target in Cloud Control. Cloud Control simply accepts the information, performs validation of the supplied data where possible and starts monitoring the target.

Note: When you manually add a non-host target to Cloud Control, the plug-in required for the target is automatically deployed to the Management Agent, which monitors the host where the non-host target exists. For the plug-in to be deployed, the Management Agent must be secure. Therefore, before manually adding a non-host target to Cloud Control, ensure that the Management Agent is secure. You can always unsecure it after the target is added to Cloud Control, that is, after the required plug-in is deployed.

To verify the secure status of a Management Agent, and to secure it if required, use any one of the following methods:

- From the **Setup** menu, select **Manage Cloud Control** and then, click **Agents**. Click the required Management Agent. Verify whether the Management Agent is secure. If it is not secure, from the **Agent** menu, click **Secure** to secure it.
- Run the following command to verify if the Management Agent is secure:

  ```
  <EMSTATE>/bin/emctl status agent
  ```

  If the Management Agent is secure, the Management Agent URL displayed in the output of the previous command is an HTTPS URL. However, if the Management Agent URL displayed is an HTTP URL, secure the Management Agent by running the following command:

  ```
  <EMSTATE>/bin/emctl secure agent
  ```

2.2.3 Discovering and Adding All Target Types By Specifying Target Monitoring Properties

To discover and add all target types by specifying target monitoring properties, follow these steps:

- Step 1: Indentifying Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Targets

2.2.3.1 Step 1: Indentifying Unmanaged Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Identify the unmanaged hosts by getting the list of hosts from your administrator or by checking the Auto Discovery Results page by selecting the **Setup** menu, **Add Targets,** and then **Auto Discovery Results.**

2.2.3.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

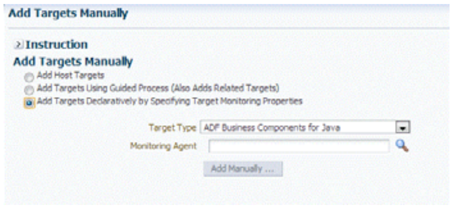
To convert unmanaged hosts to managed hosts manually, you should manually install a Management Agent on each host. You can install a Management Agent in graphical or in silent mode.

For instructions to install in graphical mode, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.* For instructions to install in silent mode, see *Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

2.2.3.3 Step 3: Adding Targets

To add a target on a managed host by specifying the target monitoring properties, follow these steps:

1. From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**. Cloud Control displays the Add Targets Manually page.
2. On the Add Targets Manually page, select **Add Targets Declaratively by Specifying Target Monitoring Properties.**



Add Targets Manually

Instruction

Add Targets Manually

○ Add Host Targets
○ Add Targets Using Guided Process (Also Adds Related Targets)
● Add Targets Declaratively by Specifying Target Monitoring Properties

Target Type: ADF Business Components for Java

Monitoring Agent:

3. Choose one of the target types to add from the Target Types list, such as **ADF Business Components for Java, Cluster Database,** or **Oracle HTTP Server.**
4. Specify the Management Agent that will be used to monitor the target, or click on the Search icon to search for and select the Management Agent. Click **Add Manually..**.
5. After you select the target type, a wizard specific to the target type guides you through the process of manually adding the target.

   Upon confirmation, the target becomes a managed target in Cloud Control. Cloud Control simply accepts the information, performs validation of the supplied data where possible and starts monitoring the target.

Note: When you manually add a non-host target to Cloud Control, the plug-in required for the target is automatically deployed to the Management Agent, which monitors the host where the non-host target exists. For the plug-in to be deployed, the Management Agent must be secure. Therefore, before manually adding a non-host target to Cloud Control, ensure that the Management Agent is secure. You can always unsecure it after the target is added to Cloud Control, that is, after the required plug-in is deployed.

To verify the secure status of a Management Agent, and to secure it if required, use any one of the following methods:

- From the **Setup** menu, select **Manage Cloud Control,** and then, click **Agents**. Click the required Management Agent. Verify whether the Management Agent is secure. If it is not secure, from the **Agent** menu, click **Secure** to secure it.
- Run the following command to verify if the Management Agent is secure:

  ```
  <EMSTATE>/bin/emctl status agent
  ```

  If the Management Agent is secure, the Management Agent URL displayed in the output of the previous command is an HTTPS URL. However, if the Management Agent URL displayed is an HTTP URL, secure the Management Agent by running the following command:

  ```
  <EMSTATE>/bin/emctl secure agent
  ```

2.2.4 Retrieving Deleted Targets

This sections covers the following:

- Retrieving Deleted Target Types
- Retrieving Deleted Host and Corresponding Management Agent Targets

2.2.4.1 Retrieving Deleted Target Types

If you have deleted one or more targets (such as a database target or a weblogic domain, or any othe target), you can retrieve them and add them back to the Enterprise Manager Cloud Control Console. If autodiscovery is configured on the host where the targets were present, the targets are automatically discovered during the next scheduled autodiscovery operation. Once they are autodiscovered, you can promote them and add them to the console. If autodiscovery is not configured on the host where the targets were present, you have to discover the targets using one of the following methods:

- By enabling autodiscovery as described in Section 2.2.1.2.3 to automatically discover the targets in the next scheduled autodiscovery operation. Once discovered, promote them as described in Section 2.2.1.2.4 and add them to the console.
- By using the guided discovery process as described in Section 2.2.2.3 to manually discover and add the discovered targets to the console.
- By specifying the target monitoring properties for each target as described in Section 2.2.3.3 to manually discover and add the discovered targets to the console.
- By using the following EM CLI verb:

```
$ emcli add_target
      -name="name"
      -type="type"
      -host="hostname"
      [-properties="pname1:pval1;pname2:pval2;..."]
      [-separator=properties="sep_string"]
      [-subseparator=properties="subsep_string"]
      [-credentials="userpropname:username;pwdpropname:password;..."]
      [-input_file="parameter_tag:file_path"]
      [-display_name="display_name"]
      [-groups="groupname1:grouptype1;groupname2:grouptype2;..."]
      [-timezone_region="gmt_offset"]
      [-monitor_mode="monitor_mode"]
      [-instances="rac_database_instance_target_name1:target_type1;..."]
      [-force]
      [-timeout="time_in_seconds"]

[ ] indicates that the parameter is optional
```

For more information, access the following URL:

http://docs.oracle.com/cd/E24628_01/em.121/e17786/cli_verb_ref.htm#CACHFHCA

2.2.4.2 Retrieving Deleted Host and Corresponding Management Agent Targets

If you have deleted a host target and the corresponding Management Agent target, you can retrieve both of them. To do so, follow these steps:

Discover and add the host and the Management Agent by running the following command from the agent instance home of the corresponding host:

```
$ emctl config agent addInternalTargets
```

Once the host and the Management Agent are discovered and added to the console, add each target on that host as targets to be monitored in the console, by running the following EM CLI verb:

```
$ emcli add_target
      -name="name"
      -type="type"
      -host="hostname"
      [-properties="pname1:pval1;pname2:pval2;..."]
      [-separator=properties="sep_string"]
      [-subseparator=properties="subsep_string"]
      [-credentials="userpropname:username;pwdpropname:password;..."]
      [-input_file="parameter_tag:file_path"]
      [-display_name="display_name"]
      [-groups="groupname1:grouptype1;groupname2:grouptype2;..."]
      [-timezone_region="gmt_offset"]
      [-monitor_mode="monitor_mode"]
      [-instances="rac_database_instance_target_name1:target_type1;..."]
      [-force]
      [-timeout="time_in_seconds"]

[ ] indicates that the parameter is optional
```

For more information, access the following URL:

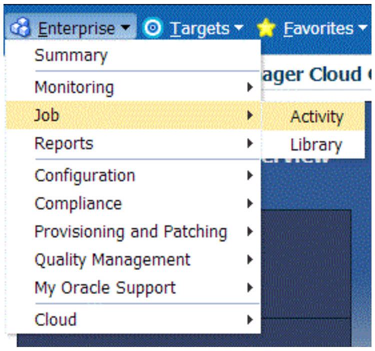
http://docs.oracle.com/cd/E24628_01/em.121/e17786/cli_verb_ref.htm#CACHFHCA

2.3 Discovering and Promoting Oracle Homes

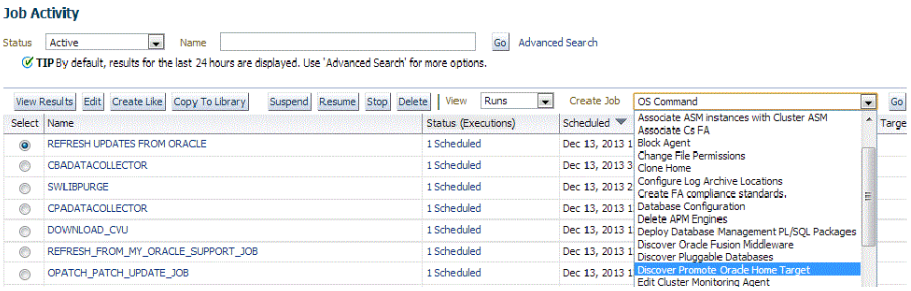
When you deploy an Oracle software component outside of the deployment procedures provided by Enterprise Manager, the Oracle home is not automatically discovered and promoted as targets. You will have to manually discover and promote the Oracle home target.

To discover and promote an Oracle home target, follow these steps:

1. From the **Enterprise** menu, select **Job,** and then select **Activity.**



2. On the Job Activity page, from the drop-down list in the table, select **Discover Promote Oracle Home Target.**


Job Activity

Status: Active — Name: — Go — Advanced Search

✓ TIP By default, results for the last 24 hours are displayed. Use 'Advanced Search' for more options.

View: Runs — Create Job: OS Command — Go

Select	Name	Status (Executions)	Scheduled
●	REFRESH UPDATES FROM ORACLE	1 Scheduled	Dec 13, 2013 1
○	CBADATACOLLECTOR	1 Scheduled	Dec 13, 2013 3
○	SWLIBPURGE	1 Scheduled	Dec 13, 2013 2
○	CPADATACOLLECTOR	1 Scheduled	Dec 13, 2013 1
○	DOWNLOAD_CVU	1 Scheduled	Dec 13, 2013 1
○	REFRESH_FROM_MY_ORACLE_SUPPORT_JOB	1 Scheduled	Dec 13, 2013 1
○	OPATCH_PATCH_UPDATE_JOB	1 Scheduled	Dec 13, 2013 1

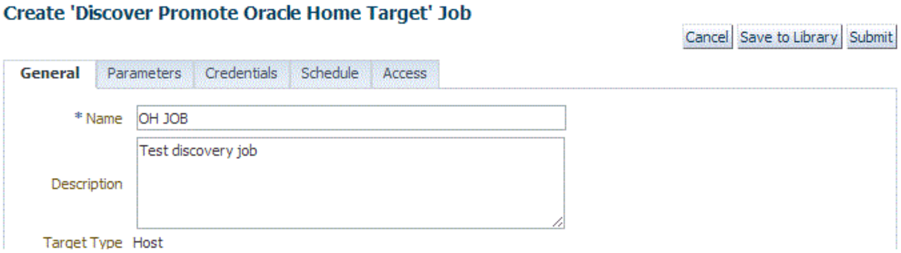
View Results
Edit
Create Like
Copy To Library
Suspend
Resume
Stop
Delete
Associate ASM instances with Cluster ASM
Associate Cs FA
Block Agent
Change File Permissions
Clone Home
Configure Log Archive Locations
Create FA compliance standards.
Database Configuration
Delete APM Engines
Deploy Database Management PL/SQL Packages
Discover Oracle Fusion Middleware
Discover Pluggable Databases
Discover Promote Oracle Home Target
Edit Cluster Monitoring Agent
Targe

Click **Go.**

3. On the 'Create Discover Promote Oracle Home Target' Job page, in the General tab, specify the name of the discovery.

   For example: `OHDiscovery`

   You can optionally add a description for the discovery.


Create 'Discover Promote Oracle Home Target' Job

* Name: OH JOB

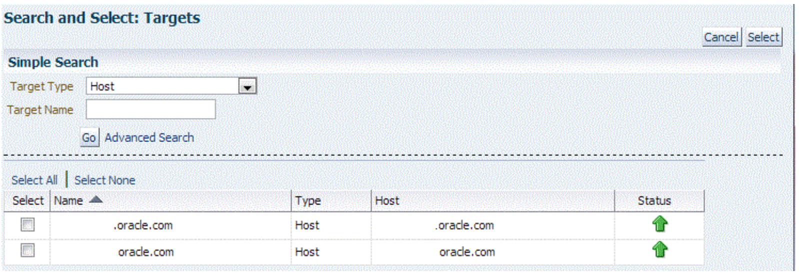
Description: Test discovery job

Target Type: Host

Click **Add.**

4. In the Search and Select: Target dialog box, select Target Type as **Host**, and then select all the host targets listed by clicking **Select All.**

   Click **Select.**



Search and Select: Targets

Cancel | Select

Simple Search

Target Type: Host

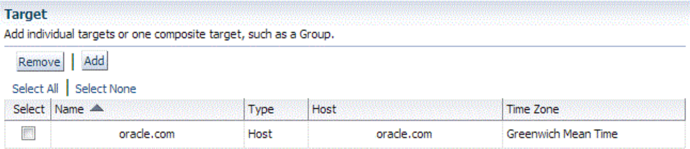
Target Name:

Go | Advanced Search

Select All | Select None

Select	Name ▲	Type	Host	Status
□	.oracle.com	Host	.oracle.com	⇧
□	oracle.com	Host	oracle.com	⇧

5. On the'Create Discover Promote Oracle Home Target' Job page, the host targets that you selected are displayed in the table.



Target

Add individual targets or one composite target, such as a Group.

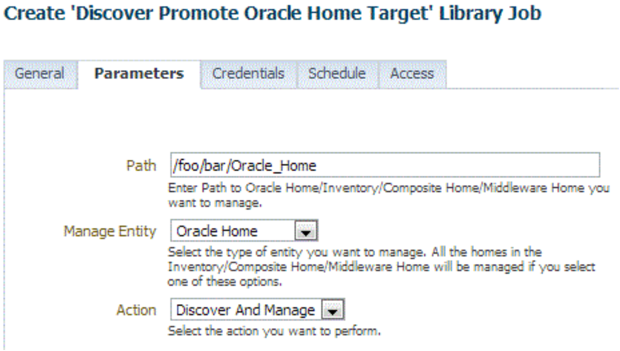
Remove | Add

Select All | Select None

Select	Name ▲	Type	Host	Time Zone
□	oracle.com	Host	oracle.com	Greenwich Mean Time

6. Select the Parameters tab, and then do one of the following:

   - To discover a single Oracle Home, specify the path to the home, and then select **Oracle Home** as the manage entity.



Create 'Discover Promote Oracle Home Target' Library Job

Path: /foo/bar/Oracle_Home

Enter Path to Oracle Home/Inventory/Composite Home/Middleware Home you want to manage.

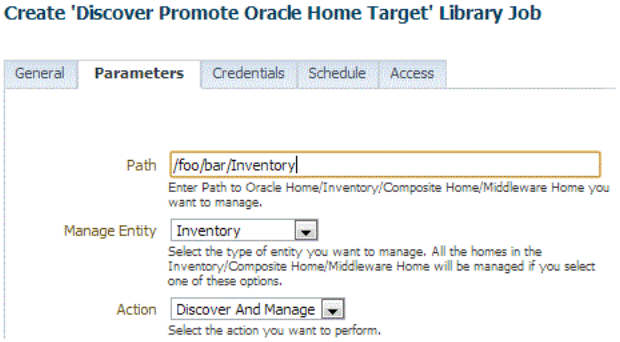
Manage Entity: Oracle Home

Select the type of entity you want to manage. All the homes in the Inventory/Composite Home/Middleware Home will be managed if you select one of these options.

Action: Discover And Manage

Select the action you want to perform.

   - To discover all Homes in an inventory, specify the path to the inventory, and then select **Inventory** as the manage entity.



Create 'Discover Promote Oracle Home Target' Library Job

Path: /foo/bar/Inventory

Enter Path to Oracle Home/Inventory/Composite Home/Middleware Home you want to manage.

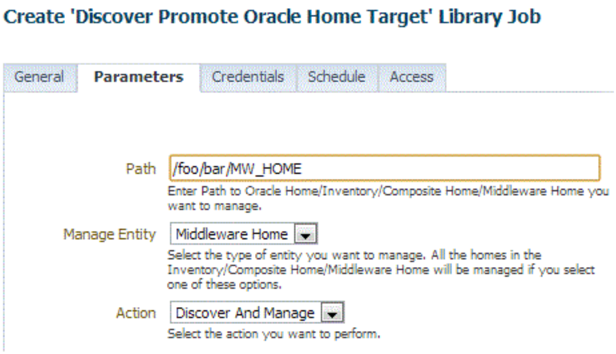
Manage Entity: Inventory

Select the type of entity you want to manage. All the homes in the Inventory/Composite Home/Middleware Home will be managed if you select one of these options.

Action: Discover And Manage

Select the action you want to perform.

   - To discover all Homes in a Middleware Home, specify the path to the Middleware Home and select **Middleware Home** as the manage entity.



Create 'Discover Promote Oracle Home Target' Library Job

Path /foo/bar/MW_HOME
Enter Path to Oracle Home/Inventory/Composite Home/Middleware Home you want to manage.

Manage Entity Middleware Home
Select the type of entity you want to manage. All the homes in the Inventory/Composite Home/Middleware Home will be managed if you select one of these options.

Action Discover And Manage
Select the action you want to perform.

7. To save the job for later, click **Save to Library.** To submit it, click **Submit.** When the discovery is successful, a confirmation is displayed on the Job Activity page.

Note: If you submit the discovery job without specifying a path, a discovery of the whole host will be performed. In order for a Home to be discoverable by the Management Agent, it needs to be registered in an inventory that the Management Agent recognizes. The default inventory is the central inventory, which in Unix systems is found in `/etc/oraInst.loc`. Any Home registered here will automatically be discovered.

If there are other inventories in the host, they need to be added to the inventory list of the Management Agent. A line must be added to `$EMSTATE/sysman/config/OUIinventories.add`.

If the inventory is not found here, the Management Agent will not know of its existence, and hence any Home registered there will not be discovered.

2.4 Discovering, Promoting, and Adding Database Targets

This section describes how you can discover, promote, and add database targets to be managed by Cloud Control. In particular, this section covers the following:

- Discovering Container Database and Pluggable Database Targets
- Discovering Cluster Database Targets
- Discovering Single Instance Database Targets
- Discovering Cluster Targets
- Discovering Single Instance High Availability Service Targets
- Discovering Cluster Automatic Storage Management Targets
- Enabling Autodiscovery of Database Targets

2.4.1 Discovering Container Database and Pluggable Database Targets

This section describes the different methods in which you can discover, promote, and add container database (CDB) and pluggable database (PDB) targets in Cloud Control. In particular, this section covers the following:

- Discovering and Promoting CDB and PDB Targets Using Autodiscovery
- Discovering and Adding CDB and PDB Targets Using the Guided Discovery Process

- Discovering and Adding CDB and PDB Targets By Specifying Target Monitoring Properties

2.4.1.1 Discovering and Promoting CDB and PDB Targets Using Autodiscovery

To discover and promote a CDB target and its associated PDB targets using automatic discovery, follow these steps:

> **Note:** By default, promoting a CDB target also promotes all its associated discovered PDB targets. Also, by default, Enterprise Manager runs a background job (every 24 hours) to automatically discover and promote newly created PDB targets present on managed hosts. Hence, to discover and promote PDB targets, you only need to discover and promote the associated CDB target, as described in this section.

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Discovering CDB and PDB Targets on the Managed Hosts
- Step 4: Promoting CDB and PDB Targets to Managed Status

2.4.1.1.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.1.2.1.

2.4.1.1.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.1.2.2.

2.4.1.1.3 Step 3: Discovering CDB and PDB Targets on the Managed Hosts

Discover the CDB targets on the managed hosts, as described in Section 2.2.1.2.3.

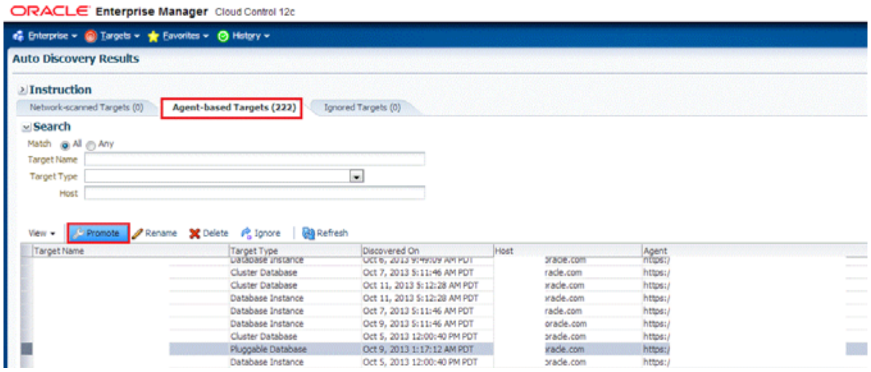
> **Note:** Autodiscovery of databases is enabled by default and this step is only required if it was disabled previously.

2.4.1.1.4 Step 4: Promoting CDB and PDB Targets to Managed Status

To promote CDB and PDB targets, follow these steps:

1. From the **Setup** menu, select **Add Target,** then select **Auto discovery Results.** Click **Agent-based Targets.**

2. Search for and select the Database Instance target that you want to promote, then click **Promote.**

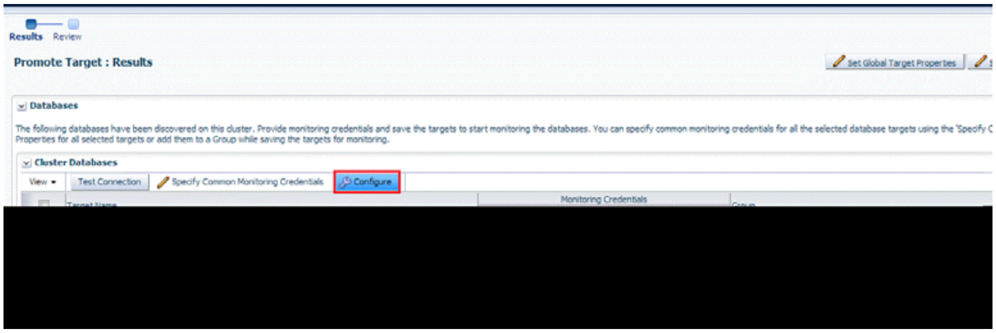


ORACLE Enterprise Manager Cloud Control 12c
Enterprise ▾ Targets ▾ Favorites ▾ History ▾
Auto Discovery Results
Instruction
Network-scanned Targets (0)
Agent-based Targets (222)
Ignored Targets (0)
Search
Match ● All ○ Any
Target Name
Target Type
Host
View ▾
Promote
Rename
Delete
Ignore
Refresh

Target Name	Target Type	Discovered On	Host	Agent
	Database Instance	Oct 6, 2013 9:49:09 AM PDT	oracle.com	https:/
	Cluster Database	Oct 7, 2013 5:11:46 AM PDT	racle.com	https:/
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	racle.com	https:/
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	racle.com	https:/
	Database Instance	Oct 7, 2013 5:11:46 AM PDT	racle.com	https:/
	Database Instance	Oct 9, 2013 5:11:46 AM PDT	oracle.com	https:/
	Cluster Database	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https:/
	Pluggable Database	Oct 9, 2013 1:17:12 AM PDT	racle.com	https:/
	Database Instance	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https:/

3. On the Promote Target: Results page, under the Databases section, select the CDB target.

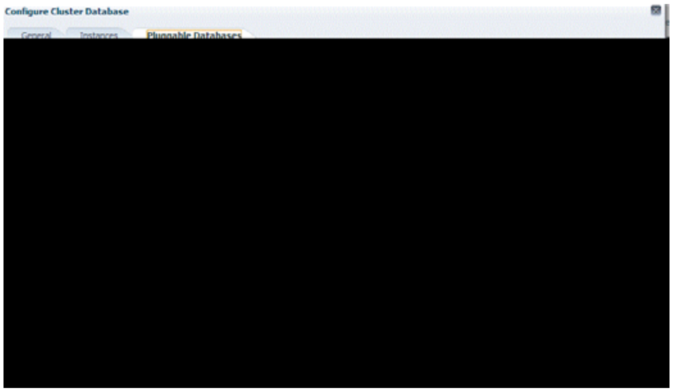
   By default, selecting a CDB target for promotion also selects all its associated discovered PDB targets for promotion. If you want to add or remove a PDB target from the ones selected for promotion, select the CDB target, then click **Configure.**



The following databases have been discovered on this cluster. Provide monitoring credentials and save the targets to start monitoring the databases. You can specify common monitoring credentials for all the selected database targets using the 'Specify C
Properties for all selected targets or add them to a Group while saving the targets for monitoring.

[redacted]

   Select the **Pluggable Databases** tab, then click **Add** or **Remove.** Click **Save.**



[redacted]

Enterprise Manager runs a background job (every 24 hours) to automatically discover and promote newly created PDB targets present on managed hosts. If you do not want Enterprise Manager to automatically promote the PDB targets associated with a particular CDB target, and instead want to promote them manually, select the CDB target on the Promote Target: Results page, then click **Configure.** Select the **Pluggable Databases** tab, then select Manual for **Pluggable Database Discovery Mode.** Click **Save.**

4. Specify the monitoring credentials for the selected CDB target, that is, the user name, password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

5. Click **Test Connection** to test the connection made to the CDB target using the specified monitoring credentials.

6. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

7. Click **Next.**

8. Review the displayed information, then click **Submit.**

2.4.1.2 Discovering and Adding CDB and PDB Targets Using the Guided Discovery Process

To discover and add a CDB target and its associated PDB targets using a guided discovery process, follow these steps:

> **Note:** By default, promoting a CDB target also promotes all its associated discovered PDB targets. Also, by default, Enterprise Manager runs a background job (every 24 hours) to automatically discover and promote newly created PDB targets present on managed hosts. Hence, to discover and promote PDB targets, you only need to discover and promote the associated CDB target, as described in this section.

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding CDB and PDB Targets

2.4.1.2.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.2.1.

2.4.1.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

---

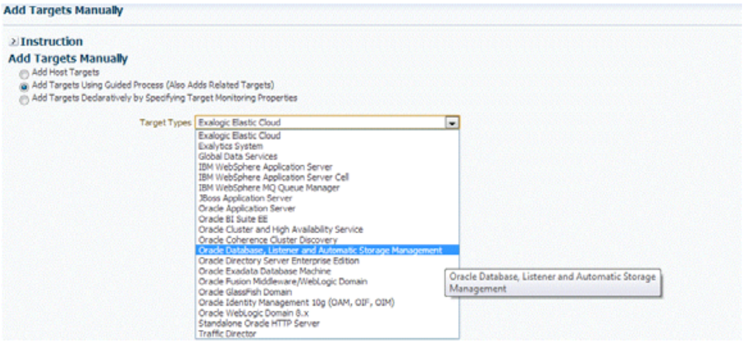
Note: Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

2.4.1.2.3 Step 3: Adding CDB and PDB Targets

To add CDB and PDB targets, follow these steps:

1. From the **Setup** menu, select **Add Target,** then select **Add Targets Manually.**
2. Select **Add Targets Using Guided Process (Also Adds Related Targets).** For **Target Types,** select **Oracle Database, Listener, and Automatic Storage Management.** Click **Add Using Guided Process.**



Add Targets Manually

Instruction

Add Targets Manually

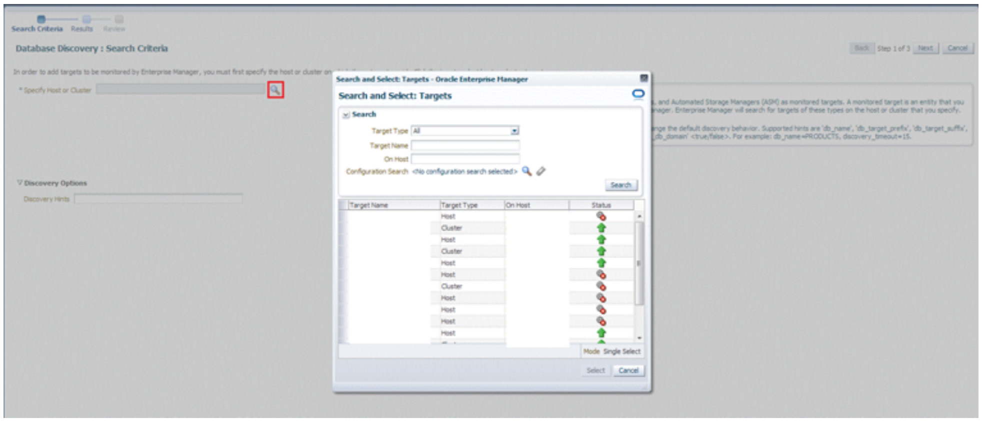
○ Add Host Targets
● Add Targets Using Guided Process (Also Adds Related Targets)
○ Add Targets Declaratively by Specifying Target Monitoring Properties

Target Types: Exalogic Elastic Cloud

- Exalogic Elastic Cloud
- Exalytics System
- Global Data Services
- IBM WebSphere Application Server
- IBM WebSphere Application Server Cell
- IBM WebSphere MQ Queue Manager
- JBoss Application Server
- Oracle Application Server
- Oracle BI Suite EE
- Oracle Cluster and High Availability Service
- Oracle Coherence Cluster Discovery
- Oracle Database, Listener and Automatic Storage Management
- Oracle Directory Server Enterprise Edition
- Oracle Exadata Database Machine
- Oracle Fusion Middleware/WebLogic Domain
- Oracle GlassFish Domain
- Oracle Identity Management 10g (OAM, OIF, OIM)
- Oracle WebLogic Domain 8.x
- Standalone Oracle HTTP Server
- Traffic Director

Oracle Database, Listener and Automatic Storage Management

3. On the Database Discovery: Search Criteria page, for **Specify Host or Cluster,** specify the CDB host.



Database Discovery : Search Criteria

In order to add targets to be monitored by Enterprise Manager, you must first specify the host or cluster on

* Specify Host or Cluster

, and Automated Storage Managers (ASM) as monitored targets. A monitored target is an entity that you
nager. Enterprise Manager will search for targets of these types on the host or cluster that you specify.

nge the default discovery behavior. Supported hints are 'db_name', 'db_target_prefix', 'db_target_suffix',
_db_domain' <true/false>. For example: db_name=PRODUCTS, discovery_timeout=15.

Discovery Options

Discovery Hints

Search and Select: Targets - Oracle Enterprise Manager

Search and Select: Targets

Search

Target Type: All

Target Name

On Host

Configuration Search: <No configuration search selected>

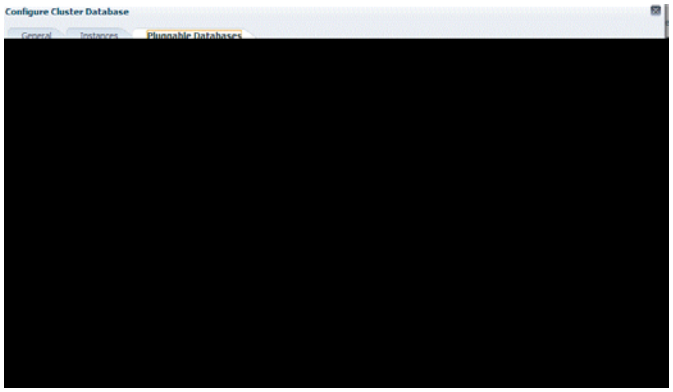
Target Name	Target Type	On Host	Status
	Host		⊘
	Cluster		⬆
	Host		⬆
	Cluster		⬆
	Host		⬆
	Host		⊘
	Cluster		⊘
	Host		⊘
	Host		⊘
	Host		⊘
	Host		⬆

Mode: Single Select

If the specified host belongs to a cluster, then you are prompted to choose if you want to discover and promote all the database targets present on only on the specified host, or all the database targets present on all the hosts that belong to the cluster.

4. Click **Next.**
5. On the Database Discovery: Results page, under the Databases section, select the CDB target.

   By default, selecting a CDB target for promotion also selects all its associated discovered PDB targets for promotion. If you want to add or remove a PDB target from the ones selected for promotion, select the CDB target, then click **Configure.** Select the **Pluggable Databases** tab, then click **Add** or **Remove.** Click **Save.**



   Enterprise Manager runs a background job (every 24 hours) to automatically discover and promote newly created PDB targets present on managed hosts. If you do not want Enterprise Manager to automatically promote the PDB targets associated with a particular CDB target, and instead want to promote them manually, select the CDB target on the Promote Target: Results page, then click **Configure.** Select the **Pluggable Databases** tab, then select Manual for **Pluggable Database Discovery Mode.** Click **Save.**

6. Specify the monitoring credentials for the selected CDB target, that is, the user name, password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

7. Click **Test Connection** to test the connection made to the CDB target using the specified monitoring credentials.
8. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

If you have selected multiple databases and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**

9. Click **Next.**

10. Review the displayed information, then click **Submit.**

2.4.1.3 Discovering and Adding CDB and PDB Targets By Specifying Target Monitoring Properties

To discover and add a CDB target and its associated PDB targets by specifying target monitoring properties, follow these steps:

> **Note:** By default, promoting a CDB target also promotes all its associated discovered PDB targets. Also, by default, Enterprise Manager runs a background job (every 24 hours) to automatically discover and promote newly created PDB targets present on managed hosts. Hence, to discover and promote PDB targets, you only need to discover and promote the associated CDB target, as described in this section.

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding CDB and PDB Targets

2.4.1.3.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.3.1.

2.4.1.3.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.3.2.

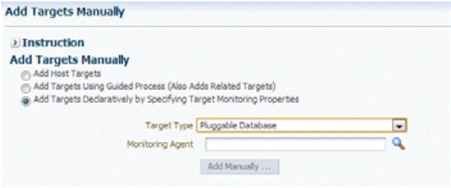
2.4.1.3.3 Step 3: Adding CDB and PDB Targets

To add a CDB or PDB target, follow these steps:

1. From the **Setup** menu, select **Add Target,** then select **Add Targets Manually.**

2. Select **Add Targets Declaratively by Specifying Target Monitoring Properties.** For **Target Type,** select **Pluggable Database.**

   For **Monitoring Agent,** specify the Management Agent present on the CDB host. Click **Add Manually.**



Add Targets Manually

Instruction

Add Targets Manually

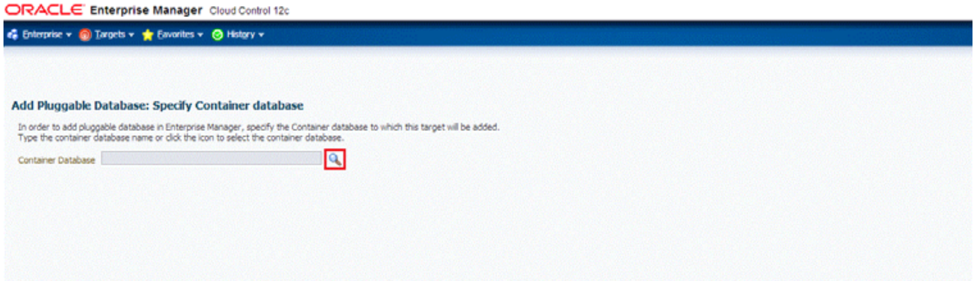
○ Add Host Targets
○ Add Targets Using Guided Process (Also Adds Related Targets)
● Add Targets Declaratively by Specifying Target Monitoring Properties

Target Type: Pluggable Database

Monitoring Agent:

3. On the Add Pluggable Database: Specify Container Database page, specify the CDB or click the search icon to select the CDB to which the target will be added.

   Click **Continue.**

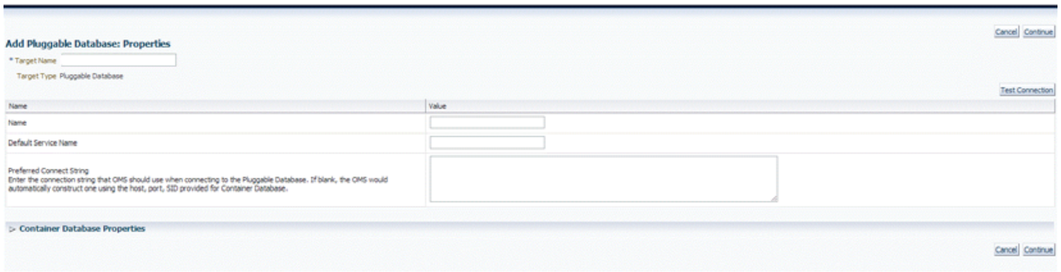


Add Pluggable Database: Specify Container database

In order to add pluggable database in Enterprise Manager, specify the Container database to which this target will be added. Type the container database name or click the icon to select the container database.

Container Database:

4. On the Add Pluggable Database: Properties page, specify a unique name for the target, the name, the default service name, and the preferred string connection.



Add Pluggable Database: Properties

* Target Name:

Target Type: Pluggable Database

Name	Value
Name	
Default Service Name	
Preferred Connect String Enter the connection string that OMS should use when connecting to the Pluggable Database. If blank, the OMS would automatically construct one using the host, port, SID provided for Container Database.	

Container Database Properties

   Expand the Container Database section to verify the properties of the CDB.

   Click **Test Connection** to test the connection made to the CDB target using the specified monitoring credentials.

   Click **Continue.**

5. Specify the required information on each page and then click **Next,** until you reach the Review page.
6. Review the displayed information, and then click **Submit.**

2.4.2 Discovering Cluster Database Targets

This section describes the different methods in which you can discover, promote, and add cluster database targets. In particular, this section cover the following:

- Discovering and Promoting Cluster Database Targets Using Autodiscovery
- Discovering and Adding Cluster Database Targets Using the Guided Discovery Process
- Discovering and Adding Cluster Database Targets By Specifying Target Monitoring Properties

2.4.2.1 Discovering and Promoting Cluster Database Targets Using Autodiscovery

To discover and promote cluster database targets using autodiscovery, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Promoting Cluster Database Targets to Managed Status

2.4.2.1.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover unmanaged hosts, as described Section 2.2.1.2.1.

2.4.2.1.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert discovered unmanaged hosts to managed hosts, as described Section 2.2.1.2.2.

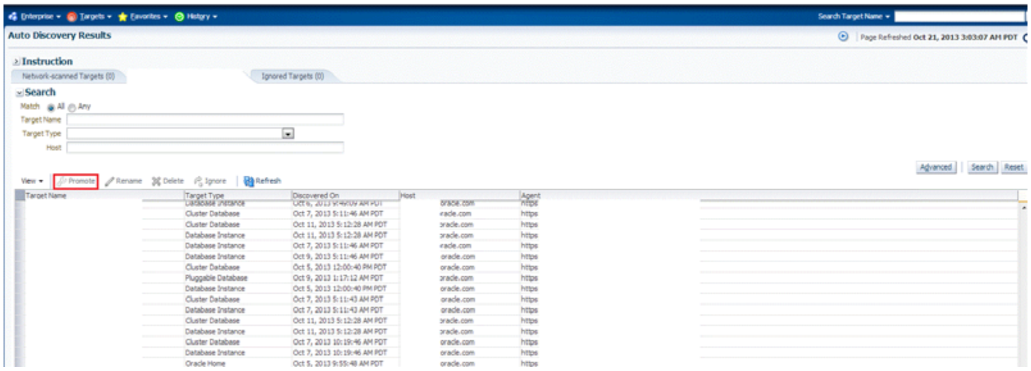
2.4.2.1.3 Step 3: Promoting Cluster Database Targets to Managed Status

To promote cluster database targets, follow these steps:

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

   > **Note:** If you do not see any results, then autodiscovery of targets has been disabled. To enable autodiscovery refer to Enabling Autodiscovery of Database Targets.

   From the results table, from the Agent-based targets tab, select the discovered cluster database target that you want to add for monitoring, and click **Promote.**



Auto Discovery Results

Search

Match ● All ○ Any

Target Name

Target Type

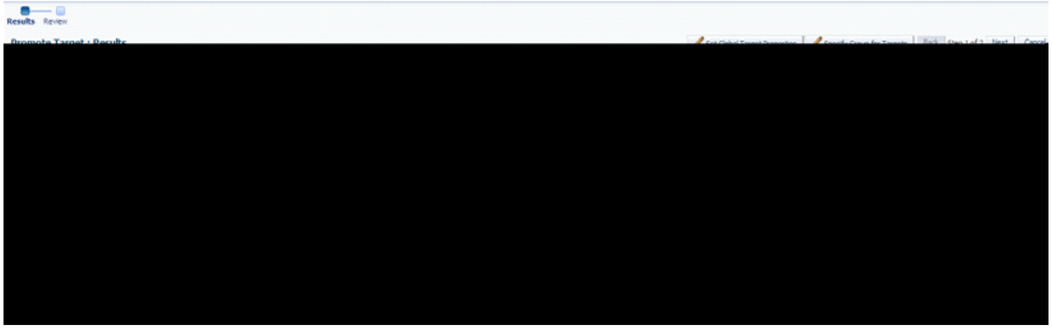
Host

Target Name	Target Type	Discovered On	Host	Agent
	Database Instance	Oct 6, 2013 9:49:09 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	racle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	racle.com	https
	Database Instance	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Database Instance	Oct 9, 2013 5:11:46 AM PDT	oracle.com	https
	Cluster Database	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Pluggable Database	Oct 9, 2013 1:17:12 AM PDT	racle.com	https
	Database Instance	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	racle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	racle.com	https
	Cluster Database	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Oracle Home	Oct 5, 2013 9:55:48 AM PDT	oracle.com	https

2. The Promote Targets:Result page displays the databases discovered on the cluster. Select the database

   On the Promote Target: Results page, under the Databases section, in the Cluster Databases section, select the cluster database target that you want to promote.

   By default, selecting the cluster database target for promotion also selects all its associated discovered database instance targets for promotion. If you want to add or remove a database instance target from the ones selected for promotion, select the cluster database target, then click **Configure.** Select the **Instances** tab, then click **Add** or **Remove.** Click **Save.**



[redacted]

3. In the Cluster Databases section, specify the monitoring credentials for the selected cluster database target, that is, the Monitor user name, Monitor password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

4. Click **Test Connection** to test the connection made to the cluster database target using the specified monitoring credentials.

5. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

6. If you have selected multiple databases and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**
7. Click **Next.**
8. Review the displayed information, then click **Submit.**

2.4.2.2 Discovering and Adding Cluster Database Targets Using the Guided Discovery Process

To discover and add cluster database targets using the guided process, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Cluster Database Targets

2.4.2.2.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.2.1.

2.4.2.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

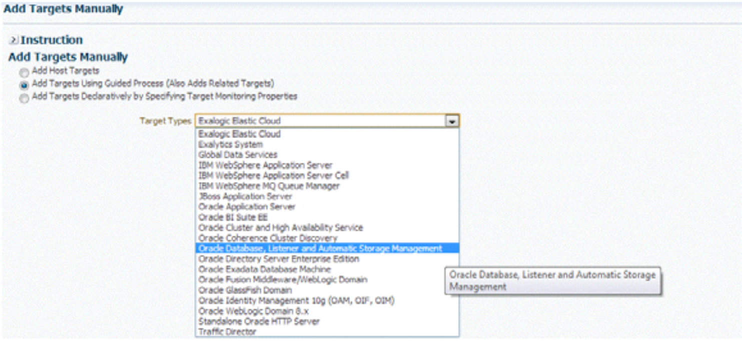
> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

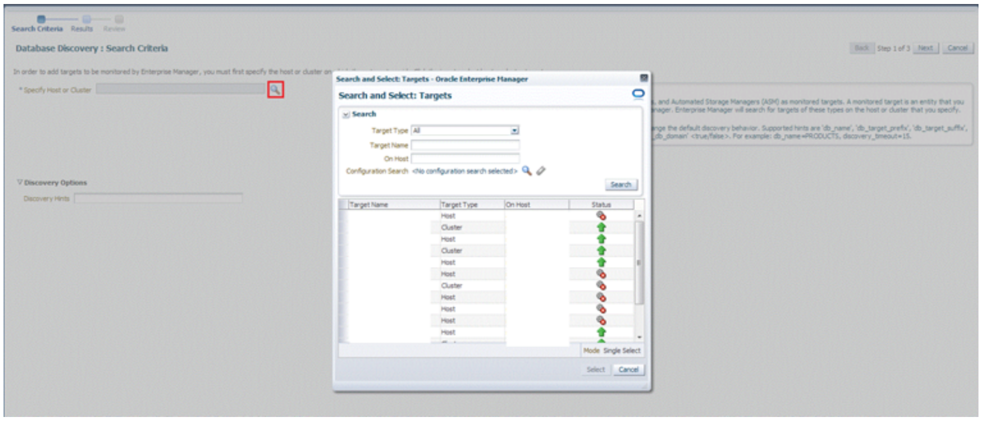
2.4.2.2.3 Step 3: Adding Cluster Database Targets

To add a cluster database target, follow these steps:

1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Add Manually page, select **Add Targets Using Guided Process (Also Adds Related Targets).**
3. From the Target Types list, select **Oracle Database, Listener, and Automatic Storage Management.**
4. Click **Add Using Guided Process.**


Add Targets Manually
Instruction
Add Targets Manually
○ Add Host Targets
● Add Targets Using Guided Process (Also Adds Related Targets)
○ Add Targets Declaratively by Specifying Target Monitoring Properties
Target Types Exalogic Elastic Cloud
Exalogic Elastic Cloud
Exalytics System
Global Data Services
IBM WebSphere Application Server
IBM WebSphere Application Server Cell
IBM WebSphere MQ Queue Manager
JBoss Application Server
Oracle Application Server
Oracle BI Suite EE
Oracle Cluster and High Availability Service
Oracle Coherence Cluster Discovery
Oracle Database, Listener and Automatic Storage Management
Oracle Directory Server Enterprise Edition
Oracle Exadata Database Machine
Oracle Fusion Middleware/WebLogic Domain
Oracle GlassFish Domain
Oracle Identity Management 10g (OAM, OIF, OIM)
Oracle WebLogic Domain 8.x
Standalone Oracle HTTP Server
Traffic Director
Oracle Database, Listener and Automatic Storage Management

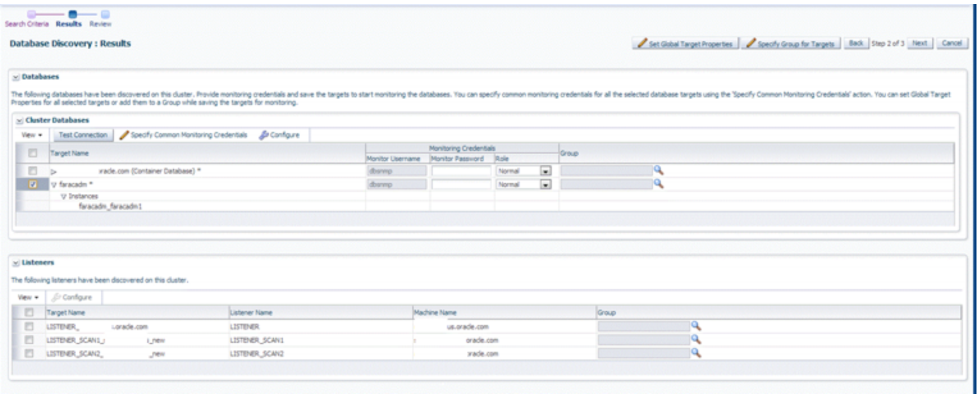
5. On the Database Discovery: Search Criteria page, specify the cluster database host, or click on the **Specify Host or Cluster** search icon to select the cluster.



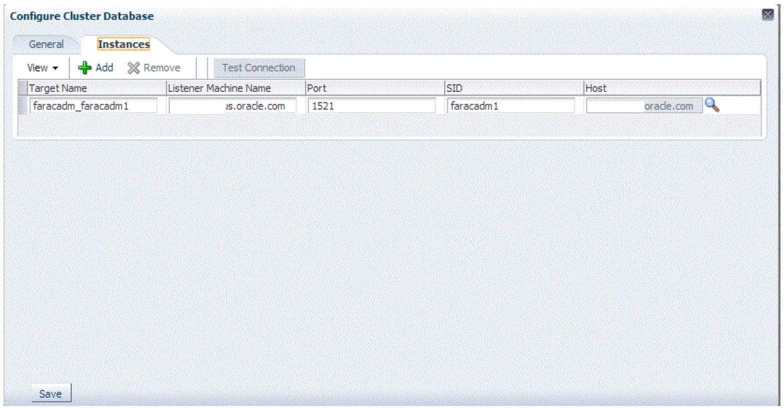
If the specified host belongs to a cluster, then you are prompted to choose if you want to discover and promote all the database targets present on only on the specified host, or all the database targets present on all the hosts that belong to the cluster.

Click **Next.**

6. On the Database Discovery: Results page, under the Databases section, in the Cluster Databases section, select the cluster database target that you want to add.


Search Criteria
Results
Review
Database Discovery : Results
Set Global Target Properties
Specify Group for Targets
Back
Step 2 of 3
Next
Cancel
Databases
The following databases have been discovered on this cluster. Provide monitoring credentials and save the targets to start monitoring the databases. You can specify common monitoring credentials for all the selected database targets using the 'Specify Common Monitoring Credentials' action. You can set Global Target Properties for all selected targets or add them to a Group while saving the targets for monitoring.
Cluster Databases
View
Test Connection
Specify Common Monitoring Credentials
Configure
Target Name
Monitoring Credentials
Monitor Username
Monitor Password
Role
Group
oracle.com (Container Database) *
faracadm *
Instances
faracadm_faracadm1
dbsnmp
Normal
Listeners
The following listeners have been discovered on this cluster.
View
Configure
Target Name
Listener Name
Machine Name
Group
LISTENER_
oracle.com
LISTENER
us.oracle.com
LISTENER_SCAN1_
_new
LISTENER_SCAN1
oracle.com
LISTENER_SCAN2_
_new
LISTENER_SCAN2
oracle.com

By default, selecting a cluster database target for promotion also selects all its associated discovered database instance targets for promotion. If you want to add or remove a database instance target from the ones selected for promotion, select the cluster database target, then click **Configure.** Select the **Instances** tab, then click **Add** or **Remove.** Click **Save.**



Target Name	Listener Machine Name	Port	SID	Host
faracadm_faracadm1	ıs.oracle.com	1521	faracadm1	oracle.com

7. Specify the monitoring credentials for the selected cluster database target, that is, the user name, password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

8. Click **Test Connection** to test the connection made to the cluster database target using the specified monitoring credentials.

9. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

   If you have selected multiple databases and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**

10. Click **Next.**

11. Review the displayed information, then click **Submit.**

2.4.2.3 Discovering and Adding Cluster Database Targets By Specifying Target Monitoring Properties

To discover and add a cluster database target declaratively by specifying target monitoring properties, follow these steps:

- Step 1: Discovering Unmanaged Hosts

- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Cluster Database Targets

2.4.2.3.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.3.1.

2.4.2.3.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

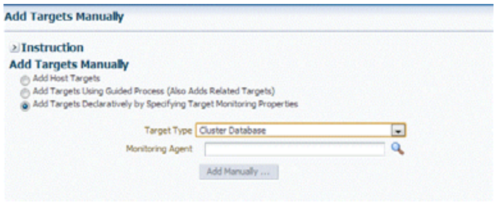
> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.3.2.

2.4.2.3.3 Step 3: Adding Cluster Database Targets

To add a cluster database target, follow these steps:

1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Add Manually page, select **Add Targets Declaratively by Specifying Target Monitoring Properties.**
3. From the Target Type list, select **Cluster Database.**
4. In the Monitoring Agent field, select the Management Agent monitoring the database.
5. Click **Add Manually.**



Add Targets Manually

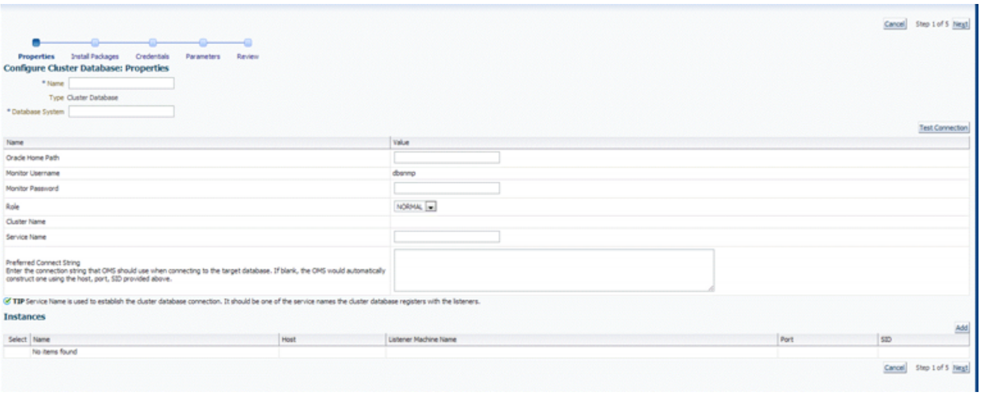
› Instruction

Add Targets Manually

○ Add Host Targets
○ Add Targets Using Guided Process (Also Adds Related Targets)
● Add Targets Declaratively by Specifying Target Monitoring Properties

Target Type: Cluster Database
Monitoring Agent:

6. On the Configure Cluster Database: Properties, specify a name and a database system name for the cluster database target. Next, specify all the properties of the target, that is, Oracle Home path, monitoring username and password, role, Listener machine name, port, database SID, and preferred connect string.



Configure Cluster Database: Properties

* Name	
Type	Cluster Database
* Database System	

Name	Value
Oracle Home Path	
Monitor Username	dbsnmp
Monitor Password	
Role	NORMAL
Cluster Name	
Service Name	
Preferred Connect String Enter the connection string that OMS should use when connecting to the target database. If blank, the OMS would automatically construct one using the host, port, SID provided above.	

TIP Service Name is used to establish the cluster database connection. It should be one of the service names the cluster database registers with the listeners.

Instances

Select	Name	Host	Listener Machine Name	Port	SID
	No items found				

Click **Next.**

7. Specify all the details required on the Install Packages, Credentials, and Parameters pages. Click **Next** after each page until you reach the Review page.

8. Review the displayed information, then click **Submit.**

2.4.3 Discovering Single Instance Database Targets

This section describes the different methods in which you can discover, promote, and add single instance database targets. In particular, this section covers the following:

- Discovering and Promoting Single Instance Database Targets Using Autodiscovery
- Discovering and Adding Single Instance Database Targets Using Guided Discovery Process
- Discovering and Adding Single Instance Database Targets By Specifying Target Monitoring Properties

2.4.3.1 Discovering and Promoting Single Instance Database Targets Using Autodiscovery

To discover and promote single instance database targets using Auto Discovery, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Promoting Single Instance Database Targets to Managed Status

2.4.3.1.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described to Section 2.2.1.2.1.

2.4.3.1.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

---

Note: Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.1.2.2.

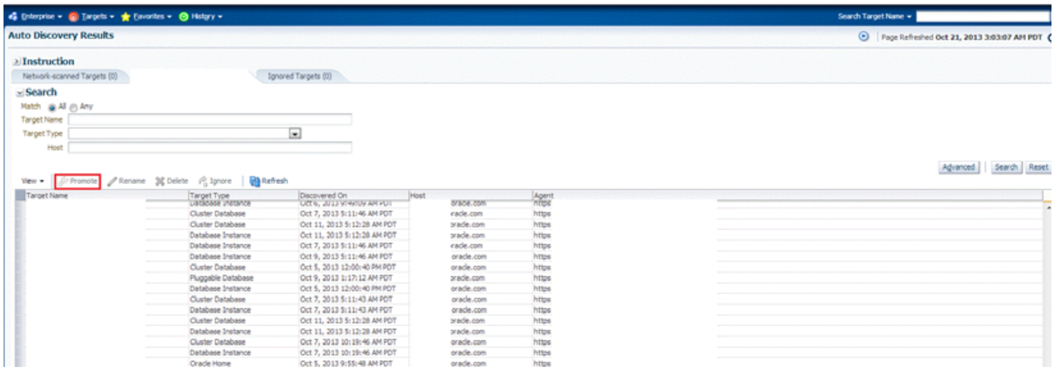
2.4.3.1.3 Step 3: Promoting Single Instance Database Targets to Managed Status

To promote single instance database targets, follow these steps:

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

   Note: If you do not see any results, then autodiscovery of targets has been disabled. To enable autodiscovery refer to Enabling Autodiscovery of Database Targets.

   From the results table, from the Agent-based targets tab, select the discovered database instance target that you want to add for monitoring, and click **Promote.**



Auto Discovery Results

Page Refreshed **Oct 21, 2013 3:03:07 AM PDT**

Search

Match ● All ○ Any

Target Name

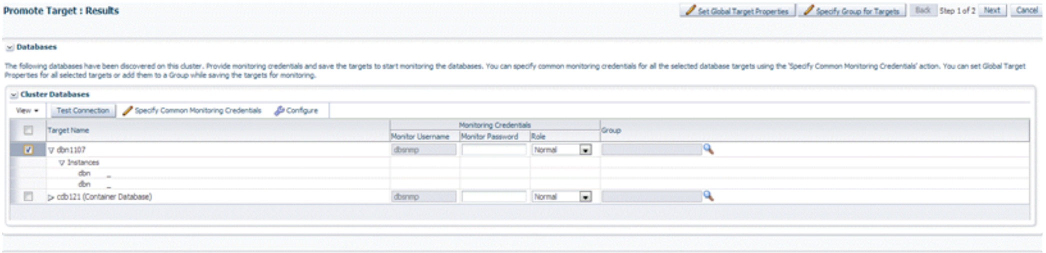
Target Type

Host

Target Name	Target Type	Discovered On	Host	Agent
	Database Instance	Oct 6, 2013 9:49:09 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Database Instance	Oct 9, 2013 5:11:46 AM PDT	oracle.com	https
	Cluster Database	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Pluggable Database	Oct 9, 2013 1:17:12 AM PDT	oracle.com	https
	Database Instance	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Oracle Home	Oct 5, 2013 9:55:48 AM PDT	oracle.com	https

2. The Promote Targets:Result page displays the databases Select the database instance.

   On the Promote Target: Results page, under the Databases section, in the Single Instance Databases section, select the database instance target that you want to promote.


Set Global Target Properties
Specify Group for Targets
Back
Next
Cancel
View ▾
Test Connection
Specify Common Monitoring Credentials
Configure

Promote Target : Results

Step 1 of 2

Databases

The following databases have been discovered on this cluster. Provide monitoring credentials and save the targets to start monitoring the databases. You can specify common monitoring credentials for all the selected database targets using the 'Specify Common Monitoring Credentials' action. You can set Global Target Properties for all selected targets or add them to a Group while saving the targets for monitoring.

Cluster Databases

□	Target Name	Monitoring Credentials			Group
		Monitor Username	Monitor Password	Role	
☑	▽ dbn1107	dbsnmp		Normal	
	▽ Instances				
	dbn_				
	dbn_				
□	▷ cdb121 (Container Database)	dbsnmp		Normal	

3. Specify the monitoring credentials for the selected database instance target, that is, the Monitor user name, Monitor password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

4. Click **Test Connection** to test the connection made to the database instance target using the specified monitoring credentials.

5. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

6. If you have selected multiple databases and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**

7. Click **Next.**

8. Review the displayed information, then click **Submit.**

2.4.3.2 Discovering and Adding Single Instance Database Targets Using Guided Discovery Process

To discover and add single instance database targets using the guided process, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Single Instance Database Targets

2.4.3.2.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.2.1.

2.4.3.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

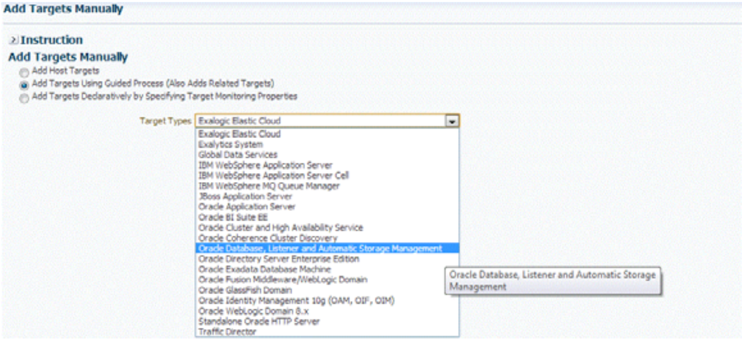
> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

2.4.3.2.3 Step 3: Adding Single Instance Database Targets

To add single instance database targets, follow these steps:

1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Add Manually page, select **Add Targets Using Guided Process (Also Adds Related Targets).**
3. From the Target Types list, select **Oracle Database, Listener, and Automatic Storage Management.**
4. Click **Add Using Guided Process.**



Add Targets Manually

Instruction

Add Targets Manually

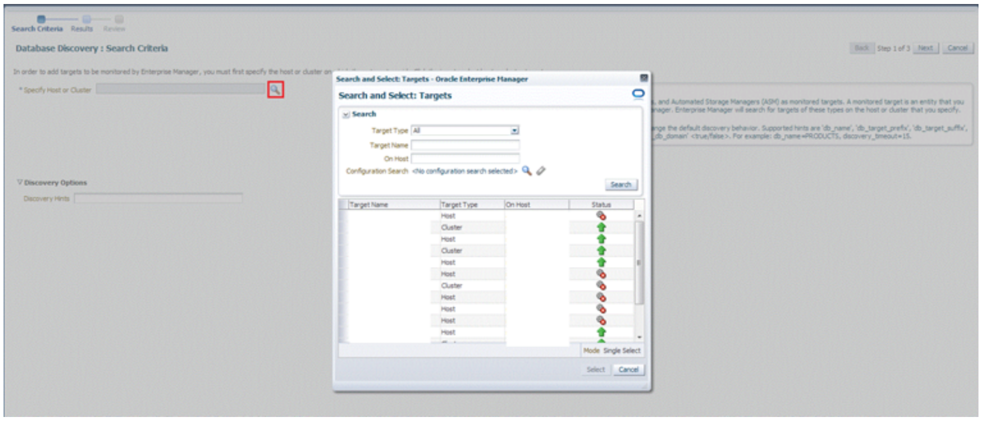
○ Add Host Targets
● Add Targets Using Guided Process (Also Adds Related Targets)
○ Add Targets Declaratively by Specifying Target Monitoring Properties

Target Types: Exalogic Elastic Cloud

- Exalogic Elastic Cloud
- Exalytics System
- Global Data Services
- IBM WebSphere Application Server
- IBM WebSphere Application Server Cell
- IBM WebSphere MQ Queue Manager
- JBoss Application Server
- Oracle Application Server
- Oracle BI Suite EE
- Oracle Cluster and High Availability Service
- Oracle Coherence Cluster Discovery
- Oracle Database, Listener and Automatic Storage Management
- Oracle Directory Server Enterprise Edition
- Oracle Exadata Database Machine
- Oracle Fusion Middleware/WebLogic Domain
- Oracle GlassFish Domain
- Oracle Identity Management 10g (OAM, OIF, OIM)
- Oracle WebLogic Domain 8.x
- Standalone Oracle HTTP Server
- Traffic Director

Oracle Database, Listener and Automatic Storage Management

5. On the Database Discovery: Search Criteria page, specify the database instance host, or click on the **Specify Host or Cluster** search icon to select the host.



Database Discovery : Search Criteria

In order to add targets to be monitored by Enterprise Manager, you must first specify the host or cluster on

* Specify Host or Cluster

, and Automated Storage Managers (ASM) as monitored targets. A monitored target is an entity that you nager. Enterprise Manager will search for targets of these types on the host or cluster that you specify.

nge the default discovery behavior. Supported hints are 'db_name', 'db_target_prefix', 'db_target_suffix', db_domain' <true/false>. For example: db_name=PRODUCTS, discovery_timeout=15.

Discovery Options

Discovery Hints

Search and Select: Targets - Oracle Enterprise Manager

Search and Select: Targets

Search

Target Type: All

Target Name:

On Host:

Configuration Search: <No configuration search selected>

Target Name	Target Type	On Host	Status
	Host		⊘
	Cluster		↑
	Host		↑
	Cluster		↑
	Host		↑
	Host		⊘
	Cluster		⊘
	Host		⊘
	Host		⊘
	Host		⊘
	Host		↑

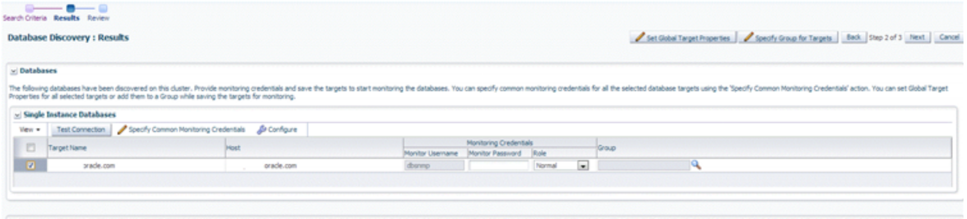
Mode: Single Select

If the specified host belongs to a cluster, then you are prompted to choose if you want to discover and promote all the database targets present on only on the specified host, or all the database targets present on all the hosts that belong to the cluster.

Click **Next.**

6. The Database Discovery:Result page displays the databases discovered on the cluster. Select the database

   On the Database Discovery: Results page, under the Databases section, in the Single Instance Databases section, select the database instance target that you want to promote.


Search Criteria
Results
Review
Set Global Target Properties
Specify Group for Targets
Back
Step 2 of 3
Next
Cancel
View ▾
Test Connection
Specify Common Monitoring Credentials
Configure

Database Discovery : Results

Databases

The following databases have been discovered on this cluster. Provide monitoring credentials and save the targets to start monitoring the databases. You can specify common monitoring credentials for all the selected database targets using the 'Specify Common Monitoring Credentials' action. You can set Global Target Properties for all selected targets or add them to a Group while saving the targets for monitoring.

Single Instance Databases

			Monitoring Credentials			
□	Target Name	Host	Monitor Username	Monitor Password	Role	Group
☑	oracle.com	oracle.com	dbsnmp		Normal	

7. Specify the monitoring credentials for the selected database instance target, that is, the Monitor user name, Monitor password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

8. Click **Test Connection** to test the connection made to the database instance target using the specified monitoring credentials.

9. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

10. If you have selected multiple databases and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**

11. Click **Next.**

12. Review the displayed information, then click **Submit.**

2.4.3.3 Discovering and Adding Single Instance Database Targets By Specifying Target Monitoring Properties

To discover and add a single instance database target declaratively by specifying target monitoring properties, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Single Instance Database Targets

2.4.3.3.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.3.1.

2.4.3.3.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

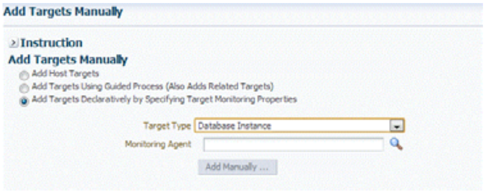
> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.3.2.

2.4.3.3.3 Step 3: Adding Single Instance Database Targets

To add single instance database targets, follow these steps:

1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Add Manually page, select **Add Targets Declaratively by Specifying Target Monitoring Properties.**
3. From the Target Type list, select **Database Instance.**
4. In the Monitoring Agent field, select the Management Agent monitoring the database.
5. Click **Add Manually.**



Add Targets Manually

Instruction

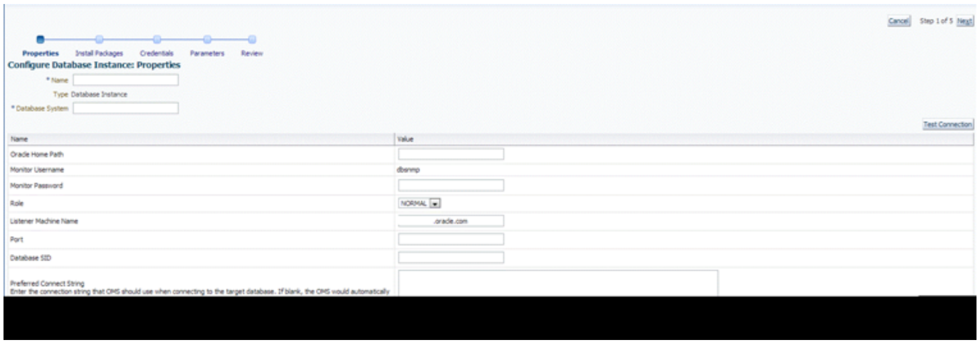
Add Targets Manually

○ Add Host Targets
○ Add Targets Using Guided Process (Also Adds Related Targets)
● Add Targets Declaratively by Specifying Target Monitoring Properties

Target Type: Database Instance

Monitoring Agent:

6. On the Configure Database Instance: Properties, specify a name and a database system name for the target, that is, Oracle Home path, monitoring username and password, role, Listener machine name, port, database SID, and preferred connect string.



Configure Database Instance: Properties

* Name:

Type: Database Instance

* Database System:

Name	Value
Oracle Home Path	
Monitor Username	dbsnmp
Monitor Password	
Role	NORMAL
Listener Machine Name	.oracle.com
Port	
Database SID	
Preferred Connect String Enter the connection string that OMS should use when connecting to the target database. If blank, the OMS would automatically	

Click **Next.**

7. Specify all the details required on the Install Packages, Credentials, and Parameters pages. Click **Next** after each page until you reach the Review page.
8. Review the displayed information, then click **Submit.**

2.4.4 Discovering Cluster Targets

This section describes the different methods in which you can discover, promote, add cluster targets. In particular, this section covers the following:

- Discovering and Promoting Cluster Targets Using Autodiscovery
- Discovering and Adding Cluster Targets Using the Guided Discovery Process
- Discovering and Adding Cluster Targets By Specifying Target Monitoring Properties

2.4.4.1 Discovering and Promoting Cluster Targets Using Autodiscovery

To automatically discover and promote cluster targets using Auto Discovery, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Promoting Cluster Targets to Managed Status

2.4.4.1.1 Step 1: Discovering Unmanaged Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.1.2.1.

2.4.4.1.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.1.2.2.

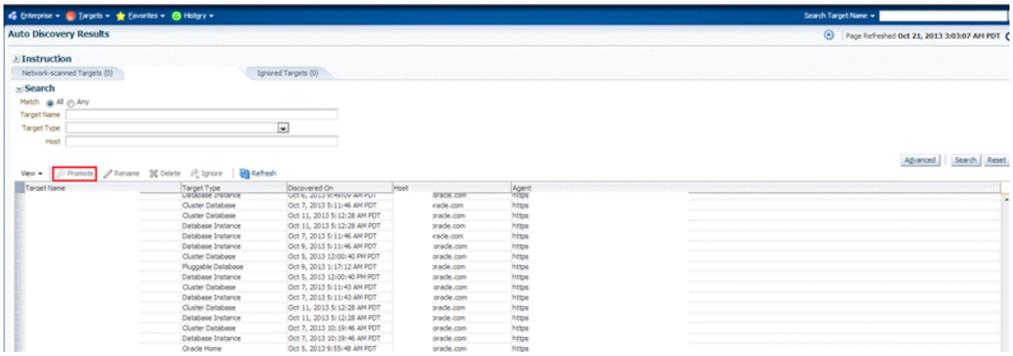
2.4.4.1.3 Step 3: Promoting Cluster Targets to Managed Status

To promote cluster targets, follow these steps:

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

   Note: If you do not see any results, then autodiscovery of targets has been disabled. To enable autodiscovery refer to Enabling Autodiscovery of Database Targets.

   From the results table, from the Agent-based targets tab, select the discovered cluster target that you want to add for monitoring, and click **Promote.**



Match ● All ○ Any

Target Name

Target Type

Host

Target Name	Target Type	Discovered On	Host	Agent
	Database Instance	Oct 6, 2013 9:49:09 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Database Instance	Oct 9, 2013 5:11:46 AM PDT	oracle.com	https
	Cluster Database	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Pluggable Database	Oct 9, 2013 1:17:12 AM PDT	oracle.com	https
	Database Instance	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Oracle Home	Oct 5, 2013 9:55:48 AM PDT	oracle.com	https

2. The Promote Targets:Result page displays the hosts discovered on the cluster. Select the host that you want to promote.

> **Note:** A host can belong to only one cluster. If a particular host is not displayed, it can mean that the host belongs to another cluster.

On the Promote Target: Results page, in the Clusters section, select the cluster target that you want to promote.

By default, selecting the cluster target for promotion also selects all its associated discovered hosts for promotion. If you want to add or remove a host from the ones selected for promotion, select the cluster database target, then click **Configure.** Select the **Hosts** tab, then click **Add** or **Remove.** Click **Save.**

3. In the Clusters section, specify the monitoring credentials for the selected cluster target, that is, the Monitor user name, Monitor password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

4. Click **Test Connection** to test the connection made to the cluster target using the specified monitoring credentials.

5. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

6. If you have selected multiple databases and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**

7. Click **Next.**

8. Review the displayed information, then click **Submit.**

2.4.4.2 Discovering and Adding Cluster Targets Using the Guided Discovery Process

To discover and add cluster targets using the guided process, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Cluster Targets

2.4.4.2.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.2.1.

2.4.4.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

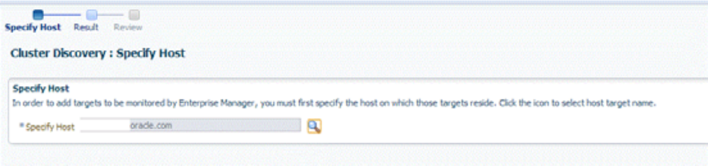
> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

2.4.4.2.3 Step 3: Adding Cluster Targets

To add cluster targets, follow these steps:

1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Add Manually page, select **Add Targets Using Guided Process (Also Adds Related Targets).**
3. From the Target Types list, select **Oracle Database, Listener, and Automatic Storage Management.**
4. Click **Add Using Guided Process.**
5. On the Cluster Discovery: Specify Host page, specify the cluster host, or click on the **Specify Host or Cluster** search icon to select the cluster.



Cluster Discovery : Specify Host

Specify Host

In order to add targets to be monitored by Enterprise Manager, you must first specify the host on which those targets reside. Click the icon to select host target name.

* Specify Host: oracle.com

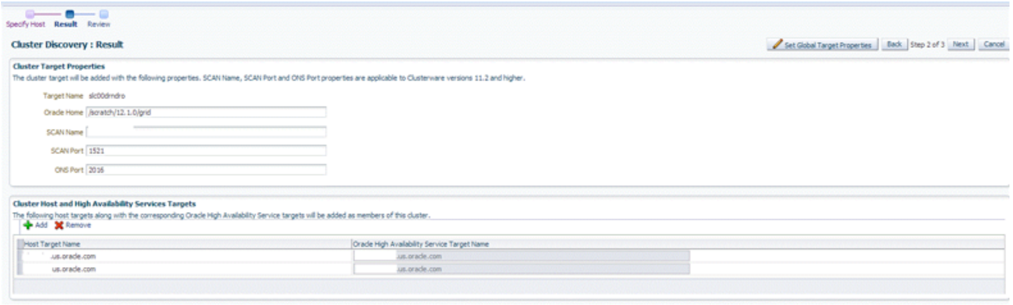
If the specified host belongs to a cluster, then you are prompted to choose if you want to discover and promote all the database targets present on only on the specified host, or all the database targets present on all the hosts that belong to the cluster.

Click **Next.**

6. The Cluster Discovery:Result page displays the hosts discovered on the cluster. Select the host that you want to add.

   > **Note:** A host can belong to only one cluster. If a particular host is not displayed, it can mean that the host belongs to another cluster.

   On the Cluster Discovery: Result page, in the Clusters Target Properties section, verify the properties of the cluster.



Cluster Discovery : Result

Cluster Target Properties

The cluster target will be added with the following properties. SCAN Name, SCAN Port and ONS Port properties are applicable to Clusterware versions 11.2 and higher.

Target Name slc00drndro

Oracle Home /scratch/12.1.0/grid

SCAN Name

SCAN Port 1521

ONS Port 2016

Cluster Host and High Availability Services Targets

The following host targets along with the corresponding Oracle High Availability Service targets will be added as members of this cluster.

Host Target Name	Oracle High Availability Service Target Name
.us.oracle.com	.us.oracle.com
us.oracle.com	.us.oracle.com

   If you want to add or remove a host, select a host from the Cluster Host and High Availability Service Targets section. Click **Add** or **Remove.**

7. Click **Next.**

8. Review the displayed information, then click **Submit.**

2.4.4.3 Discovering and Adding Cluster Targets By Specifying Target Monitoring Properties

To discover and add a cluster target declaratively by specifying target monitoring properties, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Cluster Targets

2.4.4.3.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.3.1.

2.4.4.3.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

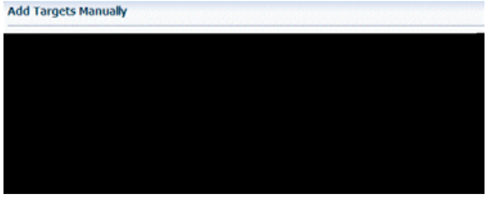
> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.3.2.

2.4.4.3.3 Step 3: Adding Cluster Targets

To add cluster targets, follow these steps:

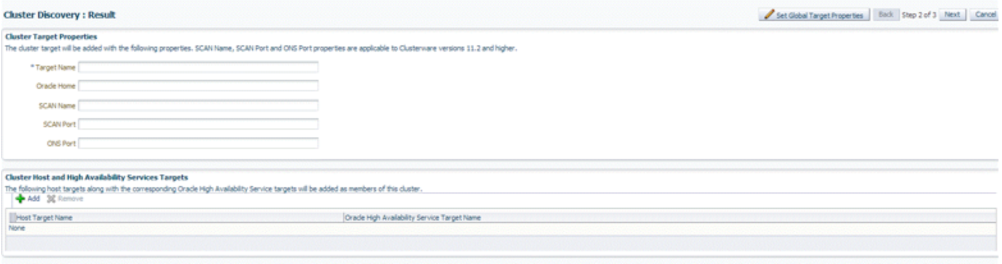
1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Add Manually page, select **Add Targets Declaratively by Specifying Target Monitoring Properties.**
3. From the Target Type list, select **Cluster.**
4. In the Monitoring Agent field, select the Management Agent monitoring the database.
5. Click **Add Manually.**



Add Targets Manually

[redacted]

6. On the Cluster Discovery:Result page, specify the target name, Oracle Home, SCAN name, SCAN port, and ONS port.



Cluster Discovery : Result

Cluster Target Properties

The cluster target will be added with the following properties. SCAN Name, SCAN Port and ONS Port properties are applicable to Clusterware versions 11.2 and higher.

* Target Name

Oracle Home

SCAN Name

SCAN Port

ONS Port

Cluster Host and High Availability Services Targets

The following host targets along with the corresponding Oracle High Availability Service targets will be added as members of this cluster.

Host Target Name	Oracle High Availability Service Target Name
None	

Note: The SCAN name, SCAN port, and ONS port properties are applicable only for Clusterware versions 11.2 and higher.

7. You can add more hosts and high availability service targets to the cluster. If a particular host is not displayed when you click **Add,** it is possible that the host already belongs to another cluster.

   To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   Click **Next.**
8. Review the displayed information, then click **Submit.**

2.4.5 Discovering Single Instance High Availability Service Targets

This section describes the different methods in which you can discover, promote, and add single instance high availability service targets. In particular, this section covers the following:

- Discovering and Promoting Single Instance High Availability Service Targets Using Autodiscovery
- Discovering and Adding Single Instance High Availability Service Targets Using the Guided Discovery Process
- Discovering and Adding Single Instance High Availability Service Targets By Specifying Target Monitoring Properties

2.4.5.1 Discovering and Promoting Single Instance High Availability Service Targets Using Autodiscovery

To automatically discover and promote single instance high availability service targets using Auto Discovery, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Promoting Single Instance High Availability Targets to Managed Status

2.4.5.1.1 Step 1: Discovering Unmanaged Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.1.2.1.

2.4.5.1.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Convert the unmanaged hosts to managed hosts, as described in Section 2.2.1.2.2.

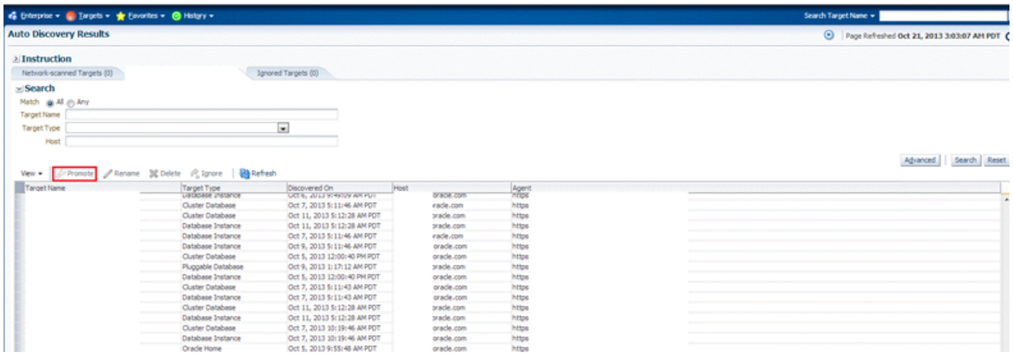
2.4.5.1.3 Step 3: Promoting Single Instance High Availability Targets to Managed Status

To promote single instance high availability targets, follow these steps:

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

   Note: If you do not see any results, then autodiscovery of targets has been disabled. To enable autodiscovery refer to Enabling Autodiscovery of Database Targets.

   From the results table, from the Agent-based targets tab, select the discovered High Availability instance target that you want to add for monitoring, and click **Promote.**



Auto Discovery Results

Page Refreshed **Oct 21, 2013 3:03:07 AM PDT**

Instruction

Search

Match ● All ○ Any

Target Name

Target Type

Host

Target Name	Target Type	Discovered On	Host	Agent
	Database Instance	Oct 6, 2013 9:49:09 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Database Instance	Oct 9, 2013 5:11:46 AM PDT	oracle.com	https
	Cluster Database	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Pluggable Database	Oct 9, 2013 1:17:12 AM PDT	oracle.com	https
	Database Instance	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Oracle Home	Oct 5, 2013 9:55:48 AM PDT	oracle.com	https

2. The Promote Targets:Result page displays the High Availability instances discovered. Select the database

   On the Promote Target: Results page, under the High Availability Services section, select the SIHA target that you want to promote.

3. Specify the monitoring credentials for the selected SIHA target, that is, the Monitor user name, Monitor password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

4. Click **Test Connection** to test the connection made to the SIHA target using the specified monitoring credentials.

5. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

6. If you have selected multiple databases and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**

7. Click **Next.**

8. Review the displayed information, then click **Submit.**

2.4.5.2 Discovering and Adding Single Instance High Availability Service Targets Using the Guided Discovery Process

To discover and add single instance high availability service targets using the guided process, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Single Instance High Availability Service Targets

2.4.5.2.1 Step 1: Discovering Unmanaged Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.2.1.

2.4.5.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

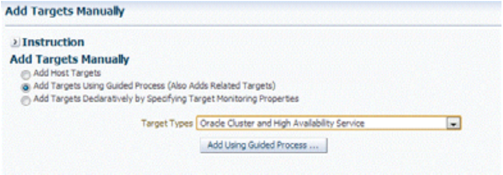
Note: Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

2.4.5.2.3 Step 3: Adding Single Instance High Availability Service Targets

To add single instance high availability service targets, follow these steps:

1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Add Manually page, select **Add Targets Using Guided Process (Also Adds Related Targets).**
3. From the Target Types list, select **Oracle Cluster and High Availability Service.**
4. Click **Add Using Guided Process.**



Add Targets Manually

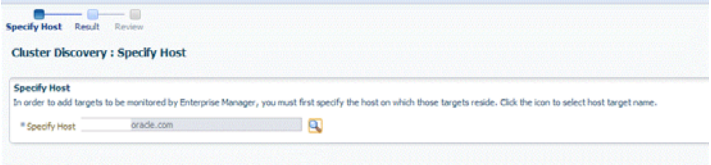
› Instruction

Add Targets Manually

○ Add Host Targets
● Add Targets Using Guided Process (Also Adds Related Targets)
○ Add Targets Declaratively by Specifying Target Monitoring Properties

Target Types: Oracle Cluster and High Availability Service

5. On the Cluster Discovery: Specify Host page, specify the single instance high availability service host, or click on the **Specify Host or Cluster** search icon to select the cluster.



Cluster Discovery : Specify Host

Specify Host

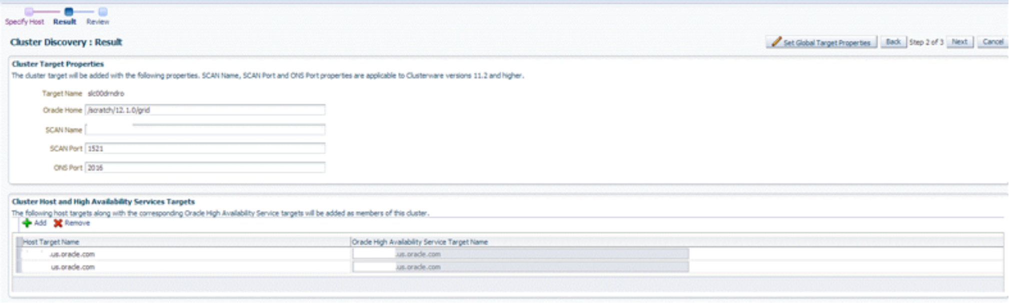
In order to add targets to be monitored by Enterprise Manager, you must first specify the host on which those targets reside. Click the icon to select host target name.

* Specify Host: oracle.com

Click **Next.**

6. The Cluster Discovery:Result page displays the high availability service instances discovered.

   On the Cluster Discovery: Result page, under the High Availability Services section, select the high availability service instance target that you want to promote.



Cluster Discovery : Result

Cluster Target Properties

The cluster target will be added with the following properties. SCAN Name, SCAN Port and ONS Port properties are applicable to Clusterware versions 11.2 and higher.

Target Name	slc00drndro
Oracle Home	/scratch/12.1.0/grid
SCAN Name	
SCAN Port	1521
ONS Port	2016

Cluster Host and High Availability Services Targets

The following host targets along with the corresponding Oracle High Availability Service targets will be added as members of this cluster.

Host Target Name	Oracle High Availability Service Target Name
.us.oracle.com	.us.oracle.com
us.oracle.com	.us.oracle.com

7. Click **Next.**

8. Review the displayed information, then click **Submit.**

2.4.5.3 Discovering and Adding Single Instance High Availability Service Targets By Specifying Target Monitoring Properties

To discover and add a single instance High Availability Service target declaratively by specifying target monitoring properties, follow these steps:

- Step 1: Discovering Unmanaged Hosts.
- Step 2: Converting Unmanaged Hosts to Managed Hosts.
- Step 3: Adding Single Instance High Availability Service Targets.

2.4.5.3.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.3.1.

2.4.5.3.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.3.2.

2.4.5.3.3 Step 3: Adding Single Instance High Availability Service Targets

To add single instance high availability service targets, follow these steps:

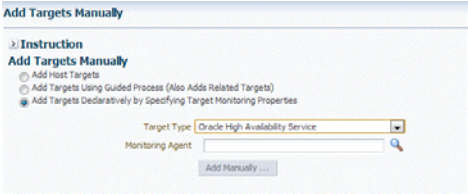
1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**

2. On the Add Targets Add Manually page, select **Add Targets Declaratively by Specifying Target Monitoring Properties.**

3. From the Target Type list, select **Oracle High Availability Service.**

4. In the Monitoring Agent field, select the Management Agent monitoring the database.

5. Click **Add Manually.**



Add Targets Manually

Instruction

Add Targets Manually

○ Add Host Targets

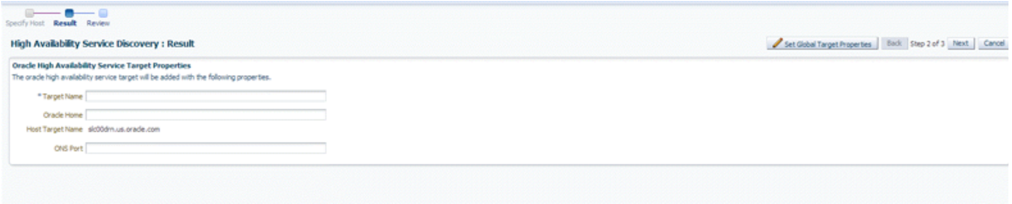
○ Add Targets Using Guided Process (Also Adds Related Targets)

● Add Targets Declaratively by Specifying Target Monitoring Properties

Target Type: Oracle High Availability Service

Monitoring Agent:

6. On the High Availability Service: Result page, specify a name for the target, the Oracle home, and the ONS port.



High Availability Service Discovery : Result

Oracle High Availability Service Target Properties

The oracle high availability service target will be added with the following properties.

* Target Name:

Oracle Home:

Host Target Name: slc00drn.us.oracle.com

ONS Port:

To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

Click **Next.**

7. Review the displayed information, and then click **Submit.**

2.4.6 Discovering Cluster Automatic Storage Management Targets

This section describes the different methods in which you can discover, promote, and add ASM cluster targets. In particular, this section covers the following:

- Discovering and Promoting Cluster ASM Targets Using Autodiscovery
- Discovering and Adding Cluster ASM Targets Using the Guided Discovery Process
- Discovering and Adding Cluster ASM Targets By Specifying Target Monitoring Properties

2.4.6.1 Discovering and Promoting Cluster ASM Targets Using Autodiscovery

To discover and promote Cluster Automatic Storage Management targets using autodiscovery, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Promoting Cluster ASM Targets to Managed Status

2.4.6.1.1 Step 1: Discovering Unmanaged Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.1.2.1.

2.4.6.1.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Convert the unmanaged hosts to managed hosts, as described in Section 2.2.1.2.2.

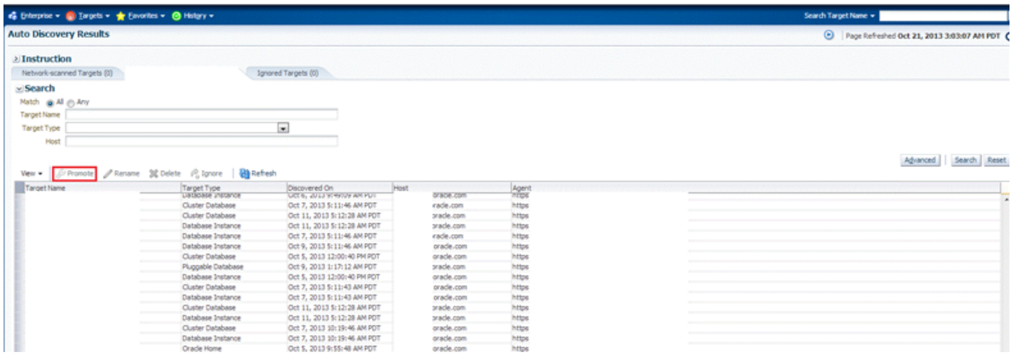
2.4.6.1.3 Step 3: Promoting Cluster ASM Targets to Managed Status

To promote cluster ASM targets, follow these steps:

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

   Note: If you do not see any results, then autodiscovery of targets has been disabled. To enable autodiscovery refer to Enabling Autodiscovery of Database Targets.

   From the results table, from the Agent-based targets tab, select the discovered cluster ASM target that you want to add for monitoring, and click **Promote.**



Auto Discovery Results

Page Refreshed Oct 21, 2013 3:03:07 AM PDT

Instruction

Network-scanned Targets (0)

Ignored Targets (0)

Search

Match ● All ○ Any

Target Name

Target Type

Host

Target Name	Target Type	Discovered On	Host	Agent
	Database Instance	Oct 6, 2013 9:49:09 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:46 AM PDT	racle.com	https
	Database Instance	Oct 9, 2013 5:11:46 AM PDT	oracle.com	https
	Cluster Database	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Pluggable Database	Oct 9, 2013 1:17:12 AM PDT	oracle.com	https
	Database Instance	Oct 5, 2013 12:00:40 PM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 5:11:43 AM PDT	oracle.com	https
	Cluster Database	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Database Instance	Oct 11, 2013 5:12:28 AM PDT	oracle.com	https
	Cluster Database	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Database Instance	Oct 7, 2013 10:19:46 AM PDT	oracle.com	https
	Oracle Home	Oct 5, 2013 9:55:48 AM PDT	oracle.com	https

2. The Promote Targets:Result page displays the targets discovered on the cluster ASM.

   On the Promote Target: Results page, in the Cluster ASM section, select the target that you want to promote.

   By default, selecting the cluster ASM target for promotion also selects all its associated discovered targets for promotion. If you want to add or remove a target from the ones selected for promotion, select the cluster ASM target, then click **Configure.** Select the **Instances** tab, then click **Add** or **Remove.** Click **Save.**

3. In the cluster ASM section, specify the monitoring credentials for the selected cluster ASM target, that is, the Monitor user name, Monitor password, and role.

Also, if you want the selected target to be added to a group, specify a value for **Group.**

If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

4. Click **Test Connection** to test the connection made to the cluster ASM target using the specified monitoring credentials.
5. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**
6. If you have selected multiple targets and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**
7. Click **Next.**
8. Review the displayed information, then click **Submit.**

2.4.6.2 Discovering and Adding Cluster ASM Targets Using the Guided Discovery Process

To discover and add cluster ASM targets using the guided process, follow these steps:

- Step 1: Discovering Unmanaged Hosts.
- Step 2: Converting Unmanaged Hosts to Managed Hosts.
- Step 3: Adding Cluster ASM Targets.

2.4.6.2.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.2.1.

2.4.6.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

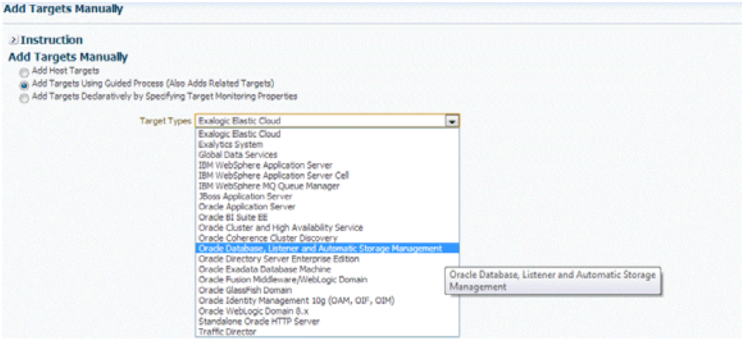
Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

2.4.6.2.3 Step 3: Adding Cluster ASM Targets

To add cluster ASM targets, follow these steps:

1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**

2. On the Add Targets Add Manually page, select **Add Targets Using Guided Process (Also Adds Related Targets).**
3. From the Target Types list, select **Oracle Database, Listener, and Automatic Storage Management.**
4. Click **Add Using Guided Process.**



Add Targets Manually

Instruction

Add Targets Manually

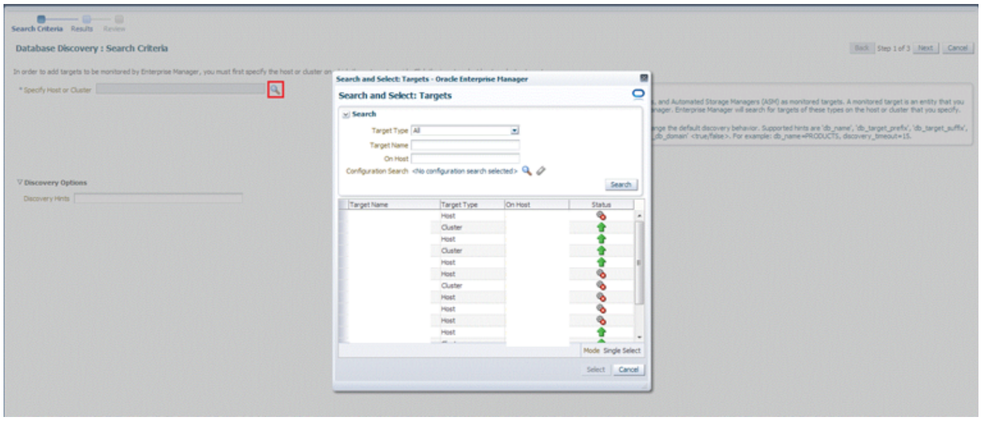
○ Add Host Targets
● Add Targets Using Guided Process (Also Adds Related Targets)
○ Add Targets Declaratively by Specifying Target Monitoring Properties

Target Types: Exalogic Elastic Cloud

- Exalogic Elastic Cloud
- Exalytics System
- Global Data Services
- IBM WebSphere Application Server
- IBM WebSphere Application Server Cell
- IBM WebSphere MQ Queue Manager
- JBoss Application Server
- Oracle Application Server
- Oracle BI Suite EE
- Oracle Cluster and High Availability Service
- Oracle Coherence Cluster Discovery
- Oracle Database, Listener and Automatic Storage Management
- Oracle Directory Server Enterprise Edition
- Oracle Exadata Database Machine
- Oracle Fusion Middleware/WebLogic Domain
- Oracle GlassFish Domain
- Oracle Identity Management 10g (OAM, OIF, OIM)
- Oracle WebLogic Domain 8.x
- Standalone Oracle HTTP Server
- Traffic Director

Oracle Database, Listener and Automatic Storage Management

5. On the Database Discovery: Search Criteria page, specify the cluster ASM host, or click on the **Specify Host or Cluster** search icon to select the cluster.



Database Discovery : Search Criteria

In order to add targets to be monitored by Enterprise Manager, you must first specify the host or cluster on

* Specify Host or Cluster

Discovery Options

Discovery Hints

Search and Select: Targets - Oracle Enterprise Manager

Search and Select: Targets

Search

Target Type: All

Target Name:

On Host:

Configuration Search: <No configuration search selected>

Target Name	Target Type	On Host	Status
	Host		●
	Cluster		↑
	Host		↑
	Cluster		↑
	Host		↑
	Host		●
	Cluster		●
	Host		●
	Host		●
	Host		●
	Host		↑

Mode: Single Select

If the specified host belongs to a cluster, then you are prompted to choose if you want to discover and promote all the database targets present on only on the specified host, or all the database targets present on all the hosts that belong to the cluster.

Click **Next.**

6. The Database Discovery:Result page displays the targets discovered on the cluster ASM target.

   On the Database Discovery: Results page, in the Cluster ASM section, select the target that you want to promote.

   By default, selecting the cluster ASM target for promotion also selects all its associated discovered targets for promotion. If you want to add or remove a target from the ones selected for promotion, select the cluster ASM target, then click **Configure.** Select the **Instances** tab, then click **Add** or **Remove.** Click **Save.**

7. In the cluster ASM section, specify the monitoring credentials for the selected cluster ASM target, that is, the Monitor user name, Monitor password, and role. Also, if you want the selected target to be added to a group, specify a value for **Group.**

   If you specify Normal for **Role,** then the user name must be `dbsnmp;` you cannot provide a different user name. However, if you specify SYSDBA for **Role**, then you can provide any SYSDBA user. Only SYSDBA users and the `dbsnmp` user have the privileges required for target monitoring.

8. Click **Test Connection** to test the connection made to the cluster ASM target using the specified monitoring credentials.

9. To specify global target properties for all the targets you have selected on the Promote Target: Results page, click **Set Global Target Properties,** specify the required properties, then click **OK.**

   To specify a common group for all the targets you have selected on the Promote Target: Results page, click **Specify Group for Targets,** select a group, then click **Select.**

10. If you have selected multiple targets and you want to set the same monitoring properties for all of them, select **Specify Common Monitoring Credentials.** Enter the monitoring credentials, monitoring password, and role. Click **Apply.**

11. Click **Next.**

12. Review the displayed information, then click **Submit.**

2.4.6.3 Discovering and Adding Cluster ASM Targets By Specifying Target Monitoring Properties

To discover and add a cluster ASM target declaratively by specifying target monitoring properties, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Cluster ASM Targets

2.4.6.3.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.3.1.

2.4.6.3.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

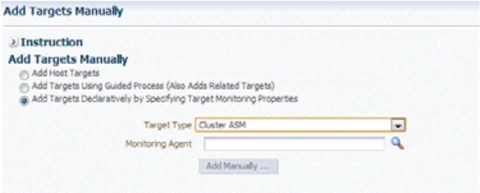
> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.3.2.

2.4.6.3.3 Step 3: Adding Cluster ASM Targets

To add a cluster ASM target, follow these steps:

1. From the Setup menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Add Manually page, select **Add Targets Declaratively by Specifying Target Monitoring Properties.**
3. From the Target Type list, select **Cluster ASM.**
4. In the Monitoring Agent field, select the Management Agent monitoring the database.
5. Click **Add Manually.**



Add Targets Manually

Instruction

Add Targets Manually

○ Add Host Targets
○ Add Targets Using Guided Process (Also Adds Related Targets)
● Add Targets Declaratively by Specifying Target Monitoring Properties

Target Type: Cluster ASM

Monitoring Agent:

6. On the Configure Cluster ASM: Properties page, specify a name for the Cluster ASM, the Oracle home path, username and password, role, cluster name, and service name.

> **Note:** The Service Name is used to establish the cluster ASM connection. It should be one of the service names the cluster ASM registers with the listeners.

7. You can add instances, ASM IO server instances, and ASM proxy instances by clicking **Add** in the respective sections.

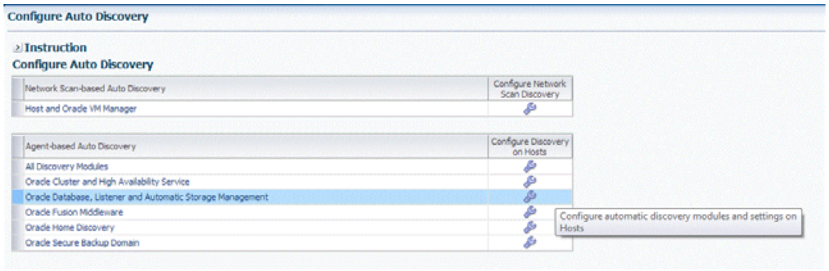
   Click **Test Connection** to test the connection made to the cluster ASM target using the specified monitoring credentials.

   OK.

2.4.7 Enabling Autodiscovery of Database Targets

Autodiscovery of database targets is enabled by default. If autodiscovery has been disabled, you can enable it, by following these steps:

1. From the **Setup** menu, select **Add Target,** then select **Configure Auto Discovery.**
2. On the Configure Auto Discovery page, in the Agent-based Auto Discovery table, select **Oracle Database, Listener, and Automatic Storage Management.**



Configure Auto Discovery

› **Instruction**

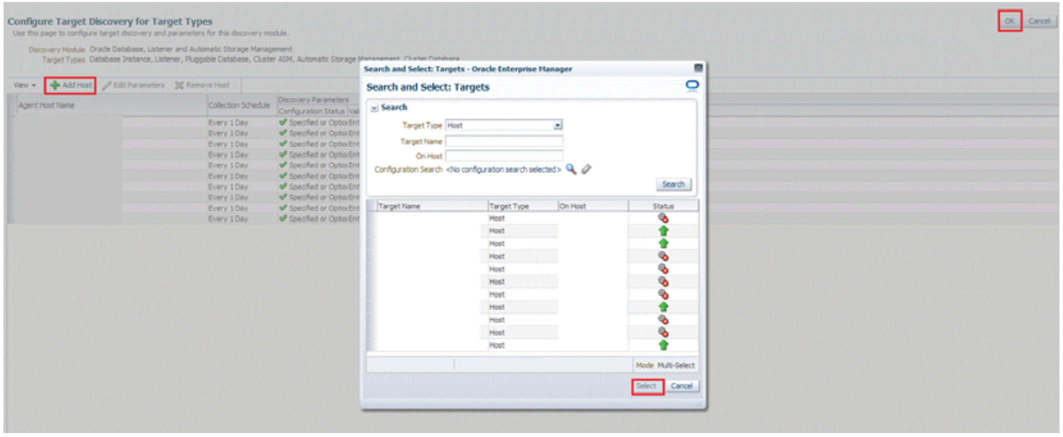
Configure Auto Discovery

Network Scan-based Auto Discovery	Configure Network Scan Discovery
Host and Oracle VM Manager	🔧

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

Configure automatic discovery modules and settings on Hosts

3. On the Configure Target Discovery page, click **Add Host.**



Configure Target Discovery for Target Types

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

Discovery Module Oracle Database, Listener and Automatic Storage Management

Target Types Database Instance, Listener, Pluggable Database, Cluster ASM, Automatic Storage Management, Cluster Database

Agent Host Name	Collection Schedule	Discovery Parameters Configuration Status	Val
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent
	Every 1 Day	✓ Specified or Optio	Ent

Search and Select: Targets - Oracle Enterprise Manager

Search and Select: Targets

Search

Target Type: Host

Target Name:

On Host:

Configuration Search <No configuration search selected>

Target Name	Target Type	On Host	Status
	Host		⊘
	Host		▲
	Host		▲
	Host		⊘
	Host		⊘
	Host		⊘
	Host		⊘
	Host		▲
	Host		⊘
	Host		⊘
	Host		▲

Mode Multi-Select

4. From the Search and Select Targets dialog box, select a target that you want to be configured, and click **Select.**

5. You can click **Edit Parameters** to edit the parameters of the target.

   Click **OK.**

2.5 Discovering, Promoting, and Adding Middleware Targets

This section describes how you can discover, promote, and add fusion middleware targets to be managed by Cloud Control. In particular, this section covers the following:

- Discovering Weblogic 9.x or 10.x Domains
- Discovering New or Modified Domain Members
- Discovering a Standalone Oracle HTTP Server
- Discovering Exalytics Targets
- Removing Middleware Targets

2.5.1 Discovering Weblogic 9.x or 10.x Domains

This section describes the different methods in which you can discover, promote, and add weblogic domain targets in Cloud Control. In particular, this section covers the following:

- Discovering and Promoting Weblogic Domains Using Autodiscovery
- Discovering and Adding WebLogic 9.x or 10.x Domains Using the Guided Discovery Process
- Adding Multiple WebLogic Domains Using EM CLI

2.5.1.1 Discovering and Promoting Weblogic Domains Using Autodiscovery

To discover and promote Weblogic domains, follow these steps:

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

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Discovering Weblogic Domains on Managed Hosts
- Step 4: Promoting Weblogic Domains to Managed Status

2.5.1.1.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged hosts, as described in Section 2.2.1.2.1.

2.5.1.1.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

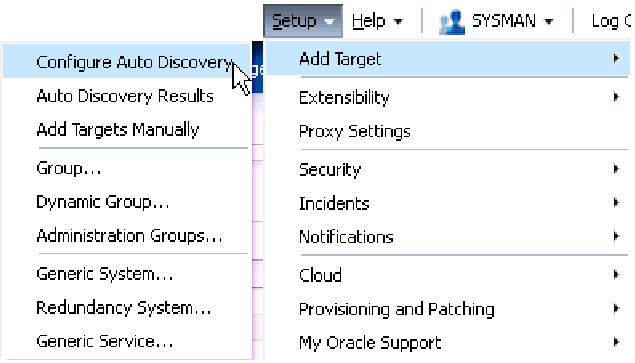
Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.1.2.2.

2.5.1.1.3 Step 3: Discovering Weblogic Domains on Managed Hosts

To discover weblogic domains on managed hosts, follow these steps:

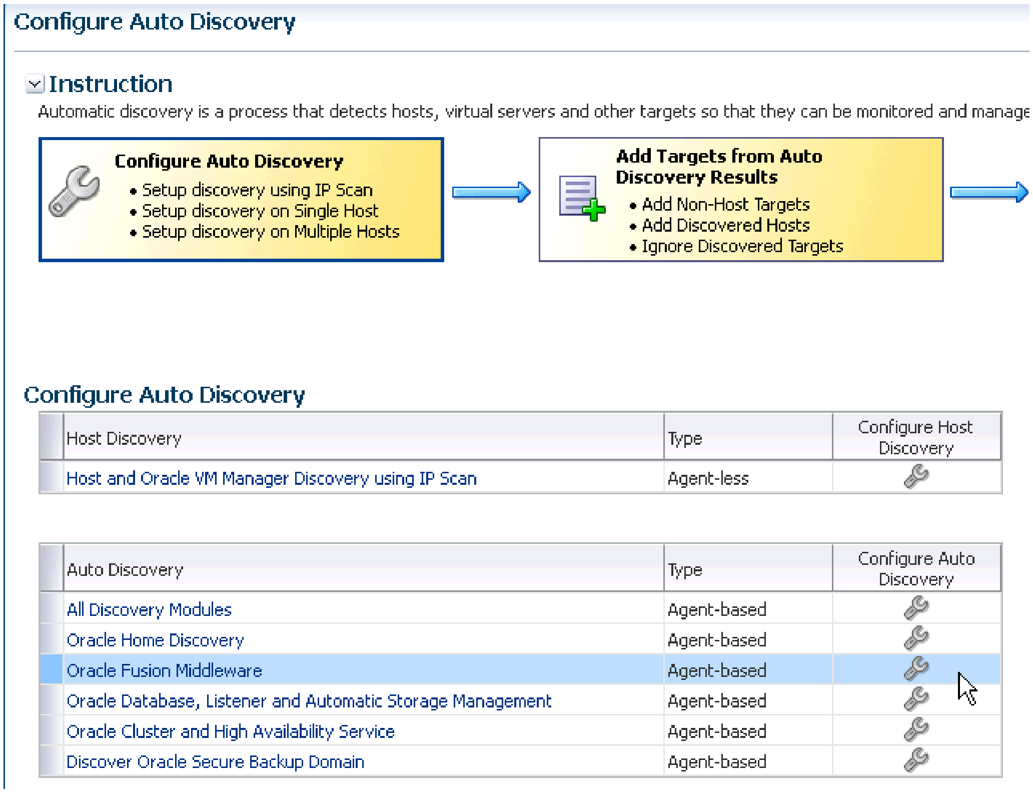
1. From the **Setup** menu, select **Add Target**, then select **Configure Auto Discovery**.

Figure 2–5 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 2–6 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

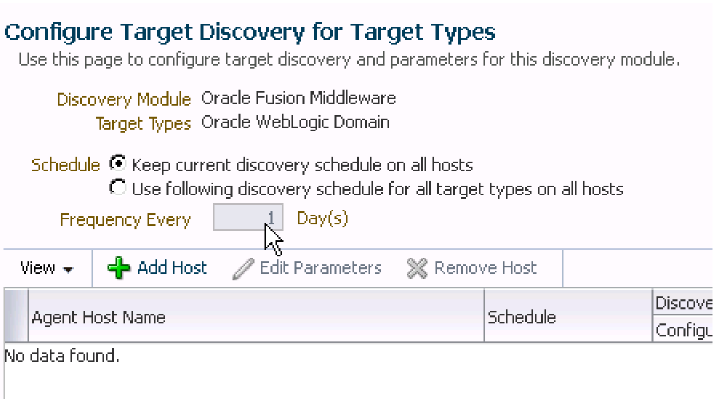
Configure Auto Discovery

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 2–7 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

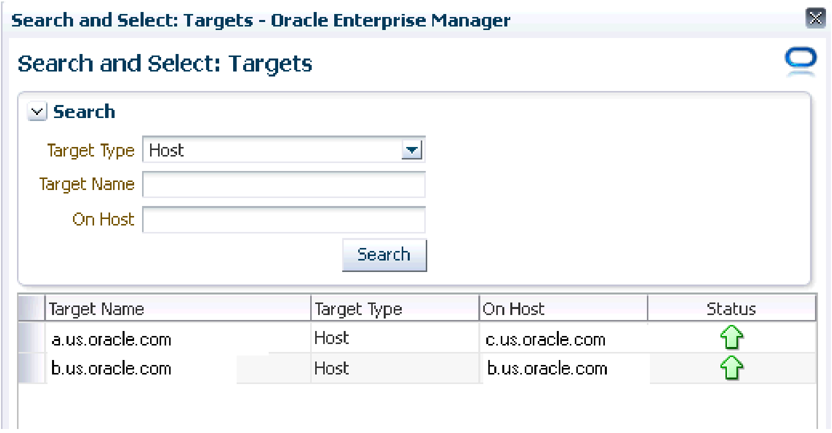
Frequency Every 1 Day(s)

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 2–8 Host Machines Available for Discovery



Search and Select: Targets - Oracle Enterprise Manager

Search and Select: Targets

Search

Target Type: Host

Target Name:

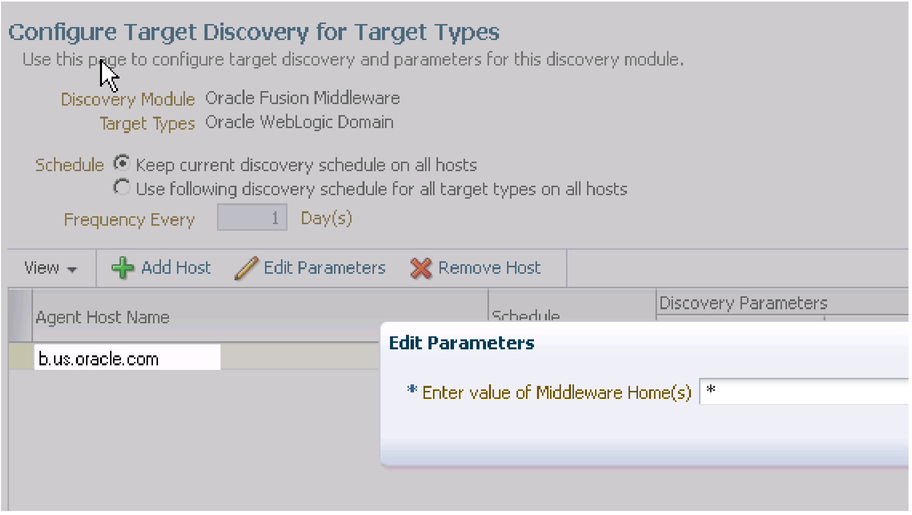
On Host:

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 2–9 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)

Agent Host Name	Schedule	Discovery Parameters
b.us.oracle.com		

Edit Parameters

* Enter value of Middleware Home(s): *

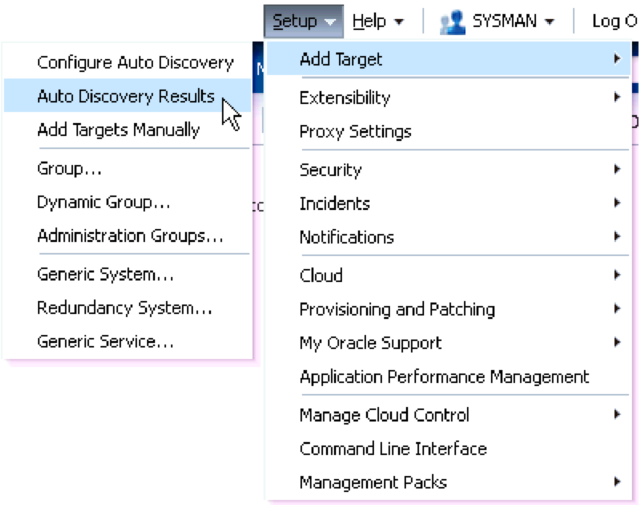
6. Click the **OK** button located at the right of the screen. At this point, automatic discovery has been enabled, and the discovery job will run at the scheduled frequency.

2.5.1.1.4 Step 4: Promoting Weblogic Domains to Managed Status

To promote weblogic domains, follow these steps:

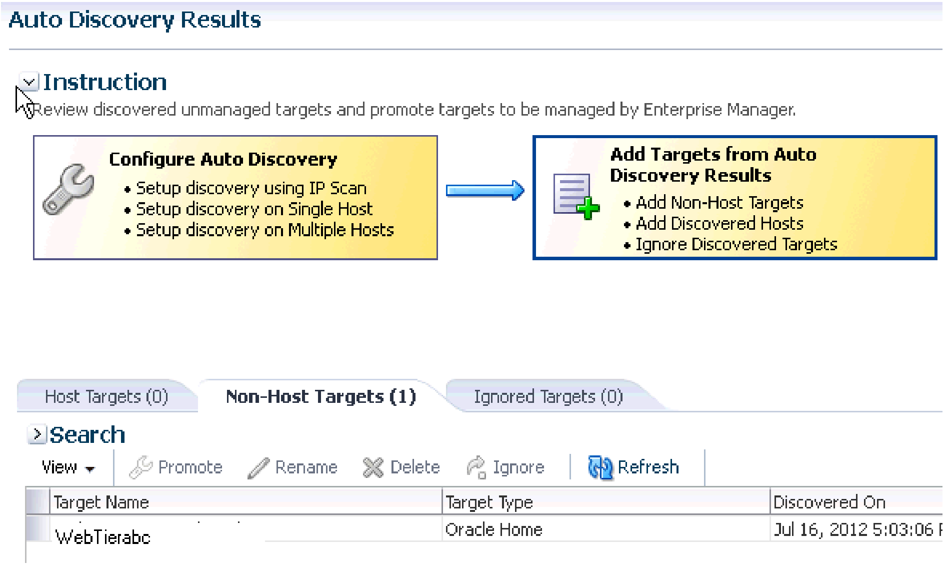
1. From the **Setup** menu, select **Add Target**, then select **Auto Discovery Results**.

Figure 2–10 Auto Discovery Results Option



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

Figure 2–11 Auto Discovery Results Page


Auto Discovery Results

Instruction

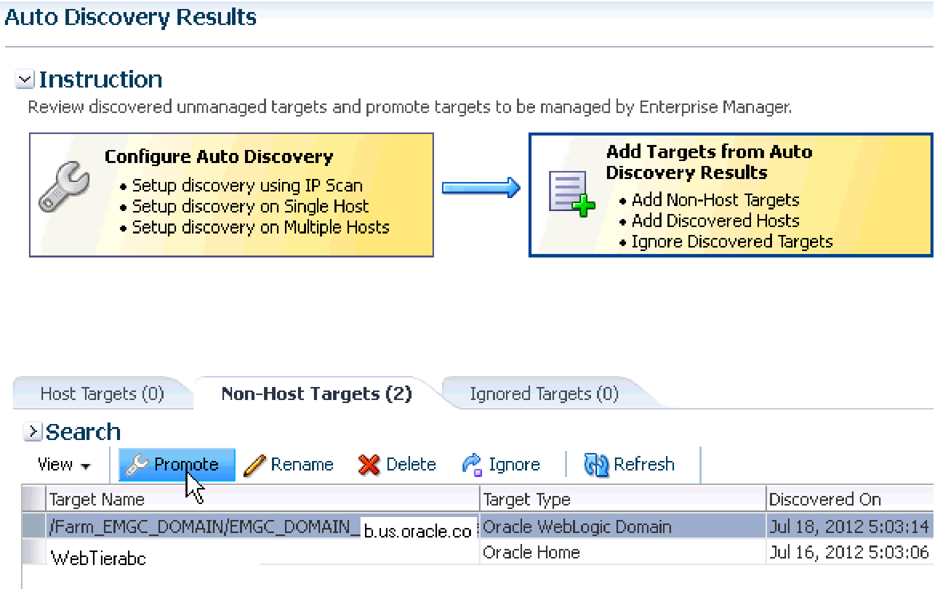
Review discovered unmanaged targets and promote targets to be managed by Enterprise Manager.

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

3. 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 2–12 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

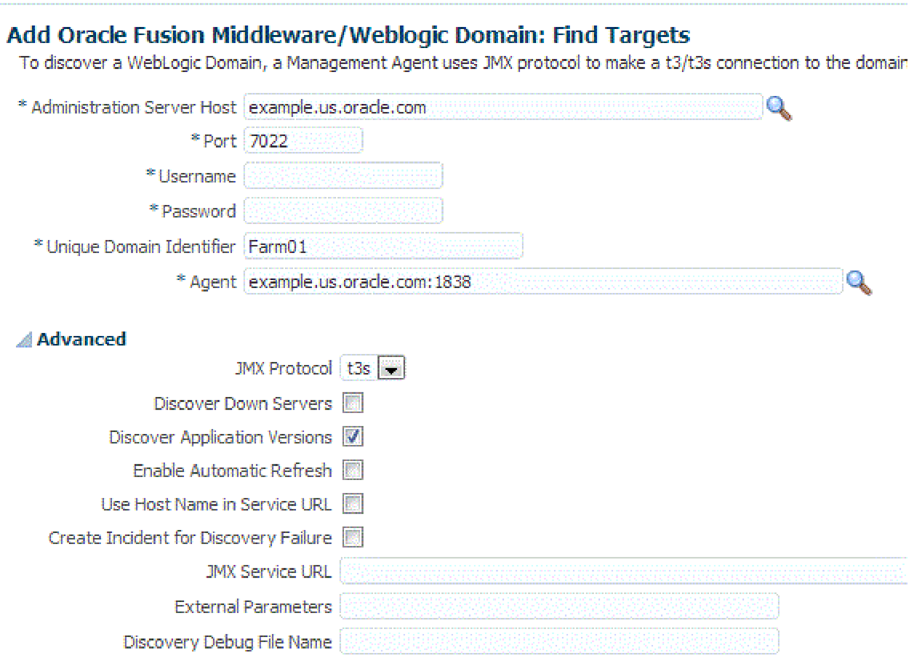
Add Targets from Auto Discovery Results
- Add Non-Host Targets
- Add Discovered Hosts
- Ignore Discovered Targets

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

4. Supply or accept values for the following parameters:

   Figure 2–13 shows the parameters that need to be provided.

Figure 2–13 Parameters



Add Oracle Fusion Middleware/Weblogic Domain: Find Targets

To discover a WebLogic Domain, a Management Agent uses JMX protocol to make a t3/t3s connection to the domair

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

Advanced

JMX Protocol	t3s
Discover Down Servers	□
Discover Application Versions	☑
Enable Automatic Refresh	□
Use Host Name in Service URL	□
Create Incident for Discovery Failure	□
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 certificate, this certificate is automatically updated to monitoring and discovery agent. If a custom certificate is used, refer to *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 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.

- Discover Application Versions

  By default, each version of a deployed Java EE application will be discovered as a target. Therefore, with every new version, a new target will be discovered. Deselect this check box if you want only the active version of the application to be discovered.

- Enable Automatic Refresh

  This option refreshes the weblogic domain every 24 hours.

- Use Host Name in Service URL

  You can use host name in service URL instead of JMX. It is recommended to use this option if you are using a private network and there are many hosts using the same IP address.

- Create Incident for Discovery Failure

  This option creates an OMS incident if discovery fails. You can view the incident from the Support workbench page.

- 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.

5. Click **Continue**. Enterprise Manager will discover all Fusion Middleware targets within the domain.
6. 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.
7. 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.
8. Click **Close** in the processing window when finished. The Results page displays the targets and Agent assignments.
9. 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.

> **Note:** After you discover a middleware target for the first time, it is recommended that you learn the best practices for monitoring and managing the discovered target. To navigate to the Target Management Best Practices page, from the target home page, select the **Weblogic Domain** menu, and then select **Target Management Best Practices.** The page lists the best practices items for a Fusion Middleware Domain.

2.5.1.2 Discovering and Adding WebLogic 9.x or 10.x Domains Using the Guided Discovery Process

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

Note: Fusion Middleware 12c discovery also discovers dynamic servers, CAM (Common Administration Model) managed components, as well as a new target type called *Domain Application*.

Domain application represents the deployment of a target to a domain.

For Fusion Middleware 12c discovery, when Cloud Control discovers a Fusion Middleware WebLogic domain, it creates a Domain Application target for each Java EE application deployed in a Weblogic domain. For any Java EE application deployed on any number of servers, only one Domain Application target will be discovered.

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.

To discover and add a weblogic domain using the guided process, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Weblogic Domains

2.5.1.2.1 Step 1: Discovering Unmanaged Hosts

Note: Skip this step if host is already managed in Enterprise Manager.

Discover the unmanaged host, as described in Section 2.2.2.1.

2.5.1.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

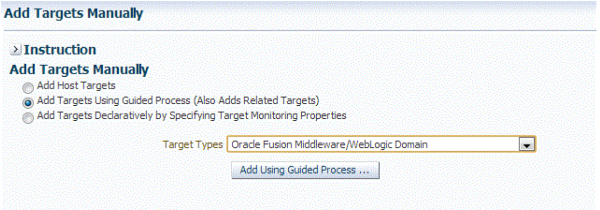
Note: Skip this step if host is already managed in Enterprise Manager.

Convert the discovered unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

2.5.1.2.3 Step 3: Adding Weblogic Domains

To add a weblogic domain, follow these steps:

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/Weblogic Domain** as the target type.
4. Click **Add Using Guided Discovery**.



Add Targets Manually

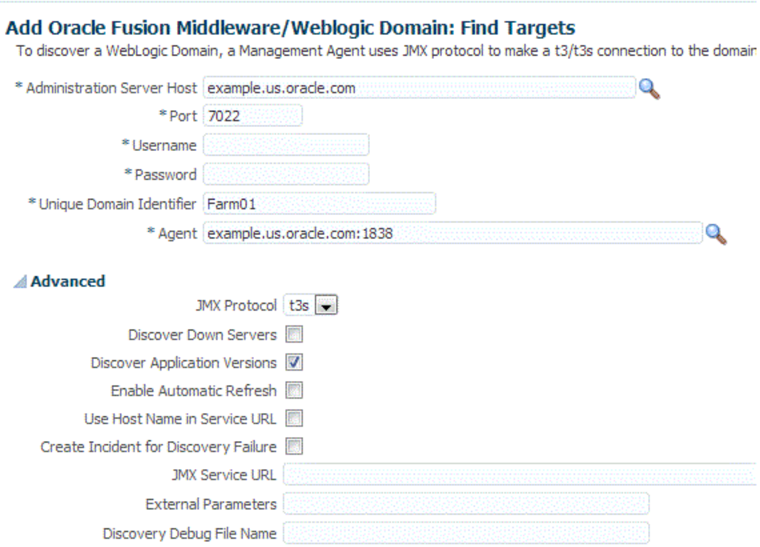
Instruction

Add Targets Manually

○ Add Host Targets
● Add Targets Using Guided Process (Also Adds Related Targets)
○ Add Targets Declaratively by Specifying Target Monitoring Properties

Target Types: Oracle Fusion Middleware/WebLogic Domain

5. Supply or accept values for the following parameters:



Add Oracle Fusion Middleware/Weblogic Domain: Find Targets

To discover a WebLogic Domain, a Management Agent uses JMX protocol to make a t3/t3s connection to the domair

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

Advanced

JMX Protocol: t3s
Discover Down Servers ☐
Discover Application Versions ☑
Enable Automatic Refresh ☐
Use Host Name in Service URL ☐
Create Incident for Discovery Failure ☐
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 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. For Secure domain JMX protocol - use t3s. If WebLogic domain is using a demo certificate, this certificate is automatically updated to monitoring and discovery Agent.

- Discover Down Servers

  Use this check box to discover servers that are down. While adding Oracle Fusion Middleware WebLogic Domain targets to 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.

- Discover Application Versions

  By default, each version of a deployed Java EE application will be discovered as a target. Therefore, with every new version, a new target will be discovered. Deselect this check box if you want only the active version of the application to be discovered.

- 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.

- Discover Application Versions

  By default, each version of a deployed Java EE application will be discovered as a target. Therefore, with every new version, a new target will be discovered. Deselect this check box if you want only the active version of the application to be discovered.

- Enable Automatic Refresh

  This option refreshes the weblogic domain every 24 hours.

- Use Host Name in Service URL

  You can use host name in service URL instead of JMX. It is recommended to use this option if you are using a private network and there are many hosts using the same IP address.

- Create Incident for Discovery Failure

  This option creates an OMS incident if discovery fails. You can view the incident from the Support workbench page.

- 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.

> **Note:** After you discover a middleware target for the first time, it is recommended that you learn the best practices for monitoring and managing the discovered target. To navigate to the Target Management Best Practices page, from the target home page, select the **Weblogic Domain** menu, and then select **Target Management Best Practices.** The page lists the best practices items for a Fusion Middleware Domain.

2.5.1.3 Adding Multiple WebLogic Domains Using EM CLI

If you have multiple WebLogic domains that you want to manage through 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.

2.5.2 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, 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

2.5.2.1 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:

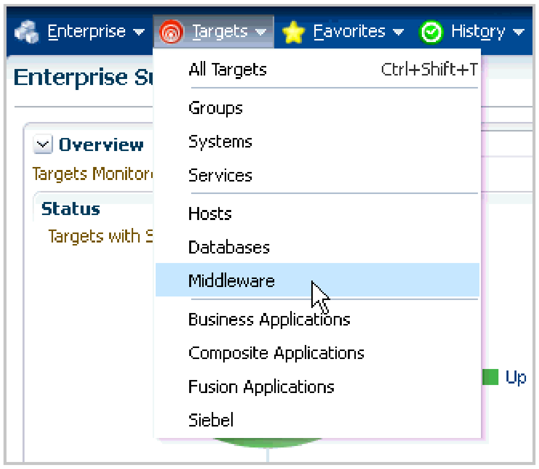
1. Click the **Jobs** tab.
2. Click the job title in the Job Activity page.
3. Click **Edit**.

2.5.2.2 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.

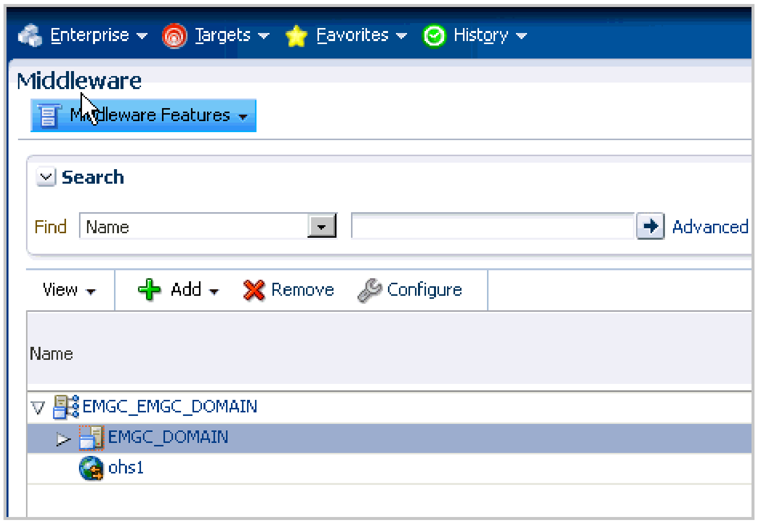
1. From the **Targets** menu, select **Middleware**.

Figure 2–14 Targets Menu



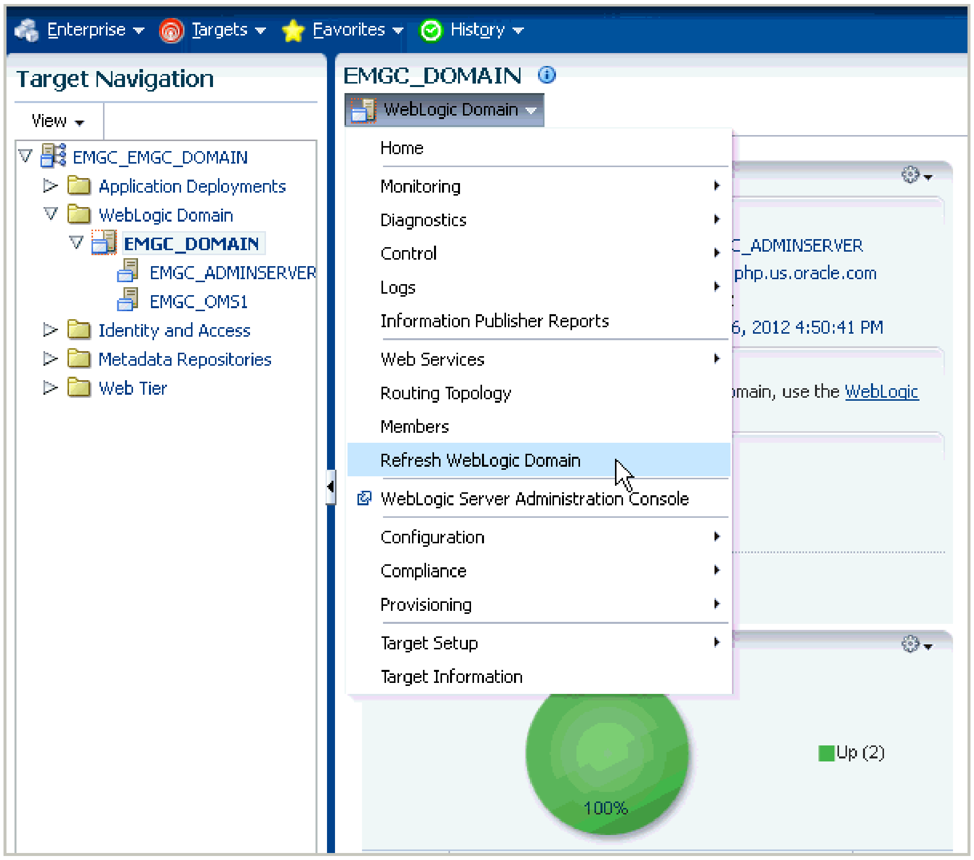
2. Click the WebLogic Domain you want to (enable the job for in the Middleware home page) refresh.

Figure 2–15 WebLogic Domain to Enable



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

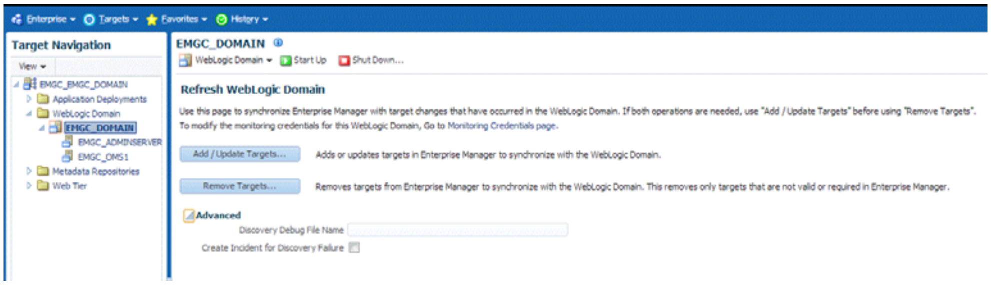
Figure 2–16 Refresh WebLogic Domain Menu Option



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.

   When any entity in a domain is removed from a Weblogic domain such as Weblogic j2eeaserver, j2eeapp, and the like, they are still displayed in Enterprise Manager. Click **Remove Targets** if you do not need the historical data of these targets. The obsolete targets which can be removed from the domain are then displayed.

Figure 2–17 Add/Update Option on Refresh WebLogic Domain Page



Refresh WebLogic Domain

Use this page to synchronize Enterprise Manager with target changes that have occurred in the WebLogic Domain. If both operations are needed, use "Add / Update Targets" before using "Remove Targets".
To modify the monitoring credentials for this WebLogic Domain, Go to Monitoring Credentials page.

Add / Update Targets... Adds or updates targets in Enterprise Manager to synchronize with the WebLogic Domain.

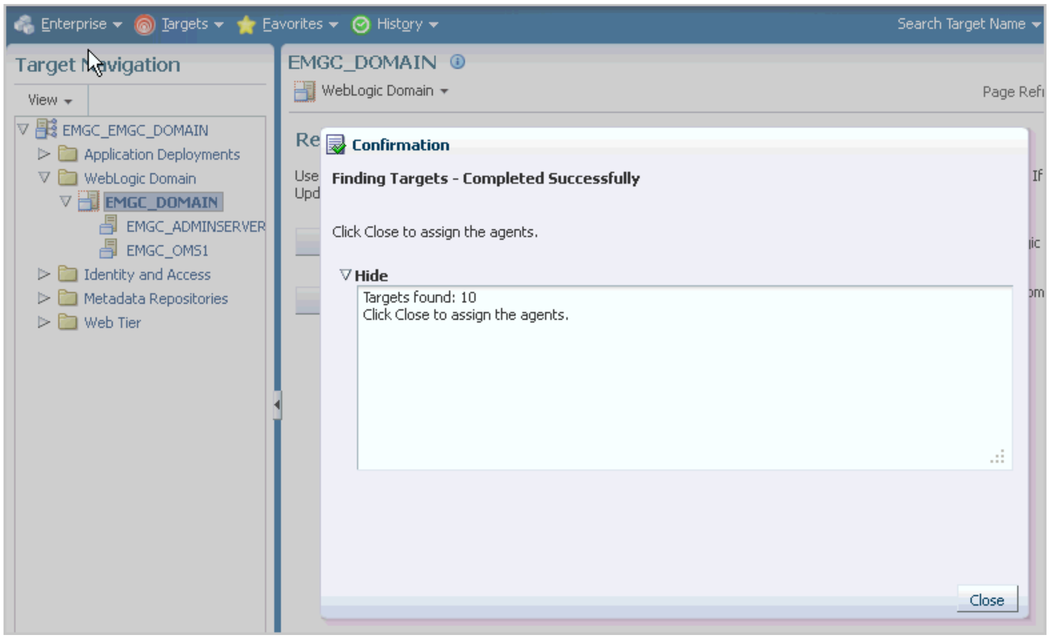
Remove Targets... Removes targets from Enterprise Manager to synchronize with the WebLogic Domain. This removes only targets that are not valid or required in Enterprise Manager.

Advanced

Discovery Debug File Name

Create Incident for Discovery Failure □

Figure 2–18 Confirmation of Finding Targets



Confirmation

Finding Targets - Completed Successfully

Click Close to assign the agents.

Targets found: 10
Click Close to assign the agents.

5. Discovery Debug File Name option

   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.

6. 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:

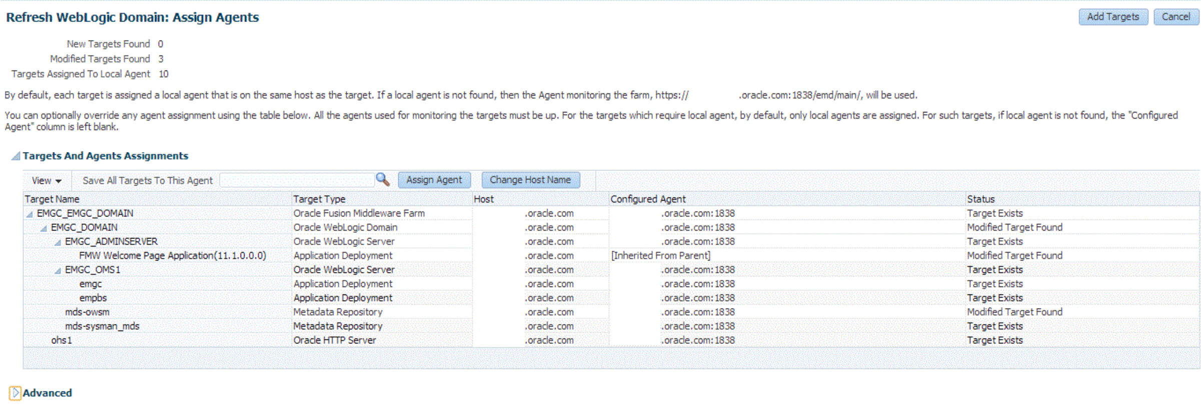
   - If a local Agent can be found on the target host, that Agent will be assigned.
   - If a local Agent cannot be found on the host, the Agent specified in the Targets page will be assigned.

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

   This page also provides the option of Selective Discovery. Using this option, you can disable the discovery of only new target types.

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

Figure 2–19 Assign Agents Page



Refresh WebLogic Domain: Assign Agents

New Targets Found	0
Modified Targets Found	3
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:// .oracle.com:1838/emd/main/, will be used.

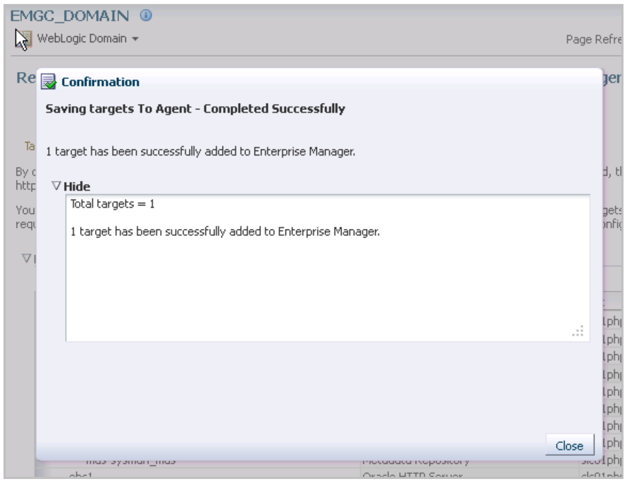
You can optionally override any agent assignment using the table below. All the agents used for monitoring the targets must be up. For the targets which require local agent, by default, only local agents are assigned. For such targets, if local agent is not found, the "Configured Agent" column is left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

Targets And Agents Assignments

Target Name	Target Type	Host	Configured Agent	Status
EMGC_EMGC_DOMAIN	Oracle Fusion Middleware Farm	.oracle.com	.oracle.com:1838	Target Exists
EMGC_DOMAIN	Oracle WebLogic Domain	.oracle.com	.oracle.com:1838	Modified Target Found
EMGC_ADMINSERVER	Oracle WebLogic Server	.oracle.com	.oracle.com:1838	Target Exists
FMW Welcome Page Application(11.1.0.0.0)	Application Deployment	.oracle.com	[Inherited From Parent]	Modified Target Found
EMGC_OMS1	Oracle WebLogic Server	.oracle.com	.oracle.com:1838	Target Exists
emgc	Application Deployment	.oracle.com	.oracle.com:1838	Target Exists
empbs	Application Deployment	.oracle.com	.oracle.com:1838	Target Exists
mds-owsm	Metadata Repository	.oracle.com	.oracle.com:1838	Modified Target Found
mds-sysman_mds	Metadata Repository	.oracle.com	.oracle.com:1838	Target Exists
ohs1	Oracle HTTP Server	.oracle.com	.oracle.com:1838	Target Exists

7. 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 2–20 Confirmation Saving Targets to Agent



Saving targets To Agent - Completed Successfully

1 target has been successfully added to Enterprise Manager.

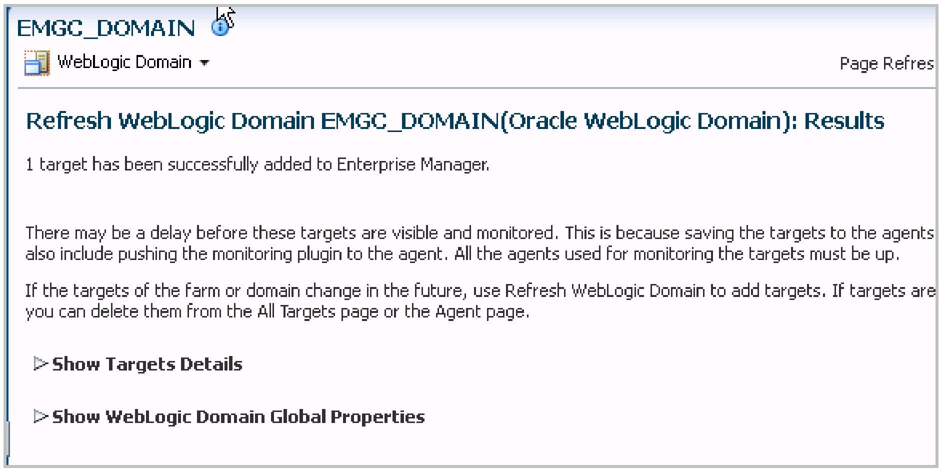
Total targets = 1

1 target has been successfully added to Enterprise Manager.

8. 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 Middleware Targets.

Figure 2–21 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

9. 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.

   Once discovery is done, you will need to set up the monitoring credentials of the domain, before you can monitor it. To do this, on the Weblogic domain homepage, from the Weblogic domain menu, select **Target setup**, and then click **Monitoring credentials.**

2.5.3 Discovering a Standalone Oracle HTTP Server

To discover standalone Oracle HTTP Servers, follow these steps:

- Meeting the Prerequisites
- Discovering a Standalone Oracle HTTP Server Using the Guided Discovery Process

---

Note: To view a visual demonstration on how to discover and manage standalone Oracle HTTP Servers, access the following URL and click **Begin Video.** The discovery described in this visual demonstration is based Enterprise Manager Cloud Control 12c Release 2 (12.1.0.3) and the Oracle Fusion Middleware Plug-in 12.1.0.5.

`http://apex.oracle.com/pls/apex/f?p=44785:24:0::::P24_CONTENT_ID,P24_PREV_PAGE:8529,1`

2.5.3.1 Meeting the Prerequisites

Before you discover a standalone Oracle HTTP server, meet the following:

- Ensure that an Oracle Management Agent (Management Agent) is installed on the host where the standalone Oracle HTTP Server is running. For instructions to install a Management Agent, see the *Oracle Enterprise Manager Cloud Control Basic Installation Guide* available in the Enterprise Manager documentation library.
- Ensure that the standalone Oracle HTTP Server you are about to discover is of one of the following releases: 11.1.1.1, 11.1.1.2, 11.1.1.3, 11.1.1.4, 11.1.1.5, 11.1.1.6, 11.1.1.7, 12.1.2.

2.5.3.2 Discovering a Standalone Oracle HTTP Server Using the Guided Discovery Process

To discover and add a standalone Oracle HTTP server, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Standalone Oracle HTTP Server Targets

2.5.3.2.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover unmanaged hosts, as described in Section 2.2.2.1.

2.5.3.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Convert unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

2.5.3.2.3 Step 3: Adding Standalone Oracle HTTP Server Targets

Add standalone Oracle HTTP server targets, by following these steps:

1. From the **Setup** menu, select **Add Target,** then select **Add Targets Manually.**
2. On the Add Targets Manually page, select **Add Targets Using Guided Process (Also Adds Related Targets).**
3. From the Target Types list, select **Standalone Oracle HTTP Server.**
4. Click **Add Using Guided Process.**
5. On the Add Standalone Oracle HTTP Server page, provide the following details, and click **Add Target.**

Element	Description
Oracle HTTP Server Host	Click the search icon to search and select the host where the standalone Oracle HTTP Server is running. In the Search and Select: Targets dialog, search the host, select it, and click **Select.** For example, `example.com`
Agent URL	URL of the Management Agent that is installed on the host where the standalone Oracle HTTP Server is running. Appears automatically by default when you select the standalone Oracle HTTP Server host. For example, `https://example.com:1838/emd/main/`

Element	Description
Target Name	Enter a unique name with which you want to monitor the standalone Oracle HTTP Server target in Enterprise Manager Cloud Control. For example, `Standalone_OHS1` The name must be unique, and no other standalone Oracle HTTP Server target already monitored in Enterprise Manager Cloud Control must have this name. The name cannot contain colons (:), semi-colons (;), or any leading or trailing blanks. Once the standalone Oracle HTTP Server is discovered and added to Enterprise Manager Cloud Control, if you want to search for this particular target, follow these steps: 1. From the **Targets** menu, select **All Targets.** 2. On the All Targets page, in the **Search Target Name** field, enter the target name with which you discovered and added the standalone Oracle HTTP Server target, and click the search icon.
Oracle Home	Click the search icon to log in to the standalone Oracle HTTP Server host, and select the Oracle home where the standalone Oracle HTTP Server is running. For example, /u01/software/oracle/Standalone_OHS1
Configuration Path	Click the search icon to log in to the standalone Oracle HTTP Server host, and select the `httpd.conf` file. The value for this field must ideally be the absolute directory path to the `httpd.conf` file. For example, `/u01/software/oracle/Standalone_OHS1/Oracle_WT1/instances/instance1/config/OHS/ohs1/`
Node Manager User Name	*(This field is only for discovering standalone Oracle HTTP Server 12c (12.1.2))* Enter the Node Manager user name, which you provided while configuring the standalone domain. For more information, see the task on configuring the node manager in *Oracle Fusion Middleware Installing and Configuring Oracle HTTP Server*.
Node Manager Password	*(This field is only for discovering standalone Oracle HTTP Server 12c (12.1.2))* Enter the Node Manager password, which you provided while configuring the standalone domain. For more information, see the task on configuring the node manager in *Oracle Fusion Middleware Installing and Configuring Oracle HTTP Server*.

2.5.4 Discovering Exalytics Targets

In order to manage and monitor Oracle Fusion Middleware components running on Exalytics, such as WebLogic domain, Oracle BI Foundation 11g, and Oracle TimesTen (in-memory database), Cloud Control must first discover the Exalytics machine containing these components.

An Exalytics system consists of one or more Exalytics machines. The machine(s) can be physical, virtualized, or a mix of both.

Once discovered, the Exalytics machine and the components within it can be promoted to "managed target" status, enabling Cloud Control to collect the data needed to monitor the target.

Related targets running on the Exalytics machine such as OBIEE, Times Ten and WebLogic, need to be discovered following the respective flows for those components.

If the Exalytics target has been discovered, the related targets will be associated with the Exalytics target when they are discovered. Else, the association will happen when the Exalytics target is discovered.

To discover and add an exalytics target, follow these steps:

- Meeting the Prerequisites
- Discovering and Adding Exalytics System Targets Using the Guided Discovery Process

2.5.4.1 Meeting the Prerequisites

Before discovering an Exalytics machine target, you must meet the following prerequisites:

- A Management Agent for discovering targets must be deployed onto the physical Exalytics machine (host).

  For discovering a virtual machine, make sure that at least one of the virtual Exalytics has a Management Agent running on it. The Management Agent should be on one of the VM Guest part of the virtual Exalytics Machine deployment. However, all virtual machines that contain components that need to be monitored require a Management Agent to be deployed on.

- To identify the Exalytics machine, ensure that you have the context info file which contains the Exalytics machine ID.
- To discover and monitor ILOM for a virtual Exalytics machine, you must install IMPITOOL on the VM guest. To install IMPITOOL, follow these steps:

  1. Download the latest Hardware Management Pack compatible with the operating system on your VM guest. Instructions for downloading the Hardware Management Pack are available here: `http://www.oracle.com/technetwork/server-storage/servermgmt/downloads/index.html`
  2. Extract the IMPITOOL package from the downloaded zip file and install it on the operating system on the VM guest.

2.5.4.2 Discovering and Adding Exalytics System Targets Using the Guided Discovery Process

To discover and add Exalytics system target in an Exalytics system, follow these steps:

- Step 1: Discovering Unmanaged Hosts
- Step 2: Converting Unmanaged Hosts to Managed Hosts
- Step 3: Adding Exalytics Targets

2.5.4.2.1 Step 1: Discovering Unmanaged Hosts

> **Note:** Skip this step if host is already managed in Enterprise Manager.

Discover unmanaged hosts, as described in Section 2.2.2.1.

2.5.4.2.2 Step 2: Converting Unmanaged Hosts to Managed Hosts

---

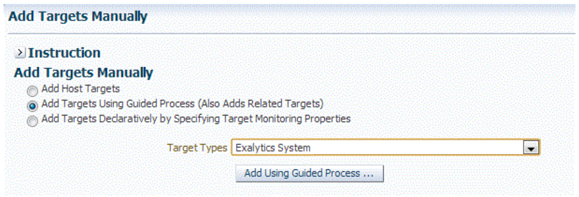
Note: Skip this step if host is already managed in Enterprise Manager.

Convert unmanaged hosts to managed hosts, as described in Section 2.2.2.2.

2.5.4.2.3 Step 3: Adding Exalytics Targets

Add Exalytics targets, by following these steps:

1. From the **Setup** menu, select **Add Target,** and then select **Add Targets Manually.**
2. On the Add Targets Manually page, select **Add Targets Using Guided Process (Also Adds Related Targets).**
3. From the Target Types drop-down list, select **Exalytics System,** and then click **Add Using Guided Process...**



Add Targets Manually

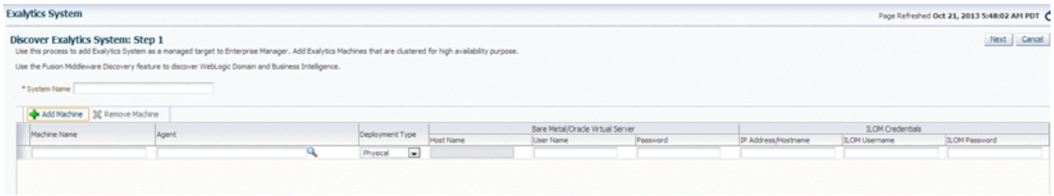
Instruction

Add Targets Manually

○ Add Host Targets
● Add Targets Using Guided Process (Also Adds Related Targets)
○ Add Targets Declaratively by Specifying Target Monitoring Properties

Target Types: Exalytics System

4. On the Discover Exalytics System page, provide a name for the Exalytics System, and then click **Add Machine.**



Exalytics System

Page Refreshed Oct 21, 2013 5:48:02 AM PDT

Discover Exalytics System: Step 1

Use this process to add Exalytics System as a managed target to Enterprise Manager. Add Exalytics Machines that are clustered for high availability purpose.

Use the Fusion Middleware Discovery feature to discover WebLogic Domain and Business Intelligence.

* System Name

Machine Name	Agent	Deployment Type	Bare Metal/Oracle Virtual Server			ILOM Credentials		
			Host Name	User Name	Password	IP Address/Hostname	ILOM Username	ILOM Password
		Physical						

5. Provide the following details:
   - **Machine Name**

     Provide a unique for the Oracle Exalytics machine target.
   - **Agent**

     Specify or select the Management Agent to use for the Oracle Exalytics Machine discovery process.
   - **Deployment Type**

     Select **Physical** or **Virtual** depending on if you want to discover a physical target or a virtual target.
   - **Host Name** (only for Virtual target)

     Enter the host name or IP Address where Oracle Virtual Server is running
   - **User Name and Password**

For a physical Exalytics machine, provide credentials of the root user which has privileges to run the imageinfo command.

For a virtual Exalytics machine, provide credentials to log in to Oracle Virtual Server (OVS). You should have privileges to run the imageinfo command.

- **ILOM Credentials**

  Specify the ILOM IP address or hostname, ILOM username, and ILOM password of the root user.

Note: The ILOM Credentials are optional. If you do not add the ILOM Credentials, the ILOM target will not be discovered.

You can add the ILOM target later by using the Refresh Exalytics System option.

Click **Next.**

6. A confirmation box appears. Click **OK.**

Note: Click **Add Targets** to save the targets as a Manageable Entity.

2.5.5 Removing Middleware Targets

Removing Middleware 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

Using Incident Management

Incident management allows you to monitor and resolve service disruptions quickly and efficiently by allowing you to focus on what is important from a broader management perspective (incidents) rather than isolated, discrete events that may point to the same underlying issue.

In this chapter:	You will learn:
Management Concepts	Fundamental approaches to managing your monitored environment. ■ Event Management ■ Incident Management ■ Problem Management
Setting Up Your Incident Management Environment	How to set up and configure key Enterprise Manager components used for incident management. ■ Setting Up Your Monitoring Infrastructure ■ Setting Up Notifications ■ Setting Up Administrators and Privileges
Working with Incidents	How to use incident management to track and resolve IT operation issues. ■ Finding What Needs to be Worked On ■ Searching for Incidents ■ Setting Up Custom Views ■ Responding and Working on a Simple Incident ■ Responding to and Managing Multiple Incidents, Events and Problems in Bulk ■ Searching My Oracle Support Knowledge ■ Open Service Request (Problems-only) ■ Suppressing Incidents and Problems ■ Managing Workload Distribution of Incidents ■ Reviewing Events on a Periodic Basis

In this chapter:	You will learn:
Common Tasks	Step-by-step examples illustrating how to perform common incident management tasks.. ■ Sending Email for Metric Alerts ■ Sending SNMP Traps for Metric Alerts ■ Sending Events to an Event Connector ■ Sending Email to Different Email Addresses for Different Periods of the Day
Advanced Topics	How to perform specialized incident management operations. ■ Defining Custom Incident Statuses ■ Clearing Stateless Alerts for Metric Alert Event Types ■ User-reported Events ■ Additional Rule Applications ■ Event Prioritization ■ Root Cause Analysis (RCA) and Target Down Events
Moving from Enterprise Manager 10/11g to 12c	Migrating notification rules to incident rules.

To supplement this chapter, Oracle has created instructional videos that provide you with a fast way to learn the basics of incident management to monitor your environment.

Instructional Videos: For video tutorials on incident management, see:

Incident Management Overview

`https://apex.oracle.com/pls/apex/f?p=44785:24:2961267987520:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5738%2C24`

Incident Management: Create Views in Incident Manager

`https://apex.oracle.com/pls/apex/f?p=44785:24:6091052115237:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5739%2C24`

Incident Management: View Incident Details

`https://apex.oracle.com/pls/apex/f?p=44785:24:107664888945874:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5740%2C24`

Incident Management: Use Incident Rule Sets Part 1

`https://apex.oracle.com/pls/apex/f?p=44785:24:114716879428375:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5758%2C24`

Incident Management: Use Incident Rule Sets Part 2

`https://apex.oracle.com/pls/apex/f?p=44785:24:102172707760983:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5759%2C24`

3.1 Management Concepts

Enterprise Manager exposes three levels of management granularity that, when combined, provide complete monitoring/management coverage of your environment. These management levels are:

- Event Management
- Incident Management
- Problem Management

3.1.1 Event Management

Intuitively, you monitor for specific events in your monitored environment. An event is a significant occurrence on a managed target that typically indicates something has occurred outside normal operating conditions--they provide a uniform way to indicate that something of interest has occurred in an environment managed by Enterprise Manager. Examples of events are:

- Metric Alerts
- Compliance Violations
- Job Events
- Availability Alerts

Existing Enterprise Manager customers may be familiar with metric alerts and metric collection errors. For Enterprise Manager 12*c*, metric alerts are a type of event, one of many different event types. The notion of an event unifies the different exception conditions that are detected by Enterprise Manager, such as monitoring issues or compliance issues, into a common concept. It is backed by a consistent and uniform set of event management capabilities that can indicate something of interest has occurred in a datacenter managed by Enterprise Manager.

All events have the following attributes:

Table 3–1 Event Attributes

Attribute	Description
Type	Type of event that is being reported. All events of a specific type share the same set of attributes that describe the exact nature of the problem. For example, Metric Alert, Compliance Standard Score Violation, or Job Status Change.
Severity	Event severity. For example, Fatal, Warning, or Critical.
Internal Name	An internal name that describes the nature of the event and can be used to search for events. For example, you can search for all *tablespacePctUsed* events.
Entity on which the event is raised.	An event can be raised on a target, a non-target source object (such as a job) or be related to a target and a non-target source object. Note: This attribute is important when determining what privileges are required to manage the event.
Message	Informational text associated with the event.
Reported Date	Time the event was reported.

Table 3–1 (Cont.) Event Attributes

Attribute	Description
Category	Functional or operational classification for an event. Available Categories: ■ Availability ■ Business ■ Capacity ■ Configuration ■ Diagnostics ■ Error ■ Fault ■ Jobs ■ Load ■ Performance ■ Security
Causal Analysis Update	Used for Root Cause Analysis of target down events. Possible Values: Root Cause or Symptom

Event Types

The *type* of an event defines the structure and payload of an event and provides the details of the condition it is describing. For example, a metric alert raised by threshold violation has a specific payload whereas a job state change has a different structure. As shown in the following table, the range of events types greatly expands Enterprise Manager's monitoring flexibility.

Event Type	Description
Target Availability	The Target Availability Event represents a target's availability status (Example: Up, Down, Agent Unreachable, or Blackout).
Metric Alert	A metric alert event is generated when an alert occurs for a metric on a specific target (Example: CPU utilization for a host target) or metric on a target and object combination Example: Space usage on a specific tablespace of a database target.
Metric Evaluation Error	A metric evaluation error is generated when the collection for a specific metric group fails for a target.
Job Status Change	All changes to the status of an Enterprise Manager job are treated as events, and these events are made available via the Job Status Change event class. **Note**: A prerequisite to creating Incident Rules, is to enable the relevant job status and add required targets to job event generation criteria. To change this criteria, from the **Setup** menu, select **Incidents**, and then **Job Events**.

Event Type	Description
Compliance Standard Rule Violation	Events are generated for compliance standard rule violations. Each event corresponds to a violation of a compliance rule on a specific target.
Compliance Standard Score Violation	Events are generated for compliance standard score violations. An event is generated when the compliance score for a compliance standard on a specific target falls below predefined thresholds.
High Availability	High Availability events are generated for database availability operations (shutdown and startup), database backups and Data Guard operations (switchover, failover, and other state changes).
Service Level Agreement Alert	These events are generated when a service level or service level objective is violated for a service. occurs for a Service Level Agreement or a Service Level Objective.
User-reported	These events are created by end-users.
Application Dependency and Performance Alert	Alerts are raised by the Application Dependency and Performance (ADP) monitoring when metrics related to a J2EE application or component have crossed some thresholds.
Application Performance Management KPI Alert	An Application Performance Management (APM) Key Performance Indicator (KPI) alert event is generated when a KPI violation alert occurs for a metric on an APM managed entity associated with a Business Application target.
JVM Diagnostics Threshold Violation	A JVMD Diagnostics event is raised when a JVMD metric exceeds its threshold value on a Java Virtual Machine target.

Event Severity

The severity of an event indicates the criticality of a specific issue. The following table shows the various event severity levels along with the associated icon.

Icon	Severity	Description
⛔	Fatal	Corresponding service is no longer available. For example, a monitored target is down (target down event). A Fatal severity is the highest level severity and only applies to the Target Availability event type.
❌	Critical	Immediate action is required in a particular area. The area is either not functional or indicative of imminent problems.
⚠	Warning	Attention is required in a particular area, but the area is still functional.
⚠	Advisory	While the particular area does not require immediate attention, caution is recommended regarding the area's current state. This severity can be used, for example, to report Oracle best practice violations.

Icon	Severity	Description
✓	Clear	Conditions that raised the event have been resolved.
ⓘ	Informational	A specific condition has just occurred but does not require any remedial action. Events with an informational severity: ▪ do not appear in the incident management UI. ▪ cannot create incidents. ▪ are not stored within Enterprise Manager.

3.1.2 Incident Management

You monitor and manage your Enterprise Manager environment via incidents and not discrete events (even though an incident can conceivably consist of a single event). Of all events raised within your managed environment, there is likely only a subset that you need to act on because they impact your business applications (such as a target down event). However, managing by incident also allows you to address more complex situations where the subset of events you are interested in are related and may indicate a higher level issue needs to be addressed as a single issue and not as individual events: A cluster of events by themselves may indicate a minor administrative issue, but when viewed together may signify a larger problem that can potentially consist of events from multiple domains/layers of your monitored infrastructure.

For example, you are monitoring a host. If you want to monitor 'load' being placed on one or more hosts you might be interested in events such as CPU utilization, memory utilization, and swap utilization exceeding acceptable metric thresholds. Individually, these events may or may not indicate an issue with the host, but together, these events form an incident indicating extreme load is being placed on a monitored host.

Incidents represent the larger service disruptions that may impact your business instead of discrete events. Managing by incidents, therefore, allows you to monitor for complex operational issues that may affect multiple domains that may impact your business. These incidents typically need to be tracked, assigned to appropriate personnel, and resolved as quickly as possible. You can effectively implement a centralized monitoring that consolidates monitoring information and more effectively allocate resource across your ecosystem to resolve or prevent issues from occurring. The end result is better implementation of your business processes that in turn lead to better performance of your IT resources.

While events indicate issues requiring attention in your managed environment, it is more efficient to work on a collective subset of related events as a single unit of work--you can work on different events representing the same issue or you can work on one incident containing multiple space-related events. For example, you have multiple space events from various targets that indicate you are running low on space. Instead of managing numerous discrete events, you can more efficiently manage a smaller set of incidents.

An incident is a significant event or set of related significant events that need to be managed because it can potentially impact your business applications. These incidents typically need to be tracked, assigned to appropriate personnel, and resolved as quickly as possible. You perform these incident management operations through Incident Manager, an intuitive UI within Enterprise Manager.

Incident Manger provides you with a central location from which to view, manage, diagnose and resolve incidents as well as identify, resolve and eliminate the root cause of disruptions. See Section 3.1.5, "Incident Manager" for more information about this UI.

3.1.2.1 Working with Incidents

When an incident is created, Enterprise Manager makes available a rich set of incident management workflow features that let you to manage and track the incident through its complete lifecycle.

- Assign incident ownership.
- Track the incident resolution status.
- Set incident priority.
- Set incident escalation level.
- Ability to provide a manual summary.
- Ability to add user comments.
- Ability to suppress/unsuppress
- Ability to manually clear the incident.
- Ability to create a ticket manually.

All incident management/tracking operations are carried out from Incident Manager. Creation of incidents for events, assignment of incidents to administrators, setting priority, sending notifications and other actions can be automated using (incident) rules.

Incident Status

The lifecycle of an incident within an organization is typically determined by two pieces of information: The current resolution state of the incident (Incident Status) and how important it is to resolve the incident relative to other incidents (Priority). As key incident attributes, the following options are available:

- New
- Work in Progress
- Closed
- Resolved

You can define additional statuses if the default options are not adequate. In addition, you can change labels using the Enterprise Manager Command Line Interface (EM CLI). See **Advanced Topics** for more information.

Priority

By changing the priority, you can escalate the incident and perform operations such as assigning it to a specific IT operator or notifying upper-management. The following priority options are available:

- None
- Low
- Medium
- High

- Very High
- Urgent

Priority is often based on simple business rules determined by the business impact and the urgency of resolution.

Incident Attributes

Every incident possesses attributes that provide information as identification, status for tracking, and ownership. The following table lists available incident attributes.

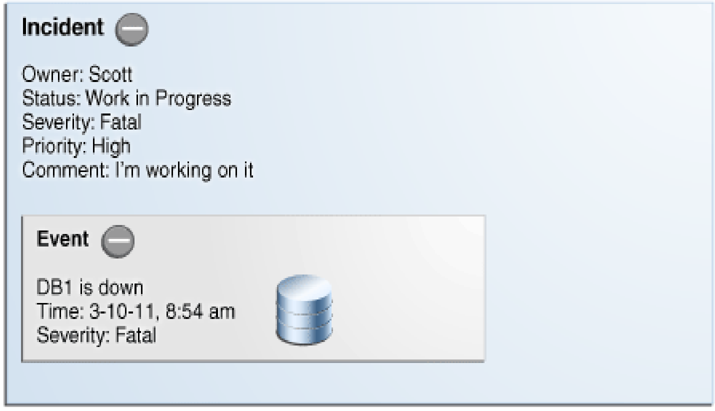
Incident Attribute	Definition
Escalated	An escalation level signifying a escalation to raise the level of attention on the incident from your organization's IT or management hierarchy. Available escalation levels: ■ None (Not escalated) ■ Level 1 through Level 5
Category	Operational or organizational classification for an incident. Incidents (and events) can have multiple categories. Categories for all events within an incident are aggregated. Available Categories: ■ Availability ■ Business ■ Capacity ■ Configuration ■ Diagnostics ■ Error ■ Fault ■ Jobs ■ Load ■ Performance ■ Security
Summary	An intuitive message indicating what the incident is about. By default, the incident summary is pulled from the message of the last event of the incident, however, this message can be changed to a fixed summary by any administrator working on the incident.
Incident Created	Date and time the incident was created.
Last Updated	Date and time the incident was last updated or when the incident was closed.
Severity	Severity is based on the worst severity of the events in the incident. For example, Fatal, Warning, or Critical.
Source	Source entities of the incident.

Incident Attribute	Definition
Priority	Priority Values ■ None (Default) ■ Low ■ Medium ■ High ■ Very High ■ Urgent
Status	Incident Status. ■ New (Default) ■ Work in Progress ■ Closed (Terminal state when the incident is closed. See below for more information.) ■ Resolved You can define additional statuses if the default options are not adequate. In addition, you can change labels using the Enterprise Manager Command Line Interface (EM CLI). Closed Status: Enterprise Manager automatically sets the status to closed when an incident severity is cleared--administrators do not manually select the Closed status. The incident severity is set to Clear when all of the events contained within the incident have been cleared. Typically the Agent sets the Clear severity, as would be the case when a metric alert value falls below a severity threshold. If an event or incident supports manual clearing, then the Clear option will be shown in the Incident Manager UI. Once an incident has been cleared by an administrator or by Enterprise Manager, only then will Enterprise Manager set the status to Closed. If you do not see the option to clear the incident in the UI, this means Enterprise Manager will automatically set the status to Clear if it detects the monitored condition no longer holds true. For example, you want to indicate that an incident has been fixed. You can set the status to Resolved and Enterprise Manager will set the status to Closed when it clears the severity.
Comment	Annotations added by an administrator to communicate analysis information or actions taken to resolve the incident.
Owner	Administrator/user currently working on the incident.
Acknowledged	Indicates that a user has accepted ownership of an incident or problem. Available options: Yes or No. When an incident is acknowledged, it will be implicitly assigned to the user who acknowledged it. When a user assigns an incident to himself, it is considered 'acknowledged'. Once acknowledged, an incident cannot be unacknowledged, but can be assigned to another user. Acknowledging an incident stops any repeat notifications for that incident.
Causal Analysis Update	Used for Root Cause Analysis of target down incidents. Possible Values: Root Cause or Symptom

3.1.2.2 Incident Composed of a Single Event

The simplest incident is composed of a single event. In the following example, you are concerned whenever any production target is down. You can create an incident for the target down event which is raised by Enterprise Manager if it detects the monitored target is down. Once the incident is created, you will have all incident management functionality required to track and manage its resolution.

Figure 3–1 Incident with a Single Event



Incident

Owner: Scott
Status: Work in Progress
Severity: Fatal
Priority: High
Comment: I'm working on it

Event

DB1 is down
Time: 3-10-11, 8:54 am
Severity: Fatal

The figure shows how both the incident and event attributes are used to help you manage the incident. From the figure, we see that the database DB1 has gone down and an event of Fatal severity has been raised. When the event is newly generated, there is no ownership or status. An incident is opened that can be updated manually or by automated rules to set owners, status, as well as other attributes. In the example, the owner/administrator Scott is currently working to resolve the issue.

The incident severity is currently Fatal as the incident inherits the worst severity of all the events within incident. In this case there is only one event associated with the incident so the severity is Fatal.

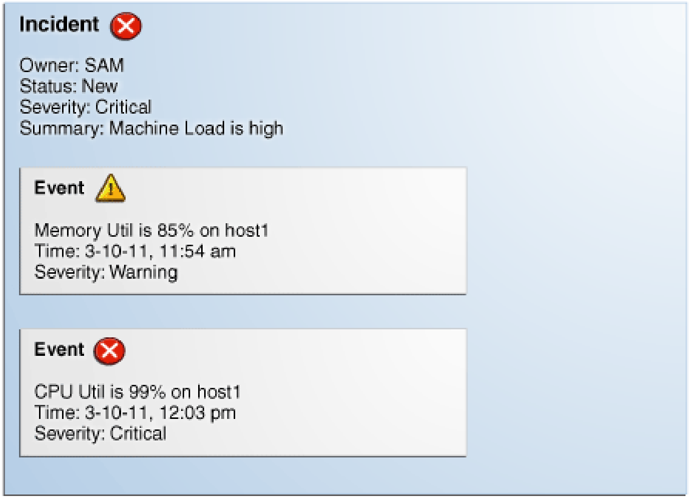
3.1.2.3 Incident Composed of Multiple Events

Situations of interest may involve more than a single event. It is an incident's ability to contain multiple events that allows you to monitor and manage complex and more meaningful issues.

> **Note:** Multi-event incidents are not automatically generated. An administrator must manually create them.

For example, if a monitored system is running out of space, separate multiple events such as *tablespace full* and *filesystem full* may be raised. Both, however, are related to running out of space. Another machine resource monitoring example might be the simultaneous raising of CPU utilization, memory utilization, and swap utilization events. See "Creating an Incident Manually" on page 3-51 for more information. Together, these events form an incident indicating extreme load is being placed on a monitored host. The following figure illustrates this example.

Figure 3–2 Incident with Multiple Events



Incident ✖

Owner: SAM
Status: New
Severity: Critical
Summary: Machine Load is high

Event ⚠

Memory Util is 85% on host1
Time: 3-10-11, 11:54 am
Severity: Warning

Event ✖

CPU Util is 99% on host1
Time: 3-10-11, 12:03 pm
Severity: Critical

Incidents inherit the worst severity of all the events within incident. The incident summary indicates why this incident should be of interest, in this case, "Machine Load is high". This message is an intuitive indicator for all administrators looking at this incident. By default, the incident summary is pulled from the message of the last event of the incident, however, this message can be changed by any administrator working on the incident.

Because administrators are interested in overall machine load, administrator Sam has manually created an incident for these two metric events because they are related—together these events represent a host overload situation. An administrator needs to take action because memory is filling up and consumed CPU resource is too high. In its current state, this condition will impact any applications running on the host.

3.1.2.4 How are Incidents Created?

Incidents are most commonly created automatically through rules and rule sets (user-defined instructions that tell Incident Manager how to handle specific events when they occur). As shown in the preceding examples, incidents can also be created manually. Once an incident is raised, its severity is inherited from the worst severity of all events within the incident. The latest event *Message*, by default, becomes the *Incident Summary*. Incidents can also be created manually. See "Creating an Incident Manually" on page 3-51 for more information.

3.1.3 Problem Management

Problem management involves the functionality that helps track the underlying root causes of incidents. Once the immediate service disruptions represented by incidents are resolved, you can then progress to understanding and resolving the underlying root cause of the issue.

For Enterprise Manager 12*c*, problems focus on the diagnostic incidents and problem diagnostic incidents/problems stored in Advanced Diagnostic Repository (ADR), which are automatically raised by Oracle software when it encounters critical errors in the software. A problem, therefore, represents the root cause of all the Oracle software incidents. For these diagnostic incidents, in order to address root cause, a problem is created that represents the root cause of these diagnostic incidents. A problem is identified by a *problem key* which uniquely identifies the particular error in software. Each occurrence of this error results in a diagnostic incident which is then associated with the problem object.

When a problem is raised for Oracle software, Oracle has determined that the recommended recourse is to open a service request (SR), send support the diagnostic logs, and eventually provide a solution from Oracle. As an incident, Enterprise Manager makes available all tracking, diagnostic, and reporting functions for problem management. Whenever you view all open incidents and problems, whether you are using Incident Manager, or in context of a target/group home page, you can easily determine what issues are actually affecting your monitored target.

To manage problems, you can use Support Workbench to package the diagnostic details gathered in ADR and open SR. Users should then manage the problems in Incident Manager. Access to Support Workbench functionality is available through Incident Manager (**Guided Resolution** area) in context of the problem.

3.1.4 Rule Sets

Incident rules and rule sets automate actions related to events, incidents and problems. They can automate the creation of incidents based on important events, perform notification actions such as sending email or opening helpdesk tickets, or perform operations to manage the incident workflow lifecycle such as changing incident ownership, priority, or escalation level.

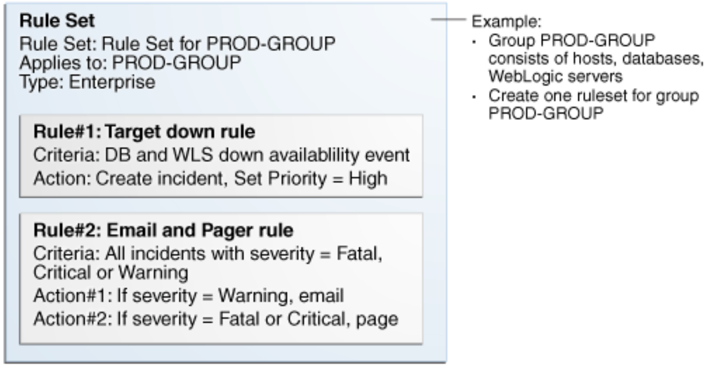
With previous versions of Enterprise Manager, you used notification rules to choose the individual targets and conditions for which you want to perform actions or receive notifications (send email, page, open a helpdesk ticket) from Enterprise Manager. For Enterprise Manager 12c, the concept and function of notification rules has been replaced with incident rules and rule sets.

- **Rules**: A rule instructs Enterprise Manager to take specific actions when incidents, events, or problems occur, such as performing notifications. Beyond notifications, rules can also instruct Enterprise Manager to perform specific actions, such as creating incidents, updating incidents and problems. The actions can also be conditional in nature. For example, a rule action can be defined to page a user when an incident severity is critical or just send email if it is warning.
- **Rule Set**: An incident rule set is a collection of rules that apply to a common set of objects such as targets (hosts, databases, groups), jobs, metric extensions, or self updates and take appropriate actions to automate the business processes underlying event, incident and problem management.

Operationally, individual rules within a rule set are executed in a specified order as are the rule sets themselves. Rule sets are executed in a specified order. By default, the execution order for both rules and rule sets is the order in which they are created, but they can be reordered from the Incident Rules UI.

The following figure shows typical rule set structure and how the individual rules are applied to a heterogeneous group of targets.

Figure 3–3 Rule Set Application



Rule Set
Rule Set: Rule Set for PROD-GROUP
Applies to: PROD-GROUP
Type: Enterprise

Rule#1: Target down rule
Criteria: DB and WLS down availablility event
Action: Create incident, Set Priority = High

Rule#2: Email and Pager rule
Criteria: All incidents with severity = Fatal, Critical or Warning
Action#1: If severity = Warning, email
Action#2: If severity = Fatal or Critical, page

Example:
- Group PROD-GROUP consists of hosts, databases, WebLogic servers
- Create one ruleset for group PROD-GROUP

The graphic illustrates a situation where all rules pertaining to a group of targets can be put into a single rule set (this is also a best practice). In the above example, a group named *PROD-GROUP* consists of hosts, databases, and WebLogic servers exists as part of a company's managed environment. A single rule set is created to manage the group.

In addition to the actual rules contained within a rule set, a rule set possesses the following attributes:

- **Name**: A descriptive name for the rule set.
- **Description**: Brief description stating the purpose of the rule set.
- **Applies To**: Object to which all rules in the rule set apply: Valid rule set objects are targets, jobs, metric extensions, and self update.
- **Owner**: The Enterprise Manager user who created the rule set. Rule set owners have the ability to update or delete the rule set and the rules in the rule set.
- **Enabled**: Whether or not the rule set is actively being applied.
- **Type**: Enterprise or Private. See "Rule Set Types" on page 3-14

3.1.4.1 Out-of-Box Rule Sets

Enterprise Manager provides out-of-box rule sets for incident creation and event clearing based on typical scenarios. Out-of-box rule sets cannot be edited or deleted, however, they can be disabled. As a best practice, you should create your own copies of out-of-box rule sets and then subscribe to the rule set copies rather than subscribing directly to the out-of-box rule sets. Effectively, you are making a copy of the rule set and changing the target criteria to fit your enterprise needs by selecting an appropriate group of targets (preferably an administration group).

Please note that out-of-box rule set definitions and actions they perform can be changed by Oracle at any time and will be applied during patching or software upgrade.

Regular Enterprise Manager administrators are allowed to perform the following operations on rule sets:

- Subscribe
- Subscribe for email notifications
- Unsubscribe
- Unsubscribe from email notifications

- Enable
- Disable

> **Note:** Even though administrators can subscribe to a rule set, they will only receive notification from the targets for which they have at least the View Target privilege.

Enterprise Manager Super Administrators have the added ability to reorder the rule sets.

Enterprise rule sets are evaluated sequentially and may go through multiple passes as needed. When there is a change to the entity being processed - such as an incident being created for an event or an incident priority changing due to a rule - we rerun through all the rules from the beginning again until there are no matches. Any rule that is matched in a prior pass will not match again (to prevent infinite loops).

For example, when a new event, incident, or problem arises, the first rule set in the list is checked to see if any of its member rules apply and appropriate actions specified in those rules are taken. The second rule is then checked to see if its rules apply and so on. Private rule sets are only evaluated once all enterprise rule set evaluations are complete and in no particular order.

> **Important:** Use caution when reordering rule sets as their order defines the event, incident, and problem handling workflow. Reordering rule sets without fully understanding the impact on your system can result in unintended actions being taken on incoming events, incidents, and problems.

3.1.4.2 Rule Set Types

There are two types of Rule Sets:

- **Enterprise**: Used to implement all operational practices within your IT organization. All supported actions are available for this type of rule set. However, because this type of rule set can perform all actions, there are restrictions as to who can create an enterprise rule set.

  In order to create or edit an enterprise rule set, an administrator must have been granted the *Create Enterprise Rule Set* privilege on the *Enterprise Rule Set* resource. However, if the rule set owner loses the *Create Enterprise Rule Set* system privilege at some future time, he can still edit or delete the rule set. Super Administrators can edit or delete any rule set.

  If the originator of the rule set wants other administrators to edit the rule set, he will need to share access in order to work collaboratively by adding co-authors. Enterprise rule sets are visible to all administrators.

- **Private**: Used when an administrator wants to be notified about something he is monitoring but not as a standard business practice. The only action a private rule set can perform is to send email to the rule set owner. Any administrator can create a private rule set regardless of whether they have been granted the *Create Enterprise Rule Set* resource privilege. Oracle recommends that private rule sets be used only in rare or exceptional situations.

When a rule set performs actions, the privileges of the rule set creator are used. For example, a rule set owner/creator must have at least View Target privilege in order to receive notifications and at least Manage Target Events privilege in order to update the incident. The exception is when a rule set sends a notification. In this case, the privileges of the user it is sent to is used.

3.1.4.3 Rules

Rules are instructions within a rule set that automate actions on incoming events or incidents or problems. Because rules operate on *incoming* incidents/events/problems, if you create a new rule, it will not act retroactively on incidents/events/problems that have already occurred.

Every rule is composed of two parts:

- **Criteria**: The events/incidents/problems on which the rule applies.
- **Action**(s): The ordered set of one or more operations on the specified events, incidents, or problems. Each action can be executed based on additional conditions.

The following table shows how rule criteria and actions determine rule application. In this rule operation example there are three rules which take actions on selected events and incidents. Within a rule set, rules are executed in a specified order. The rule execution order can be changed at any time. By default, rules are executed in the order they are created.

Table 3–2 Rule Operation

Rule Name	Execution Order	Criteria	Action	
			Condition	**Actions**
Rule 1	First	CPU Util(%), Tablespace Used(%) metric alert events of warning or critical severity		Create incident.
Rule 2	Second	Incidents of warning or critical severity	If severity = critical	Notify by page
			If severity =warning	Notify by email
Rule 3	Third	Incidents are unacknowledged for more than six hours		Set escalation level to 1

In the rule operation example, *Rule 1* applies to two metric alert events: *CPU Utilization* and *Tablespace Used*. Whenever these events reach either Warning or Critical severity threshold levels, an incident is created.

When the incident severity level (the incident severity is inherited from the worst event severity) reaches Warning, *Rule 2* is applied according to its first condition and Enterprise Manager sends an email to the administrator. If the incident severity level reaches Critical, *Rule 2*'s second condition is applied and Enterprise Manager sends a page to the administrator.

If the incident remains open for more than six hours, *Rule 3* applies and the incident escalation level is increased from None to Level 1. At this point, Enterprise Manager runs through all the rule sets and their rules from the beginning again.

3.1.4.3.1 Rule Application Each rule within a rule set applies to an event, incident OR problem. For each of these, you can choose rule application criteria such as:

- Apply the rule to incoming events or updated events only

- Apply the rule to critical events only.

Rules are applied to events, incidents, and problems according to criteria selected at the time of rule creation (or update). The following situations illustrate the methodology used to apply rules.

- If one of the rules creates a new incident in response to an incoming event, Enterprise Manager finishes matching the event to any further rules/rule sets. Once completed, Enterprise Manager then matches the newly created incident to all the rule sets from the beginning to see if any incident-specific rules match.
- If an incoming event is already associated with an incident (for example, a *Warning* event creates an incident and then a *Critical* event is generated for the same issue), Enterprise Manager applies all the matching rules to the event and then matches all rules to the incident.
- If, while applying a rule to an incident, changes are made to the incident (change priority. for example), Enterprise Manager stops rule application at that point and then re-applies the rules to the incident from the beginning. The conditional action that updated the incident will not be matched again in the same rule application cycle.

3.1.4.3.2 Rule Criteria

The following tables list selectable criteria for each type.

Table 3–3 Rule Criteria: Events

Criteria	Description
Type	Rule applies to a specific event type.
Severity	Rule applies to a specific event severity.
Category	Rule applies to a specific event category.
Target type	Rule applies to a specific target type.
Target Lifecycle Status	Rule applies to a specific lifecycle status for a target. Lifecycle status is a target property that specifies a target's operational status.
Associated with incident	Typically, events are associated with incidents through rules. Specify Yes or No.
Event name	Rule applies to events with a specific name. The specified name can either be an exact match or a pattern match.
Causal analysis update	Upon completion of Root Cause Analysis (RCA) event, the rule applies to the event that is marked either as root cause or symptom. Alternatively, the rule can act on an RCA event when it is no longer a symptom.
Associated incident acknowledged	Rule applies to an event that is associated with a specific incident when that incident is acknowledged by an administrator. Specify Yes or No.
Total occurrence count	For duplicated events, the rule is applies when the total number of event occurrences reaches a specified number.
Comment added	Rule applies to events where an administrator adds a comment.

For incidents, a rule can apply to all new and/or updated incidents, or newly created incidents that match specific criteria shown in the following table.

Table 3–4 Rule Criteria: Incidents

Criteria	Description
Rules that created the incident	Rule applies to incidents raised by a specific rule.
Category	Rule applies to a specific incident category.
Target Type	Rule applies to a specific target type.
Target Lifecycle Status	Rule applies to a specific lifecycle status for a target. Lifecycle status is a target property that specifies a target's operational status.
Severity	Rule applies to a specific incident severity.
Acknowledged	Rule applies if the incident has been acknowledged by an administrator. Specify Yes or No.
Owner	Rule applies for a specified incident owner.
Priority	Rule applies when incident priority matches a selected priority.
Status	Rule applies when the incident status matches a selected incident status.
Escalation Level	Rule applies when the incident escalation level matches the selected level. Available escalation levels: None, Level 1, Level 2, Level 3, Level 4, Level 5
Associated with Ticket	Rule applies when the incident is associated with a helpdesk ticket. Specify Yes or No.
Associated with Service Request	Rule applies when the incident is associated with a service request. Specify Yes or No.
Diagnostic Incident	Rule applies when the incident is a diagnostic incident. Specify Yes or No.
Unassigned	Rule applies if the newly raised incident does not have an owner.
Comment Added	Rule applies if an administrator adds a comment to the incident.

For problems, a rule can apply to all new and/or updated problems, or newly created problems that match specific criteria shown in the following table.

Table 3–5 Rule Criteria: Problems

Criteria	Description
Problem key	Each problem has a problem key, which is a text string that describes the problem. It includes an error code (such as ORA 600) and in some cases, one or more error parameters. Rule can apply to a specific problem key or a key matching a specific pattern (using a wildcard character).
Category	Rule applies to a specific problem category.
Target Type	Rule applies to a specific target type.
Target Lifecycle Status	Rule applies to a specific lifecycle status for a target. Lifecycle status is a target property that specifies a target's operational status.
Acknowledged	Rule applies when the problem is acknowledged.
Owner	Rule applies for a specified problem owner.
Priority	Rule applies when problem priority matches a selected priority.

Table 3–5 (Cont.) Rule Criteria: Problems

Criteria	Description
Status	Rule applies when the problems matches a specific status.
Escalation Level	Rule applies when the problem escalation level matches the selected level. Available escalation levels: None, Level 1, Level 2, Level 3, Level 4, Level 5
Incident Count	Rule applies when the number of incidents related to the problem reaches the specified count limit. The problem owner and the Operations manager are notified via email.
Associated with Service Request	Rule applies if the incoming problem is has an associated Service Request. Specify Yes or No.
Associated with Bug	Rule applies if the incoming problem is has an associated bug. Specify Yes or No.
Unassigned	Rule applies if the newly raised incident does not have an owner.
Comment Added	Rule applies if an administrator adds a comment to the problem.

3.1.4.3.3 Rule Actions For each rule, Enterprise Manager allows you to define specific actions.

Some examples of the types of actions that a rule set can perform are:

- Create an incident based on an event.
- Perform notification actions such as sending an email or generating a helpdesk ticket.
- Perform actions to manage incident workflow notification via email/PL/SQL methods/ SNMP traps. For example, if a target down event occurs, create an incident and email administrator Joe about the incident. If the incident is still open after two days, set the escalation level to one and email Joe's manager.

The following table summarizes available actions for each rule application.

Table 3–6 Available Rule Actions

Action	Event	Incident	Problem
Email	Yes	Yes	Yes
Page	Yes	Yes	Yes
Advanced Notifications			
Send SNMP Trap	Yes	No	No
Run OS Command	Yes	Yes	Yes
Run PL/SQL Procedure	Yes	Yes	Yes
Create an Incident	Yes	No	No
Set Workflow Attributes	Yes Note: Within an event rule, the workflow attributes of the associated incident can also be updated.	Yes	Yes

Table 3–6 (Cont.) Available Rule Actions

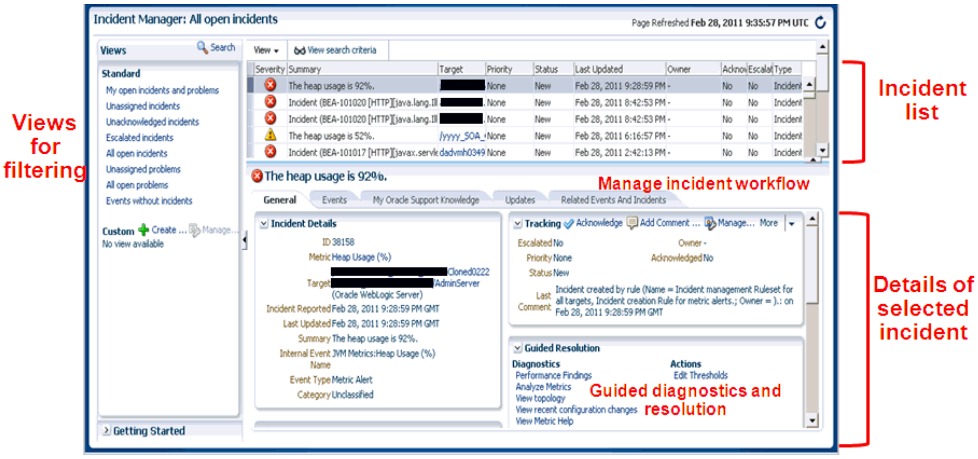
Action	Event	Incident	Problem
Create a Helpdesk Ticket	Yes Note: Action performed indirectly by first creating an incident and then creating a ticket for the incident.	Yes	No

3.1.5 Incident Manager

Incident Manager provides, in one location, the ability to search, view, manage, and resolve incidents and problems impacting your environment. Use Incident Manager to perform the following tasks:

- Filter incidents, problems, and events by using custom views
- Search for specific incidents by properties such as target name, summary, status, or target lifecycle status
- Respond and work on an incident
- Manage incident lifecycle including assigning, acknowledging, tracking its status, prioritization, and escalation
- Access (in context) My Oracle Support knowledge base articles and other Oracle documentation to help resolve the incident.
- Access direct in-context diagnostic/action links to relevant Enterprise Manager functionality allowing you to quickly diagnose or resolve the incident.

Figure 3–4 incident Manager



Severity	Summary	Target	Priority	Status	Last Updated	Owner	Acknow	Escalat	Type
✕	The heap usage is 92%.	[redacted]	None	New	Feb 28, 2011 9:28:59 PM	-	No	No	Incident
✕	Incident (BEA-101020 [HTTP][java.lang.Il	[redacted].	None	New	Feb 28, 2011 8:42:53 PM	-	No	No	Incident
✕	Incident (BEA-101020 [HTTP][java.lang.Il	[redacted].	None	New	Feb 28, 2011 8:42:53 PM	-	No	No	Incident
⚠	The heap usage is 52%.	/yyyy_SOA_	None	New	Feb 28, 2011 6:16:57 PM	-	No	No	Incident
✕	Incident (BEA-101017 [HTTP][javax.servl	dadvmh0349	None	New	Feb 28, 2011 2:42:13 PM	-	No	No	Incident

The heap usage is 92%.

Incident Details

ID 38158
Metric Heap Usage (%)
Target [redacted]Cloned0222 [redacted]/AdminServer (Oracle WebLogic Server)
Incident Reported Feb 28, 2011 9:28:59 PM GMT
Last Updated Feb 28, 2011 9:28:59 PM GMT
Summary The heap usage is 92%.
Internal Event Name JVM Metrics:Heap Usage (%)
Event Type Metric Alert
Category Unclassified

Tracking

Escalated No
Owner -
Priority None
Acknowledged No
Status New
Last Comment Incident created by rule (Name = Incident management Ruleset for all targets, Incident creation Rule for metric alerts.; Owner =).: on Feb 28, 2011 9:28:59 PM GMT

For example, you have an open incident. You can use Incident Manager to track its ownership, its resolution status, set the priority and, if necessary, add annotations to the incident to share information with others when working in a collaborative environment. In addition, you have direct access to pertinent information from MOS and links to other areas of Enterprise Manager that will help you resolve issues quickly. By drilling down on an open incident, you can access this information and modify it accordingly.

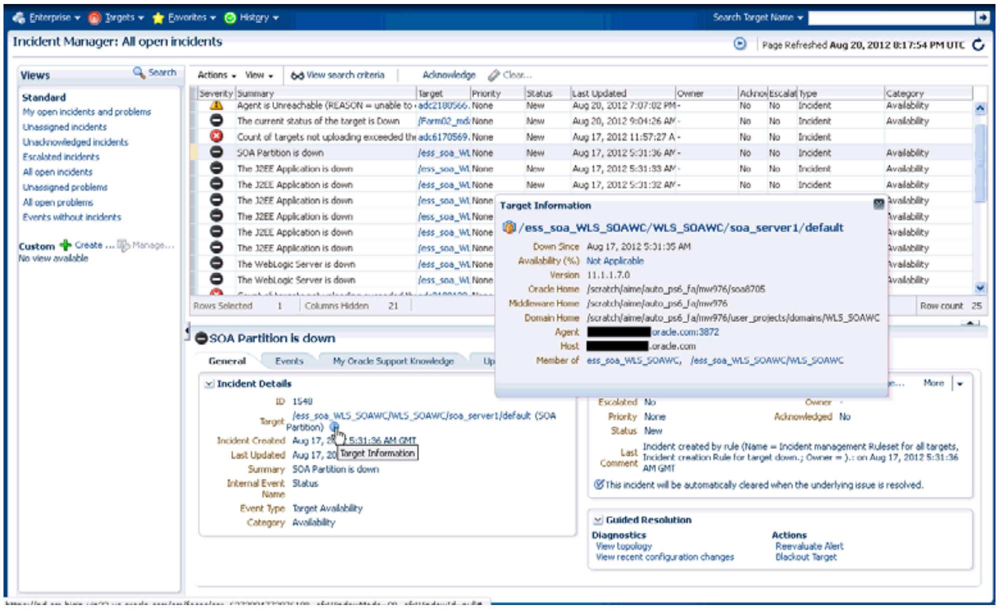
Displaying Target Information in the Context of an Incident

You can directly view information about a target for which an incident or event has been raised. The type of information shown varies depending on the target type.

To display in-context target information:

1. From the **Enterprise** menu, select **Monitoring** and then **Incident Manager**.
2. From the Incident Manager UI, choose an incident. Information pertaining to the incident displays.
3. From the Incident Details area of the General tab, click on the information icon "i" next to the *target*. Target information as it pertains to the incident displays. See Figure 3–5

Figure 3–5 Target Information in Context of an Incident



Incident Manager: All open incidents

Page Refreshed **Aug 20, 2012 8:17:54 PM UTC**

Severity	Summary	Target	Priority	Status	Last Updated	Owner	Acknov	Escalat	Type	Category
⚠	Agent is Unreachable (REASON = unable to	adc2100566.	None	New	Aug 20, 2012 7:07:02 PM	-	No	No	Incident	Availability
⊖	The current status of the target is Down	/Farm02_md	None	New	Aug 20, 2012 9:04:26 AM	-	No	No	Incident	Availability
⊗	Count of targets not uploading exceeded th	adc6170569.	None	New	Aug 17, 2012 11:57:27 A	-	No	No	Incident	
⊖	SOA Partition is down	/ess_soa_WL	None	New	Aug 17, 2012 5:31:36 AM	-	No	No	Incident	Availability
⊖	The J2EE Application is down	/ess_soa_WL	None	New	Aug 17, 2012 5:31:33 AM	-	No	No	Incident	Availability
⊖	The J2EE Application is down	/ess_soa_WL	None	New	Aug 17, 2012 5:31:32 AM	-	No	No	Incident	Availability
⊖	The J2EE Application is down	/ess_soa_WL	None							vailability
⊖	The J2EE Application is down	/ess_soa_WL	None							vailability
⊖	The J2EE Application is down	/ess_soa_WL	None							vailability
⊖	The J2EE Application is down	/ess_soa_WL	None							vailability
⊖	The WebLogic Server is down	/ess_soa_WL	None							vailability
⊖	The WebLogic Server is down	/ess_soa_WL	None							vailability

Rows Selected 1 Columns Hidden 21 Row count 25

Target Information

/ess_soa_WLS_SOAWC/WLS_SOAWC/soa_server1/default

Down Since	Aug 17, 2012 5:31:35 AM
Availability (%)	Not Applicable
Version	11.1.1.7.0
Oracle Home	/scratch/aime/auto_ps6_fa/mw976/soa8705
Middleware Home	/scratch/aime/auto_ps6_fa/mw976
Domain Home	/scratch/aime/auto_ps6_fa/mw976/user_projects/domains/WLS_SOAWC
Agent	[redacted]oracle.com:3872
Host	[redacted].oracle.com
Member of	ess_soa_WLS_SOAWC, /ess_soa_WLS_SOAWC/WLS_SOAWC

SOA Partition is down

Incident Details

ID	1540
Target	/ess_soa_WLS_SOAWC/WLS_SOAWC/soa_server1/default (SOA Partition)
Incident Created	Aug 17, 2 5:31:36 AM GMT
Last Updated	Aug 17, 20
Summary	SOA Partition is down
Internal Event Name	Status
Event Type	Target Availability
Category	Availability

Target Information

Escalated	No	Owner	-
Priority	None	Acknowledged	No
Status	New		
Last Comment	Incident created by rule (Name = Incident management Ruleset for all targets, Incident creation Rule for target down.; Owner =).: on Aug 17, 2012 5:31:36 AM GMT		

This incident will be automatically cleared when the underlying issue is resolved.

Guided Resolution

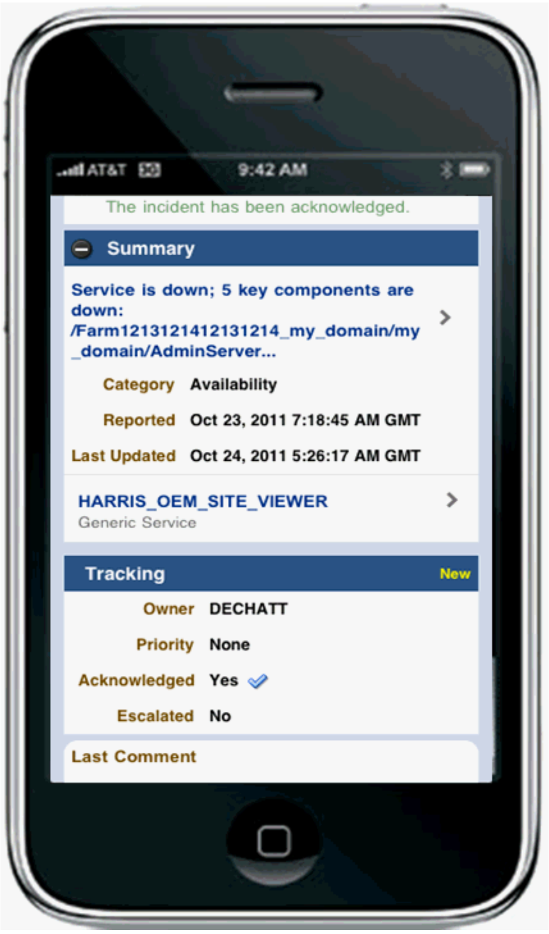
Diagnostics	Actions
View topology	Reevaluate Alert
View recent configuration changes	Blackout Target

Being able to display target information in this way provides you with more operational context about the targets on which the events and incidents are raised. This in turn helps you manage the lifecycle of the incident more efficiently.

Cloud Control Mobile

Also available is the mobile application Cloud Control Mobile, which lets you manage incidents and problems on the go using any iDevice to remotely connect to Enterprise Manager.

Figure 3–6 Cloud Control Mobile



The incident has been acknowledged.

Summary

Service is down; 5 key components are down: /Farm1213121412131214_my_domain/my_domain/AdminServer...

Category Availability

Reported Oct 23, 2011 7:18:45 AM GMT

Last Updated Oct 24, 2011 5:26:17 AM GMT

HARRIS_OEM_SITE_VIEWER
Generic Service

Tracking New

Owner DECHATT

Priority None

Acknowledged Yes ✓

Escalated No

Last Comment

For more information about this mobile application, see Chapter 28, "Remote Access To Enterprise Manager"

3.1.5.1 Views

Views let you work efficiently with incidents by allowing you to categorize and focus on only those incidents of interest. A view is a set of search criteria for filtering incidents and problems in the system. Incident Manager provides a set of predefined *standard* views that cover the most common event, incident, and problem search scenarios. In addition, Incident Manager also allows you to create your own custom views. Custom views can be shared with other users. For instructions on creating custom views, see "Setting Up Custom Views" on page 3-45. For instructions on sharing a custom view, see "Sharing/Unsharing Custom Views" on page 3-46.

3.1.6 Summing Up

- **Event**: A significant occurrence of interest on a target that has been detected by Enterprise Manager.

  Goal: Ensure that your environment is monitored.

- **Incident**: A set of significant events or combination of related events that pertain to the same issue.

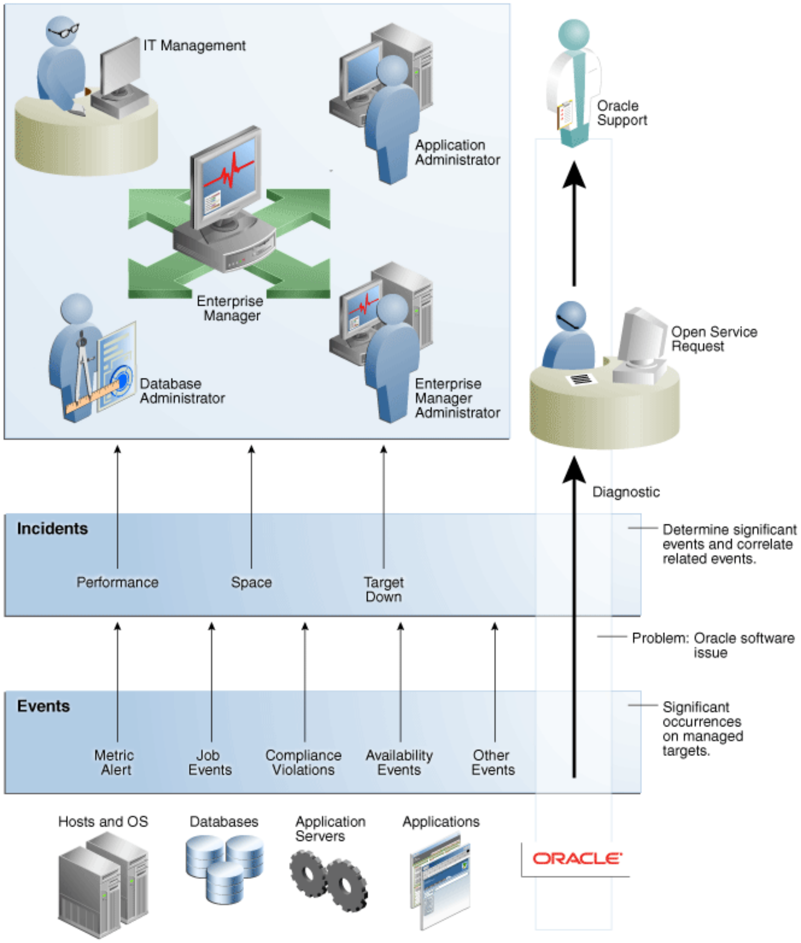
  Goal: Ensure that service disruptions are either avoided or resolved quickly.

- **Problems**: The underlying root cause of incidents. Currently, this represents critical errors in Oracle software that represents the underlying root cause of diagnostic incidents.

  Goal: Ensure underlying root causes of issues are resolved to avoid future occurrence of issues.

Events, incidents, and problems work in concert to allow you to manage your complete IT ecosystem both effectively and efficiently. The following illustration summarizes how they work within your managed environment.

Figure 3–7 Event/Incident/Problem Flow



The following sections delve into events, incidents, and problems in more detail.

3.2 Setting Up Your Incident Management Environment

Before you can monitor and manage your environment using incidents, you must ensure that your monitoring environment is properly configured. Proper configuration consists of the following:

- Setting Up Your Monitoring Infrastructure
- Setting Up Notifications
- Setting Up Administrators and Privileges

3.2.1 Setting Up Your Monitoring Infrastructure

The first step in setting up your monitoring infrastructure is to determine which conditions need to be monitored and hence are the source of events. To prevent an inordinate number of extraneous events from being generated, thus reducing system and administrator overhead, you need to determine what is of interest to you and enable monitoring based on your requirements. You can leverage Enterprise Manager features such as Administrations Groups to automatically apply management settings such as monitoring settings or compliance standards when new targets are added to your monitored environment. This greatly simplifies the task of ensuring that events are raised only for those conditions in which you are interested. For more information, see Chapter 7, "Using Administration Groups".

Example: You want to ensure that the database containing your human resource information is available round the clock. One condition you are monitoring for is whether that database target is up or down. If it goes down, you want the appropriate person to be notified and have them resolve the problem as quickly as possible. Other conditions that you may want to monitor include performance threshold violations, any changes in application configuration files, or job failures. Working with events, you are monitoring and managing individual targets and issues directly related to those targets. For example, you monitor for individual database availability, individual host threshold violations such as CPU and I/O load, or perhaps the performance of a Web service.

In general, if you are primarily interested in availability and some key performance related metrics, you should use default monitoring templates and other template features to ensure the only those specific metrics are collected and events are raised only for those metrics.

Job Events: The status of a job can change throughout its lifecycle - from the time it is submitted to the time it has executed. For each of these job statuses, events can be raised to notify administrators of the status of the job.

As a general rule, events should be generated only for job status values that require administration attention. These job status values include Action Required and Problem status values such as Failed or Stopped. However, in order to avoid overloading the system with unnecessary events, job events are not enabled for any target by default. Hence, if you would like to generate events for jobs, you must:

1. Set the appropriate job status. You can use the default settings or modify them as required.
2. Specify the set of targets for which you would like job-related events to be generated.

   You can perform these operations from the *Job Event Generation Criteria* page. From the **Setup** menu, choose **Incidents** and then **Job Events**.

3.2.1.1 Rule Set Development

Before creating incident rules/rule sets, the first step is to strategically determine when incidents should be created based on the business requirements of your organization. Important questions to consider are:

1. What events should create incidents? Which service disruptions need to be tracked and resolved by IT administrators?
2. Which administrators should be notified for incoming events or incidents?
3. Are any of the events or incidents being forwarded to external systems (such as a helpdesk ticketing system)?

Once the exact business requirements are understood, you translate those into enterprise rule sets. Adhering to the following guidelines will result in efficient use of system resource as well as operational efficiency.

- For rule sets that operate on targets (for example, hosts and databases), use groups to consolidate targets into a smaller number of monitoring entities for the rule set. Groups should be composed of targets that have similar monitoring requirements including incident management and response.
- All the rules that apply to the same groups of targets should be consolidated into one rule set. You can create multiple rules that apply to the targets in the rule set. You can create rules for events specific to an event class, rules that apply to events of a specific event class and target type, or rules that apply to incidents on these targets.
- Leverage the execution order of rules within the rule set. Rule sets and rules within a rule set are executed in sequential order. Therefore, ensure that rules and rule sets are sequenced with that in mind.

Event rules that create incidents

When creating a new rule, you are given a choice as to what object the rule will apply— events, incidents or problems. Use the following rule usage guidelines to help guide your selection.

Incident notificaion

Incident escalatin

Table 3–7 Rule Usage Guidelines

Rule Usage	Application
Rules on Event	To create incidents for the events managed in Enterprise Manager.
	To send notifications on events.
	To create tickets for incidents managed by helpdesk analysts, you want to create an incident for an event, then create a ticket for the incident.
	Send events to third-party management systems.
Rules on Incidents	Automate management of incident workflow operations (assign owner, set priority, escalation levels..) and send notifications
	Create tickets based on incident conditions. For example, create a ticket if the incident is escalated to level 2.
Rules on Problems	Automate management of problem workflow operations (assign owner, set priority, escalation levels..) and send notifications

Rule Set Example

The following example illustrates many of the implementation guidelines just discussed. All targets have been consolidated into a single group, all rules that apply to group members are part of the same rule set, and the execution order of the rules has been set. In this example, the rule set applies to a group (Production Group G) that consists of the following targets:

- DB1 (database)
- Host1 (host)
- WLS1 (WebLogic Server)

All rules in the rule set perform three types of actions: incident creation, notification, and escalation.

Example 3–1 ***Example Rule Set***

- Rule Set applies to target: Group Target G
- Rules in the Rule Set:
  1. Rule(s) to create incidents for specified events
  2. Rule(s) that send notifications on incidents
  3. Rule(s) that escalate incidents based on some condition. For example, the length of time an incident is open.

In a more detailed view of the rule set, we can see how the guidelines have been followed.

Example 3–2 ***Example Rule Set in Greater Detail***

- Rule Set for Production Group G
  - Target: Production Group G
  - Rule 1: Create an incident for all *target down* events.
  - Rule 2: Create an incident for specific database, host, and WebLogic Server metric alert event of critical or warning severity.
  - Rule 3: Create an incident for any problem job events.
  - Rule 4: For all critical incidents, sent a page. For all warning incidents, send email.
  - Rule 5: If a Fatal incident is open for more than 12 hours, set the excalation level to 1 and email a manager.

In this detailed view, there are five rules that apply to all group members. The execution sequence of the rules (rule 1 - rule 5) has been leveraged to correspond to the three types of rule actions in the rule set: Rules 1-3

- Rules 1-3: Incident Creation
- Rule 4: Notification
- Rule 5: Escalation

By synchronizing rule execution order with the progression of rule action categories, execution efficiency is achieved. As shown in this example, by using conditional actions that take different actions for the same set of events based on severity, it is easier to change the event selection criteria in the future without having to change multiple rules. **Note**: This assumes that the action requirements for all incidents (from rules 1 - 3) are the same.

The following table illustrates explicit rule set operation for this example.

Table 3–8 ***Example Rule Set for Production Group G***

Rule Name	Execution Order	Criteria	Action	
			Condition	Actions
		Rule Set: Targets within Production Group G		
Rule 1	First	DB1 goes down . Host1 goes down. WLS1 goes down.		Create incident.

Table 3–8 (Cont.) Example Rule Set for Production Group G

Rule Name	Execution Order	Criteria	Action	
			Condition	Actions
Rule 2	Second	**DB1**	If severity=Warning	Create incident.
		Tablespace Full (%)	If severity=Critical	
		Note: The warning and critical thresholds are defined in Metric and Policy settings, not from the rules UI.		
		Host1		
		CPU Utilization (%)		
		WLS1		
		Heap Usage (%)		
Rule 3	Third	Event generated for problem job status changes for DB1, Host1, and WLS1.		Create incident.
Rule 4	Fourth	All incidents for Production Group G	Severity=Warning	Send email
			Severity=Critical	Send page
Rule 5	Fifth	Incident remains open for more than 12 days.	Status=Fatal	Increase escalation level to 1.

3.2.1.1.1 Before Using Rules Before you use rules, ensure the following prerequisites have been set up:

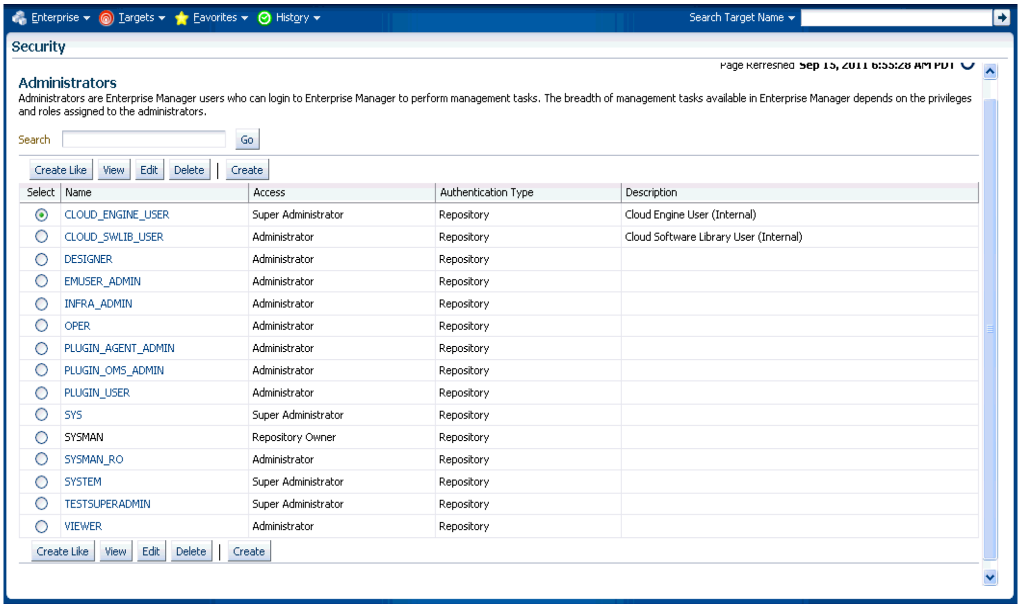
- User’s Enterprise Manager account has notification preferences (email and schedule). This is required not just for the administrator who is creating/editing a rule, but also for any user who is being notified as a result of the rule action.
- If you decide to use connectors, tickets, or advanced notifications, you need to configure them before using them in the actions page.
- Ensure that the SMTP gateway has been properly configured to send email notifications.
- User’s Enterprise Manager account has been granted the appropriate privileges to manage incidents from his managed system.

3.2.1.1.2 Setting Up Notifications After determining which events should be raised for your monitoring environment, you need to establish a comprehensive notification infrastructure for your enterprise by configuring Enterprise Manager to send out email and or pages, setting up email addresses for administrators and tagging them as email/paging. In addition, depending on the needs of your organization, notification setup may involve configuring advanced notification methods such as OS scripts, PL/SQL procedures, or SNMP traps. For detailed information and setup instructions for Enterprise Manager notifications, see Chapter 4, "Using Notifications".

3.2.2 Setting Up Administrators and Privileges

This step involves defining the appropriate administrators (which includes assigning the proper privileges for security) and then setting up notification assignments based on their defined roles and domain ownership within your organization.

To perform user account administration, click **Setup** on the Enterprise Manager home page, select **Security**, then select **Administrators** to access the Administrators page.



Security

Page Refreshed **Sep 15, 2011 6:55:28 AM PDT**

Administrators

Administrators are Enterprise Manager users who can login to Enterprise Manager to perform management tasks. The breadth of management tasks available in Enterprise Manager depends on the privileges and roles assigned to the administrators.

Search

Select	Name	Access	Authentication Type	Description
●	CLOUD_ENGINE_USER	Super Administrator	Repository	Cloud Engine User (Internal)
○	CLOUD_SWLIB_USER	Administrator	Repository	Cloud Software Library User (Internal)
○	DESIGNER	Administrator	Repository	
○	EMUSER_ADMIN	Administrator	Repository	
○	INFRA_ADMIN	Administrator	Repository	
○	OPER	Administrator	Repository	
○	PLUGIN_AGENT_ADMIN	Administrator	Repository	
○	PLUGIN_OMS_ADMIN	Administrator	Repository	
○	PLUGIN_USER	Administrator	Repository	
○	SYS	Super Administrator	Repository	
○	SYSMAN	Repository Owner	Repository	
○	SYSMAN_RO	Administrator	Repository	
○	SYSTEM	Super Administrator	Repository	
○	TESTSUPERADMIN	Super Administrator	Repository	
○	VIEWER	Administrator	Repository	

There are two types of administrators typically involved in incident management.

- *Business Rules Architect/Analyst*: Administrator who has a deep understanding of how the business works and translates this knowledge to operational rules. Once these rules have been deployed, the business architect uses their knowledge of the dynamic organization to keep these rules up-to-date.

  In order to create or edit an enterprise rule set, the business architect/analyst must have been granted the *Create Enterprise Rule Set* privilege on the *Enterprise Rule Set* resource. The architect/analyst can share ownership of the rule sets with other administrators who may or may not have the *Create Enterprise Rule Set* privilege but are responsible for managing a specific rule set.

- *IT Operator/Manager*: The IT manager is responsible for day-to-day management of incident assignment. The IT operator is assigned the incidents and is responsible for their resolution.

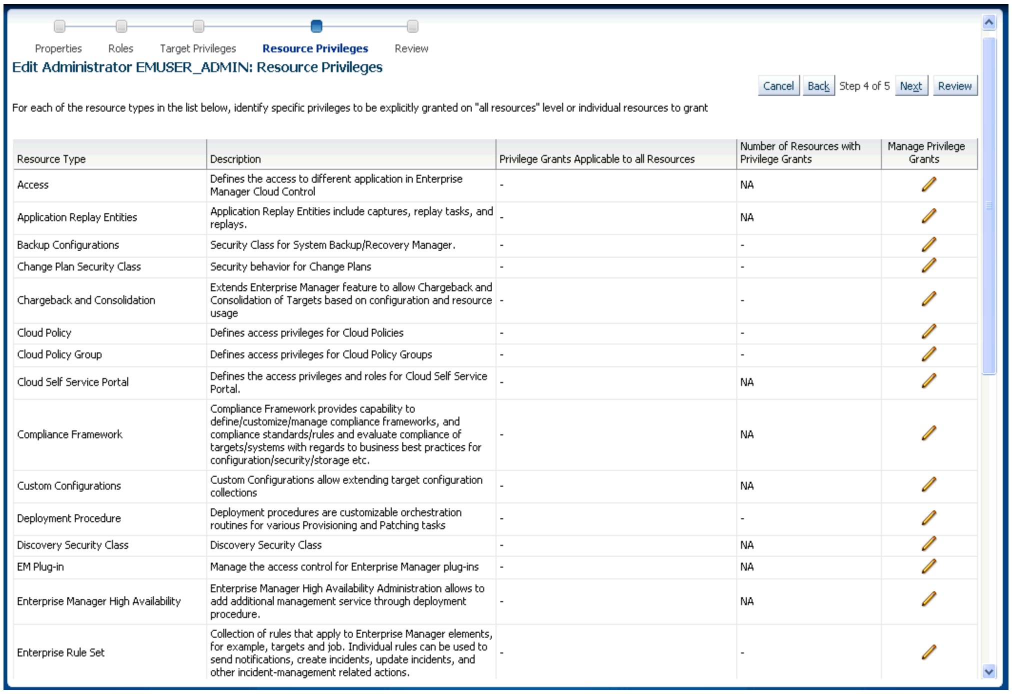
Privileges Required for Enterprise Rule Sets

As the owner of the rule set, an administrator can perform the following:

- Update or delete the rule set, and add, modify, or delete the rules in the rule set.
- Assign co-authors of the rule set. Co-authors can edit the rule set the same as the author. However, they cannot delete rule sets nor can they add additional co-authors.
- When a rule action is to update an event, incident, or problem (for example, change priority or clear an event), the action succeeds only if the owner has the privilege to take that action on the respective event, incident, or problem.
- Additionally, user must be granted privilege to create an enterprise rule set.

If an incident or problem rule has an update action (for example, change priority), it will take the action only if the owner of the respective rule set has manage privilege on the matching incident or problem.

To grant privileges, from the **Setup** menu on the Enterprise Manager home page, select **Security**, then select **Administrators** to access the Administrators page. Select an administrator from the list, then click **Edit** to access the Administrator properties wizard as shown in the following graphic.



Edit Administrator EMUSER_ADMIN: Resource Privileges

For each of the resource types in the list below, identify specific privileges to be explicitly granted on "all resources" level or individual resources to grant

Resource Type	Description	Privilege Grants Applicable to all Resources	Number of Resources with Privilege Grants	Manage Privilege Grants
Access	Defines the access to different application in Enterprise Manager Cloud Control	-	NA	✎
Application Replay Entities	Application Replay Entities include captures, replay tasks, and replays.	-	NA	✎
Backup Configurations	Security Class for System Backup/Recovery Manager.	-	-	✎
Change Plan Security Class	Security behavior for Change Plans	-	-	✎
Chargeback and Consolidation	Extends Enterprise Manager feature to allow Chargeback and Consolidation of Targets based on configuration and resource usage	-	-	✎
Cloud Policy	Defines access privileges for Cloud Policies	-	-	✎
Cloud Policy Group	Defines access privileges for Cloud Policy Groups	-	-	✎
Cloud Self Service Portal	Defines the access privileges and roles for Cloud Self Service Portal.	-	NA	✎
Compliance Framework	Compliance Framework provides capability to define/customize/manage compliance frameworks, and compliance standards/rules and evaluate compliance of targets/systems with regards to business best practices for configuration/security/storage etc.	-	NA	✎
Custom Configurations	Custom Configurations allow extending target configuration collections	-	NA	✎
Deployment Procedure	Deployment procedures are customizable orchestration routines for various Provisioning and Patching tasks	-	-	✎
Discovery Security Class	Discovery Security Class	-	NA	✎
EM Plug-in	Manage the access control for Enterprise Manager plug-ins	-	NA	✎
Enterprise Manager High Availability	Enterprise Manager High Availability Administration allows to add additional management service through deployment procedure.	-	NA	✎
Enterprise Rule Set	Collection of rules that apply to Enterprise Manager elements, for example, targets and job. Individual rules can be used to send notifications, create incidents, update incidents, and other incident-management related actions.	-	-	✎

Granting User Privileges for Events, Incidents and Problems

In order to work with incidents, all relevant Enterprise Manager administrator accounts must be granted the appropriate privileges to manage incidents. Privileges for events, incidents, and problems are determined according to the following rules:

- Privileges on events are calculated based on the privilege on the underlying source objects. For example, the user will have VIEW privilege on an event if he can view the target for the event.
- Privileges on an incident are calculated based on the privileges on the events in the incident.
- Similarly, problem privileges are calculated based on privileges on underlying incidents.

Users are granted privileges for events, incidents, and problems in the following situations.

For events, two privileges are defined in the system:

- The *View Event* privilege allows you to view an event and add comments to the event.
- The *Manage Event* privilege allows you to take update actions on an event such as closing an event, creating an incident for an event, and creating a ticket for an event. You can also associate an event with an incident.

Important: Incident privilege is inherited from the underlying events.

If an event is raised on a target alone (the majority of event types are raised on targets such as metric alerts, availability events or service level agreement), you will need the following privileges:

- *View* on target to view the event.
- *Manage Target Events* to manage the event.

  Note: This is a sub-privilege of Operator.

If an event is raised on both a target and a job, you will need the following privileges:

- *View on target* and *View* on the job to view the event.
- *View on target* and *Full* on the job to manage the event.

If the event is raised on a job alone, you will need the following privileges:

- *View* on the job to view the event.
- *Full* on the job to manage the event.

If an event is raised on a metric extension, you will need *View* privilege on the metric extension to view the event. Because events raised on metric extensions are informational (and do not appear in Incident Manager) event management privileges do not apply in this situation.

If an event is raised on a Self-update, only system privilege is required. Self-update events are strictly informational.

For incidents, two privileges are defined in the system:

- The View Incident privilege allows you to view an incident, and add comments to the incident.
- The Manage Incident privilege allows you to take update actions on an incident. The update actions supported for an incident includes incident assignment and prioritization, resolution management, manually closing events, and creating tickets for incidents.

If an incident consists of a single event, you can view the incident if you can view the event and manage the incident if you can manage the event.

If an incident consists of more than one event, you can view the incident if you can view at least one event and manage incident if you can manage at least one of the events.

For problems, two privileges are defined:

- The View Problem privilege allows you to view a problem and add comments to the problem.
- The Manage Problem privilege allows you to take update actions on the problem. The update actions supported for a problem include problem assignment and prioritization, resolution management, and manually closing the problem.

In Enterprise Manager 12*c*, problems are always related to a single target. So the View Problem privilege, if an administrator has View privilege on the target, and the Manage Problem privilege, if an administrator has *manage_target_events* privilege on the target, implicitly grants management privileges on the associated event. This, in turn, grants management privileges on the incident within the problem.

3.2.3 Monitoring Privileges

The monitoring functions that an administrator can perform within the Enterprise Manager environment depend on privileges that have been granted to that user. To maintain the integrity and security of a monitored infrastructure, only the required privileges for a specific role should be granted. The following guidelines can be used to grant proper privilege levels based on user roles.

Administrators who set up monitoring

Create a role with privileges and grant it to administrators:

- Recommend using individual user accounts instead of shared account
- If using super administrator, do not use sysman
- If privilege is based on targets, create privilege-propagating group containing the targets (or use administration group if it meets requirements) and grant privilege on the group to the role

Administrators who respond to events / incidents

- Create a role and grant it to administrators
- Create privilege-propagating group (or use administration group if it meets requirements) containing relevant targets and grant appropriate privilege on the group to the role

Example: You create the role *DB_Admins* and grant *Manage Target Events* on a the privilege-propagating group named *DB-group* containing relevant databases. You then grant role DB_Admins to the DBAs.

Monitoring Actions and Required Privileges

Enterprise Manager supports fine-grained privileges to enable more granular control over actions performed in Enterprise Manager.

The table below shows a (non-exhaustive) list of various job responsibilities and the corresponding privilege in Enterprise Manager required to support these

The following tables summarize the privilege levels required to perform specific monitoring responsibilities.

Table 3–9 Monitoring Operations and Required Privileges

Monitoring Operation	Required Privilege(s)
Monitoring Setup	
Configure SMTP gateway (email)	Super Administrator
Create Advanced Notification Methods (e.g. SNMP traps)	Super Administrator
Configure event or ticketing connector	Super Administrator
Creating Roles	Super Administrator
Create Administration Group Hierarchy	Full Any Target Create Privilege Propagating Group

Table 3–9 (Cont.) Monitoring Operations and Required Privileges

Monitoring Operation	Required Privilege(s)
Edit Administration Group Hierarchy	Full Any Target Create Privilege Propagating Group (if adding new target property values as group criteria within a level of the administration group hierarchy)
Delete Administration Group Hierarchy	Full Any Target
View entire Administration Group hierarchy in Group Administration pages	View Any Target Note: Administrators who have privileges to only a subset of the groups can view these groups in the Groups list page accessible via Targets-->Groups
Use Monitoring Templates	No privileges required to create new monitoring templates. However if the monitoring template contains a corrective action, then Create on Job System privilege is required View on specific monitoring template to use the template created by another user (e.g. to add the monitoring template to a Template Collection
Use Template Collections	Create Template Collection (to create new Template Collections) View Template Collection on specific Template Collection to view/associate the Template Collection created by another user View Any Template Collection to view/associate any Template Collection Full Template Collection on specific Template Collection to edit/delete the Template Collection created by another user
Associate a Template Collection with an Administration Group	Manage Template Collection Operations on the group (this includes Manage Target Compliance and Manage Target Metrics privileges) View Template Collection on the Template Collection
Operations on the Administration Group	
Manage privileges on the group (for example, grant to other users)	Group Administration on the group
Add a target to an Administration Group by setting its target properties	Configure Target (on the target to be added to the Administration Group)
Perform a manual sync of the group with the associated Template Collection	Manage Template Collection Operations on the group

Table 3–9 (Cont.) Monitoring Operations and Required Privileges

Monitoring Operation	Required Privilege(s)
Operations on the members of the Administration Group	
Delete the target from Enterprise Manager	Full on the target (Full also contains the privileges enumerated below Operator on the target also contains the following privileges:
Set blackout for planned downtime	■ Blackout Target on the target
Change monitoring settings	■ Manage Target Metrics on the target
Change monitoring configuration	■ Configure Target on the target
Manage events and incidents on the target	■ Manage Target Events on the target
View target, receive notifications for events or incidents	■ View on the target
Create Incident Rule Sets	Create Enterprise Rule Set Manage Target Events on target if rule is creating incidents for the target
Granting privileges on administration group to roles	No extra privilege required if creator of the administration group
Set a target's property values	Configure Target
Edit Monitoring Template that is part of Template Collection	Full on the Monitoring Template Manage Target Metrics on administration group
Change monitoring settings on specific target	Manage Target Metrics
Receive email for events, incidents	View on Target and/or View on source object (for example, view on job for job events)
Create incident for event	Manage Target Events
Incident management actions (for example, acknowledge, assign incident, prioritize, set escalation level)	Manage Target Events

Note: SYSMAN is a system account intended for Enterprise Manager infrastructure installation and maintenance. It should never be used for administrator access to Enterprise Manager as a Super Administrator.

3.2.4 Setting Up Rule Sets

Rule sets automate actions in response to incoming events, incidents and problems or updates to them. This section covers the most common tasks and examples.

- Creating a Rule Set
- Creating a Rule to Create an Incident
- Creating a Rule to Manage Escalation of Incidents
- Creating a Rule to Escalate a Problem
- Testing Rule Sets
- Subscribing to Receive Email from a Rule
- Receiving Email for Private Rules

3.2.4.1 Creating a Rule Set

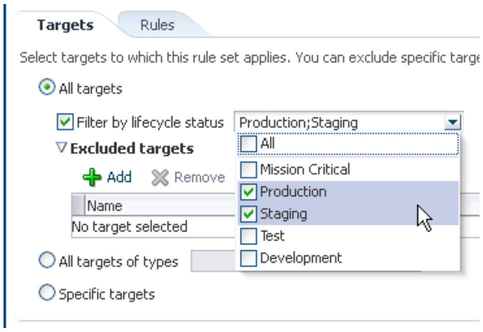
In general, to create a rule set, perform the following steps:

1. From the **Setup** menu, select **Incidents** then select **Incident Rules**.
2. On the Incident Rules - All Enterprise Rules page, edit the existing rule set or create a new rule set. For new rule sets, you will need to first select the targets to which the rules apply. Rules are created in the context of a rule set.

> **Note:** In the case where there is no existing rule set, create a rule set by clicking **Create Rule Set...** You then create the rule as part of creating the rule set.

Narrowing Rule Set Scope Based on Target Lifecycle Status

When creating a new rule set, you can choose to have the rule set apply to a narrower set of targets based on the target's *Lifecycle Status* value. For example, you can create one rule set that only applies only to targets that have a *Lifecycle Status* of *Staging* and *Production*. As shown in the following graphic, you determine rule set scope by setting the *Lifecycle Status* filter.



Select targets to which this rule set applies. You can exclude specific targe

● All targets

☑ Filter by lifecycle status: Production;Staging

▽ Excluded targets

Name
No target selected

○ All targets of types

○ Specific targets

Using this filter allows you to create rules for targets based on their *Lifecycle Status* without having to first create a group containing only such targets.

3. In the Rules tab of the Edit Rule Set page, click **Create...** and select the type of rule to create (Event, Incident, Problem) on the Select Type of Rule to Create pop-up dialog. Click **Continue**.
4. In the Create New Rule wizard, provide the required information.

5. Once you have finished defining the rule, click **Continue** to add the rule to the rule set. Click **Save** to save the changes made to the rule set.

3.2.4.2 Creating a Rule to Create an Incident

To create a rule that creates an incident, perform the following steps:

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. Determine whether there is an existing rule set that contains a rule that manages the event. In the **Incident Rules** page, use the Search option to find the rule/rule set name, description, target name, or target type for the target and the associated rule set. You can search by target name or the group target name to which this target belongs to locate the rule sets that manage the targets.

   Note: In the case where there is no existing rule set, create a rule set by clicking **Create Rule Set...** You then create the rule as part of creating the rule set.
3. Select the rule set that will contain the new rule. Click **Edit...** In the Rules tab of the Edit Rule Set page,

   1. Click **Create ...**
   2. Select "Incoming events and updates to events"
   3. Click **Continue**.

   Provide the rule details using the Create New Rule wizard.

   a. Select the Event Type the rule will apply to, for example, Metric Alert. (Metric Alert is available for rule sets of the type Targets.) **Note**: Only one event type can be selected in a single rule and, once selected, it cannot be changed when editing a rule.

      You can then specify metric alerts by selecting **Specific Metrics**. The table for selecting metric alerts displays. Click the **+Add** button to launch the metric selector. On the Select Specific Metric Alert page, select the target type, for example, Database Instance. A list of relevant metrics display. Select the ones in which you are interested. Click **OK**.

      You also have the option to select the severity and corrective action status.

   b. Once you have provided the initial information, click **Next**. Click **+Add** to add the actions to occur when the event is triggered. One of the actions is to **Create Incident**.

      As part of creating an incident, you can assign the incident to a particular user, set the priority, and create a ticket. Once you have added all the conditional actions, click **Continue**.

   c. After you have provided all the information on the Add Actions page, click **Next** to specify the name and description for the rule. Once on the Review page, verify that all the information is correct. Click **Back** to make corrections; click **Continue** to return to the Edit (Create) Rule Set page.

   d. Click **Save** to ensure that the changes to the rule set and rules are saved to the database.
4. Test the rule by generating a metric alert event on the metrics chosen in the previous steps.

3.2.4.3 Creating a Rule to Manage Escalation of Incidents

To create a rule to manage incident escalation, perform the following steps:

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. Determine whether there is an existing rule set that contains a rule that manages the incident. You can add it to any of your existing rule sets on incidents.

   Note: In the case where there is no existing rule set, create a rule set by clicking **Create Rule Set...** You then create the rule as part of creating the rule set.
3. Select the rule set that will contain the new rule. Click **Edit...** in the Rules tab of the Edit Rule Set page, and then:
   1. Click **Create ...**
   2. Select "Newly created incidents or updates to incidents"
   3. Click **Continue**.
4. For demonstration purposes, the escalation is in regards to a production database.

   As per the organization's policy, the DBA manager is notified for escalation level 1 incidents where a fatal incident is open for 48 hours. Similarly, the DBA director is paged if the incident has been escalated to level 2, the severity is fatal and it has been open for 72 hours. If the fatal incident is still open after 96 hours, then it is escalated to level 3 and the operations VP is notified.

   Provide the rule details using the Create New Rule wizard.

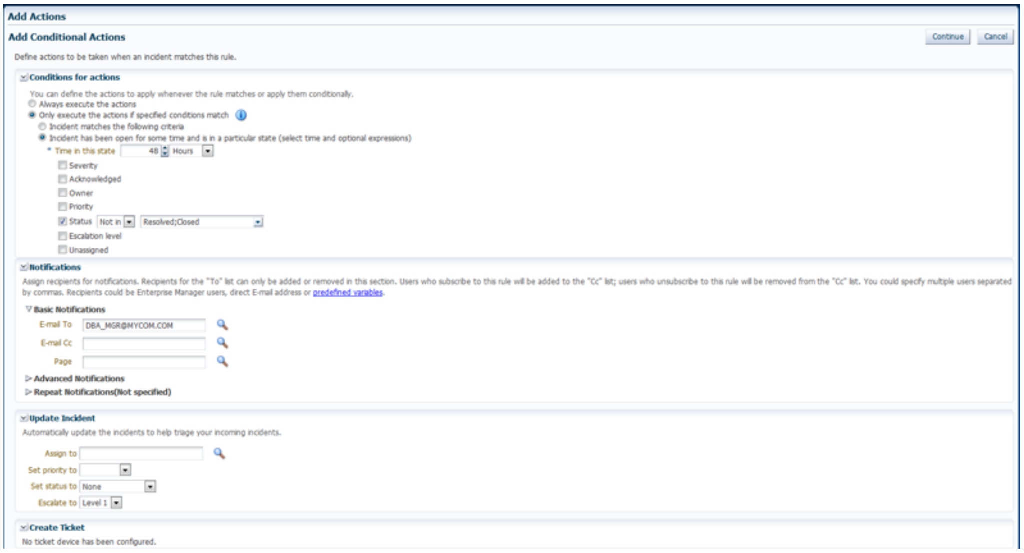
   a. To set up the rule to apply to all newly created incidents or when the incident is updated with *fatal* severity, select the **Specific Incidents** option and add the condition *Severity is Fatal* .

   b. In the **Conditions for Actions** region located on the Add Actions page, select **Only execute the actions if specified conditions match**.

      Select **Incident has been open for some time and is in a particular state (select time and optional expressions)**.

      Select the time to be 48 hours and Status is not resolved or closed.

   c. In the **Notification** region, type the name of the administrator to be notified by email or page. Click **Continue** to save the current set of conditions and actions.



Add Actions

Add Conditional Actions

Define actions to be taken when an incident matches this rule.

Conditions for actions

You can define the actions to apply whenever the rule matches or apply them conditionally.

○ Always execute the actions

● Only execute the actions if specified conditions match

○ Incident matches the following criteria

● Incident has been open for some time and is in a particular state (select time and optional expressions)

* Time in this state 48 Hours

□ Severity

□ Acknowledged

□ Owner

□ Priority

☑ Status Not in Resolved;Closed

□ Escalation level

□ Unassigned

Notifications

Assign recipients for notifications. Recipients for the "To" list can only be added or removed in this section. Users who subscribe to this rule will be added to the "Cc" list; users who unsubscribe to this rule will be removed from the "Cc" list. You could specify multiple users separated by commas. Recipients could be Enterprise Manager users, direct E-mail address or predefined variables.

Basic Notifications

E-mail To DBA_MGR@MYCOM.COM

E-mail Cc

Page

Update Incident

Automatically update the incidents to help triage your incoming incidents.

Assign to

Set priority to

Set status to None

Escalate to Level 1

Create Ticket

No ticket device has been configured.

   d. Repeat steps b and c to page the DBA director (Time in this state is 72 hours, Status is Not Resolved or Closed). If open for more than 96 hours, set escalation level to 3, page Operations VP.

   e. After reviewing added actions sets, click **Next**.

   f. Click **Next** to go to the Summary screen. Review the summary information and click **Continue** to save the rule.

5. Review the sequence of existing enterprise rules and position the newly created rule in the sequence.

   In Edit Rule Set page, click on the **desired rule from the Rules** table and select **Reorder Rules** from the **Actions** menu to reorder rules within the rule set, then click **Save** to save the rule sequence changes.

Example Scenario

To facilitate the incident escalation process, the administration manager creates a rule to escalate unresolved incidents based on their age:

- To level 1 if the incident is open for 30 minutes
- To level 2 if the incident is open for 1 hour
- To level 3 if the incident is open for 90 minutes

As per the organization's policy, the DBA manager is notified for escalation level 1. Similarly, the DBA director and operations VP are paged for incidents escalated to levels "2" and "3" respectively.

Accordingly, the administration manager inputs the above logic and the respective Enterprise Manager administrator IDs in a separate rule to achieve the above notification requirement. Enterprise Manager administrator IDs represents the respective users with required target privileges and notification preferences (that is, email addresses and schedule).

3.2.4.4 Creating a Rule to Escalate a Problem

In an organization, whenever an unresolved problem has more than 20 occurrences of associated incidents, the problem should be auto-assigned to the appropriate administrator based on target type of the target on which the problem has been raised.

Accordingly, a problem rule is created to observe the count of incidents attached to the problem and notify the appropriate administrator handling that specific target type.

The problem owner and the Operations manager are notified by email.

To create a rule to escalate a problem, perform the following steps:

1. Navigate to the Incident Rules page.

   From the **Setup** menu, select **Incidents**, then select **Incident Rules**.

2. On the Incident Rules - All Enterprise Rules page, either create a new rule set (click **Create Rule Set...**) or edit an existing rule set (highlight the rule set and click **Edit...**). Rules are created in the context of a rule set.

   Note: In the case where there is no existing rule set, create a rule set by clicking **Create Rule Set...** You then create the rule as part of creating the rule set.

3. In the Rules section of the Edit Rule Set page, select **Create...**

4. From the **Select Type of Rule to Create** dialog, select **Newly created problems or updates to problems** and click **Continue**.

5. On the Create New Rule page, select **Specific problems** and add the following criteria:

   The Attribute Name is **Incident Count**, the Operator is **Greater than or equals** and the Values is **20**.

   Click **Next**.

6. In the Conditions for Actions region on the Add Actions page select **Always execute the action**. As the actions to take when the rule matches the condition:

   - In the Notifications region, send email to the owner of the problem and to the Operations Manager.
   - In the Update Problem region, enter the email address of the appropriate administrator in the **Assign to** field.

   Click **Continue**.

7. Review the rules summary. Make corrections as needed. Click **Continue** to return to Edit Rule Set page and then click **Save** to save the rule set.

3.2.4.5 Testing Rule Sets

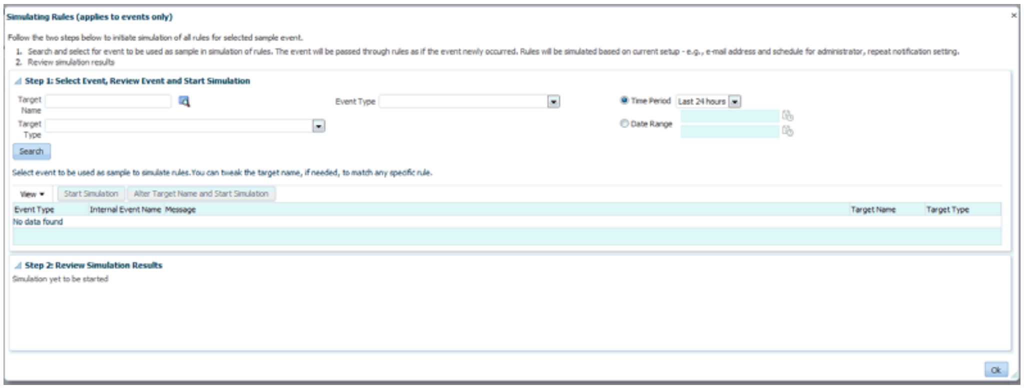
When developing a rule set, it can be difficult to develop rule criteria to match all possible event conditions. Previously, the only way to test rules was to trigger an event within your monitored environment and seeing which rules match the event and what actions the rules perform. Beginning with Enterprise Manager Release 12.1.0.4, you can simulate existing events, thus allowing you to test rule actions during the rule set development phase and not waiting for specific event conditions to occur. The rule simulation feature lets you see how the rules will perform given a specific event. You immediately see which rules match for a given event and then see what actions are taken.

> **Note:** The simulate rule feature can only be used with event rules
>
> Incident rules cannot be tested with this feature.

To simulate rules:

This procedure assumes you have already created rule sets. See "Creating a Rule Set" on page 3-33 for instructions on creating a rule set. Ensure that the rule type is *Incoming events and updates to events*.

1. From the Setup menu, select Incidents, and then Incident Rules. The *Incident Rules - All Enterprise Rules* page displays.
2. Click **Simulate Rules**. The Simulate Rules dialog displays.



Simulating Rules (applies to events only)

Follow the two steps below to initiate simulation of all rules for selected sample event.

1. Search and select for event to be used as sample in simulation of rules. The event will be passed through rules as if the event newly occurred. Rules will be simulated based on current setup - e.g., e-mail address and schedule for administrator, repeat notification setting.
2. Review simulation results

Step 1: Select Event, Review Event and Start Simulation

Target Name:

Target Type:

Event Type:

● Time Period: Last 24 hours

○ Date Range

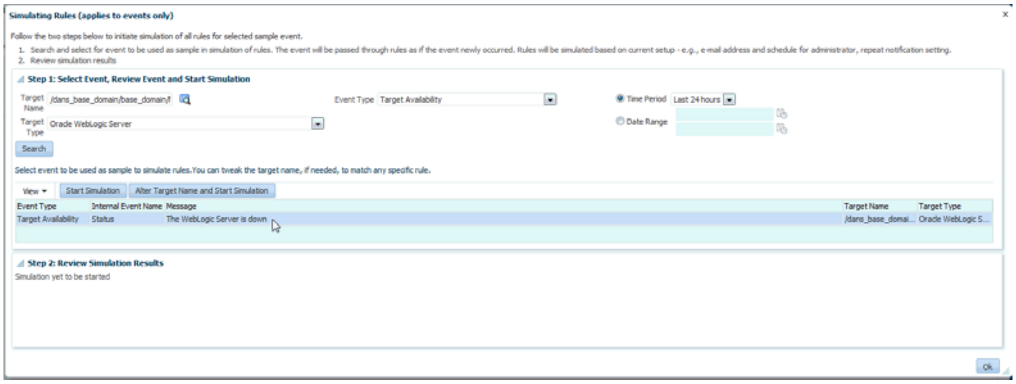
Select event to be used as sample to simulate rules.You can tweak the target name, if needed, to match any specific rule.

Event Type	Internal Event Name	Message	Target Name	Target Type
No data found				

Step 2: Review Simulation Results

Simulation yet to be started

3. Enter the requisite search parameters to find matching events and click **Search**.
4. Select an event from the list of results.



Simulating Rules (applies to events only)

Follow the two steps below to initiate simulation of all rules for selected sample event.

1. Search and select for event to be used as sample in simulation of rules. The event will be passed through rules as if the event newly occurred. Rules will be simulated based on current setup - e.g., e-mail address and schedule for administrator, repeat notification setting.
2. Review simulation results

Step 1: Select Event, Review Event and Start Simulation

Target Name: /dans_base_domain/base_domain/t

Target Type: Oracle WebLogic Server

Event Type: Target Availability

● Time Period: Last 24 hours

○ Date Range

Select event to be used as sample to simulate rules.You can tweak the target name, if needed, to match any specific rule.

Event Type	Internal Event Name	Message	Target Name	Target Type
Target Availability	Status	The WebLogic Server is down	/dans_base_domai...	Oracle WebLogic S...

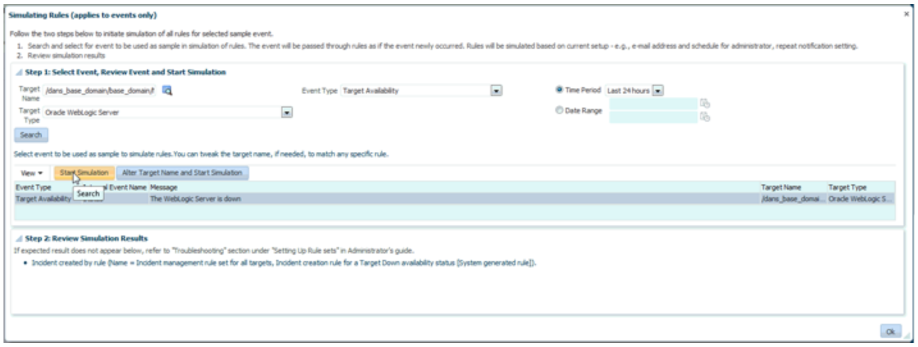
Step 2: Review Simulation Results

Simulation yet to be started

5. Click **Start Simulation**. The event will be passed through the rules as if the event had newly occurred. Rules will be simulated based on the current notification configuration (such as email address, schedule for the assigned administrator, or repeat notification setting).

   Changing the Target Name: Under certain circumstances, an event matching rule criteria may occur on a target that is not a rule target. For testing purposes, you are only interested in the event. To use the alternate target for the simulation, click **Alter Target Name and Start Simulation.**

   Results are displayed.



Simulating Rules (applies to events only)

Follow the two steps below to initiate simulation of all rules for selected sample event.

1. Search and select for event to be used as sample in simulation of rules. The event will be passed through rules as if the event newly occurred. Rules will be simulated based on current setup - e.g., e-mail address and schedule for administrator, repeat notification setting.
2. Review simulation results

Step 1: Select Event, Review Event and Start Simulation

Target Name: /dans_base_domain/base_domain/t

Target Type: Oracle WebLogic Server

Event Type: Target Availability

● Time Period: Last 24 hours

○ Date Range

Select event to be used as sample to simulate rules.You can tweak the target name, if needed, to match any specific rule.

Event Type	Internal Event Name	Message	Target Name	Target Type
Target Availability		The WebLogic Server is down	/dans_base_domai...	Oracle WebLogic S...

Step 2: Review Simulation Results

If expected result does not appear below, refer to "Troubleshooting" section under "Setting Up Rule sets" in Administrator's guide.

- Incident created by rule (Name = Incident management rule set for all targets, Incident creation rule for a Target Down availability status [System generated rule]).

6. If the rule actions are not what you intended, edit the rules and repeat the rule simulation process until the rules perform the desired actions.

3.2.4.6 Subscribing to Receive Email from a Rule

A DBA is aware that incidents owned by him will be escalated when not resolved in 48 hours. The DBA wants to be notified when the rule escalates the Incident. The DBA can subscribe to the Rule, which escalates the Incident and will be notified whenever the rule escalates the Incident.

Before you set up a notification subscription, ensure there exists a rule that escalates High Priority Incidents for databases that have not been resolved in 48 hours

Perform the following steps:

1. From the **Setup** menu, select **Incidents**, and then select **Incident Rules**.
2. On the Incident Rules - All Enterprise Rules page, click on the rule set containing incident escalation rule in question and click **Edit..**. Rules are created in the context of a rule set.

   Note: In the case where there is no existing rule set, create a rule set by clicking **Create Rule Set...** You then create the rule as part of creating the rule set.
3. In the Rules section of the Edit Rule Set page, highlight the escalation rule and click **Edit...**.
4. Navigate to the Add Actions page.
5. Select the action that escalates the incident and click **Edit...**
6. In the Notifications section, add the DBA to the **email cc** list.
7. Click **Continue** and then navigate back to the **Edit Rule Set** page and click **Save**.

As a result of the edit to the enterprise rule, when an incident stays unresolved for 48 hours, the rule marks it to escalation level 1. An email is sent out to the DBA notifying him about the escalation of the incident.

Alternate Rule Set Subscription Method: From the Incident Rules - All Enterprise Rules page, select the rule in incident rules table. From the **Actions** menu, select **email** and then **Subscribe me** (or **Subscribe administrator....**).

3.2.4.7 Receiving Email for Private Rules

A DBA has setup a backup job on the database that he is administering. As part of the job, the DBA has subscribed to email notification for "completed" job status. Before you create the rule, ensure that the DBA has the requisite privileges to create jobs. See Chapter 11, "Utilizing the Job System and Corrective Actions" for job privilege requirements.

Perform the following steps:

1. Navigate to the Rules page.

   From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. On the Incident Rules - All Enterprise Rules page, either edit an existing rule set (highlight the rule set and click **Edit...**) or create a new rule set.

   Note: The rule set must be defined as a Private rule set.
3. In the Rules tab of the Edit Rule Set page, select **Create...** and select **Incoming events and updates to events**. Click **Continue**.
4. On the Select Events page, select **Job Status Change** as the Event Type. Select the job in which you are interested either by selecting a specific job or selecting a job by providing a pattern, for example, Backup Management.

Add additional criteria by adding an attribute: Target Type as Database Instance.

5. Add conditional actions: Event matches the following criteria (Severity is Informational) and email Me for notifications.
6. Review the rules summary. Make corrections as needed. Click **Save**.
7. Create a database backup job and subscribe for email notification when the job completes.

When the job completes, Enterprise Manager publishes the informational event for "Job Complete" state of the job. The newly created rule is considered ’matching’ against the incoming job events and email will be sent to the DBA.

The DBA receives the email and clicks the link to access the details section in Enterprise Manager console for the event.

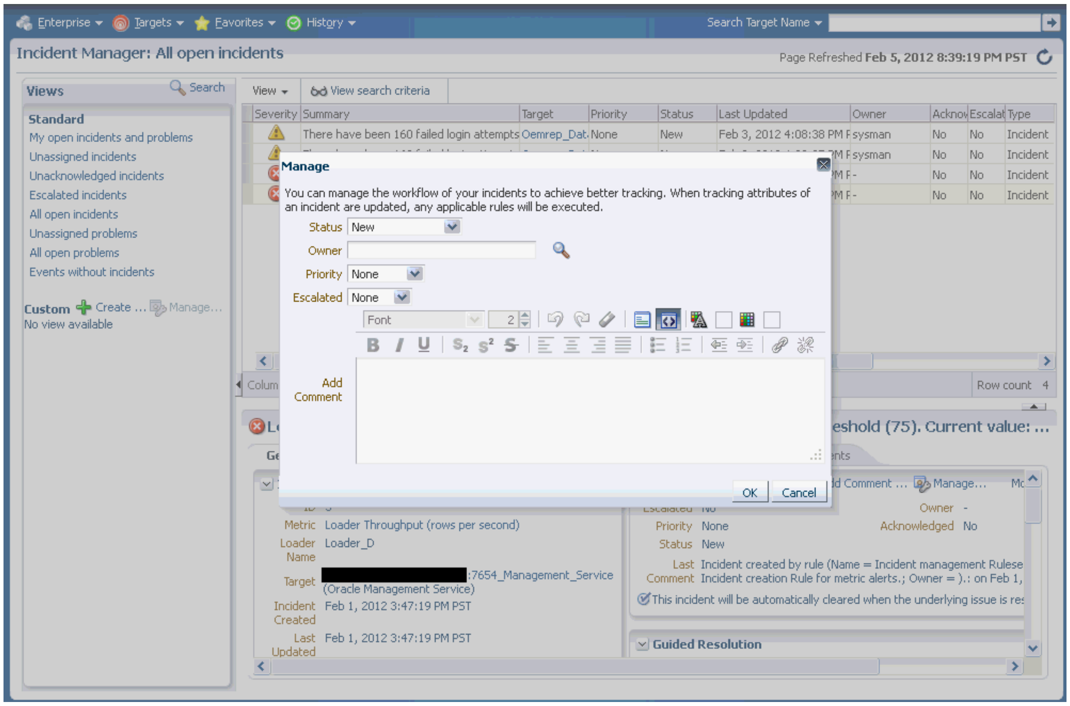
3.3 Working with Incidents

Data centers follow operational practices that enable them to manage events and incidents by business priority and in a collaborative manner. Enterprise Manager provides the following features to enable this management and automation:

- Send notifications to the appropriate administrators.
- Create incidents and rules.
- Assigning initial ownership of an incident and perhaps transferring ownership based on shift assignments or expertise.
- Tracking its resolution status.
- Assigning priorities based on the component affected and nature of the incident.
- Escalating incidents.
- Accessing My Oracle Support knowledge articles.
- Opening Oracle Service Requests to request assistance with issues with Oracle software (Problems).

You can update resolution information for an incident by performing the following:

1. In the **All Open Incidents** view, select the incident.
2. In the resulting Details page, click the **General** tab, then click **Manage**. The **Manage** dialog displays.



Incident Manager: All open incidents

Page Refreshed **Feb 5, 2012 8:39:19 PM PST**

Standard

- My open incidents and problems
- Unassigned incidents
- Unacknowledged incidents
- Escalated incidents
- All open incidents
- Unassigned problems
- All open problems
- Events without incidents

Severity	Summary	Target	Priority	Status	Last Updated	Owner	Acknov	Escalat	Type
⚠	There have been 160 failed login attempts	Oemrep_Dat	None	New	Feb 3, 2012 4:08:38 PM F	sysman	No	No	Incident
⚠					PM F	sysman	No	No	Incident
⊗					PM F	-	No	No	Incident
⊗					PM F	-	No	No	Incident

Manage

You can manage the workflow of your incidents to achieve better tracking. When tracking attributes of an incident are updated, any applicable rules will be executed.

Status: New

Owner:

Priority: None

Escalated: None

Add Comment:

eshold (75). Current value: ...

Metric: Loader Throughput (rows per second)

Loader Name: Loader_D

Target: [redacted]:7654_Management_Service (Oracle Management Service)

Incident Created: Feb 1, 2012 3:47:19 PM PST

Last Updated: Feb 1, 2012 3:47:19 PM PST

Owner: -

Priority: None

Acknowledged: No

Status: New

Last Comment: Incident created by rule (Name = Incident management Rulese Incident creation Rule for metric alerts.; Owner =).: on Feb 1,

✓ This incident will be automatically cleared when the underlying issue is res

You can then adjust the priority, escalate the incident, and assign it to a specific IT operator.

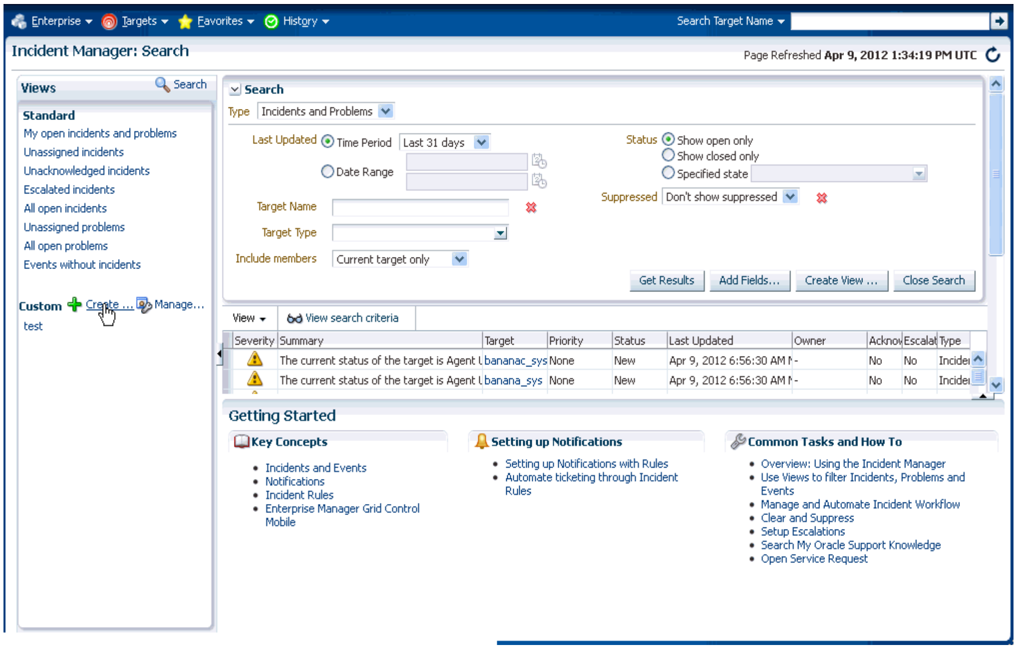
Working with incidents involves the following stages:

1. Finding What Needs to be Worked On
2. Searching for Incidents
3. Setting Up Custom Views
4. Responding and Working on a Simple Incident
5. Responding to and Managing Multiple Incidents, Events and Problems in Bulk
6. Managing Workload Distribution of Incidents
7. Creating an Incident Manually

3.3.1 Finding What Needs to be Worked On

Enterprise Manager provides multiple access points that allow you to find out what needs to be worked on. The primary focal point for incident management is the Incident Manager console, however Enterprise Manager also provides other methods of notification. The most common way to be notified that you have an issue that needs to be addressed is by email. However, incident information can also be found in the following areas:

Custom Views (See "Setting Up Custom Views")



Incident Manager: Search

Page Refreshed **Apr 9, 2012 1:34:19 PM UTC**

Standard

- My open incidents and problems
- Unassigned incidents
- Unacknowledged incidents
- Escalated incidents
- All open incidents
- Unassigned problems
- All open problems
- Events without incidents

test

Search

Type: Incidents and Problems

Last Updated: ● Time Period: Last 31 days; ○ Date Range

Status: ● Show open only ○ Show closed only ○ Specified state

Target Name:

Target Type:

Suppressed: Don't show suppressed

Include members: Current target only

Severity	Summary	Target	Priority	Status	Last Updated	Owner	Acknov	Escalat	Type
⚠	The current status of the target is Agent U	bananac_sys	None	New	Apr 9, 2012 6:56:30 AM N	-	No	No	Incide
⚠	The current status of the target is Agent U	banana_sys	None	New	Apr 9, 2012 6:56:30 AM N	-	No	No	Incide

Getting Started

Key Concepts

- Incidents and Events
- Notifications
- Incident Rules
- Enterprise Manager Grid Control Mobile

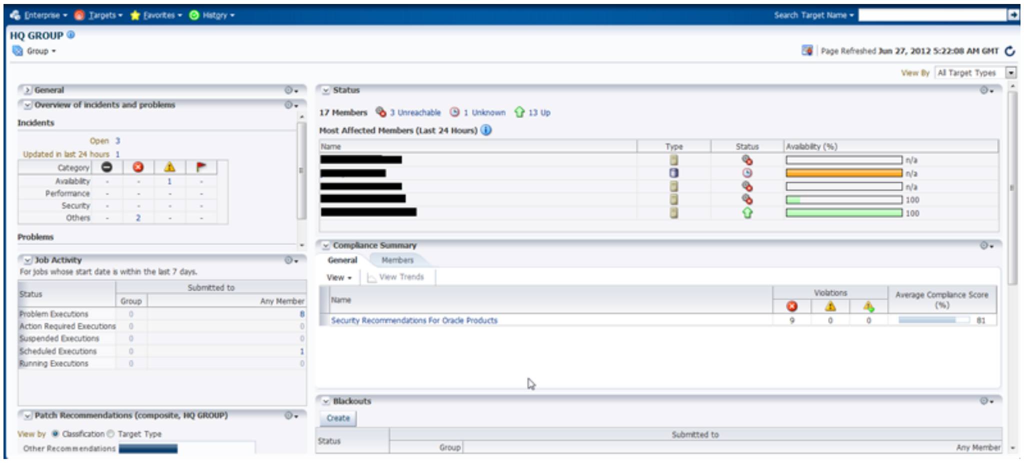
Setting up Notifications

- Setting up Notifications with Rules
- Automate ticketing through Incident Rules

Common Tasks and How To

- Overview: Using the Incident Manager
- Use Views to filter Incidents, Problems and Events
- Manage and Automate Incident Workflow
- Clear and Suppress
- Setup Escalations
- Search My Oracle Support Knowledge
- Open Service Request

Group or System Homepages (See Chapter 6, "Managing Groups")



HQ GROUP

Page Refreshed **Jun 27, 2012 5:22:08 AM GMT**

View By: All Target Types

Overview of incidents and problems

Incidents

Open 3

Updated in last 24 hours 1

Category	⛔	✖	⚠	🚩
Availability	-	-	1	-
Performance	-	-	-	-
Security	-	-	-	-
Others	-	2	-	-

Problems

Job Activity

For jobs whose start date is within the last 7 days.

Status	Submitted to	
	Group	Any Member
Problem Executions	0	8
Action Required Executions	0	0
Suspended Executions	0	0
Scheduled Executions	0	1
Running Executions	0	0

Patch Recommendations (composite, HQ GROUP)

View by ● Classification ○ Target Type

Other Recommendations

Status

17 Members 3 Unreachable 1 Unknown 13 Up

Most Affected Members (Last 24 Hours)

Name	Type	Status	Availability (%)
[redacted]			n/a
[redacted]			n/a
[redacted]			n/a
[redacted]			100
[redacted]		⇧	100

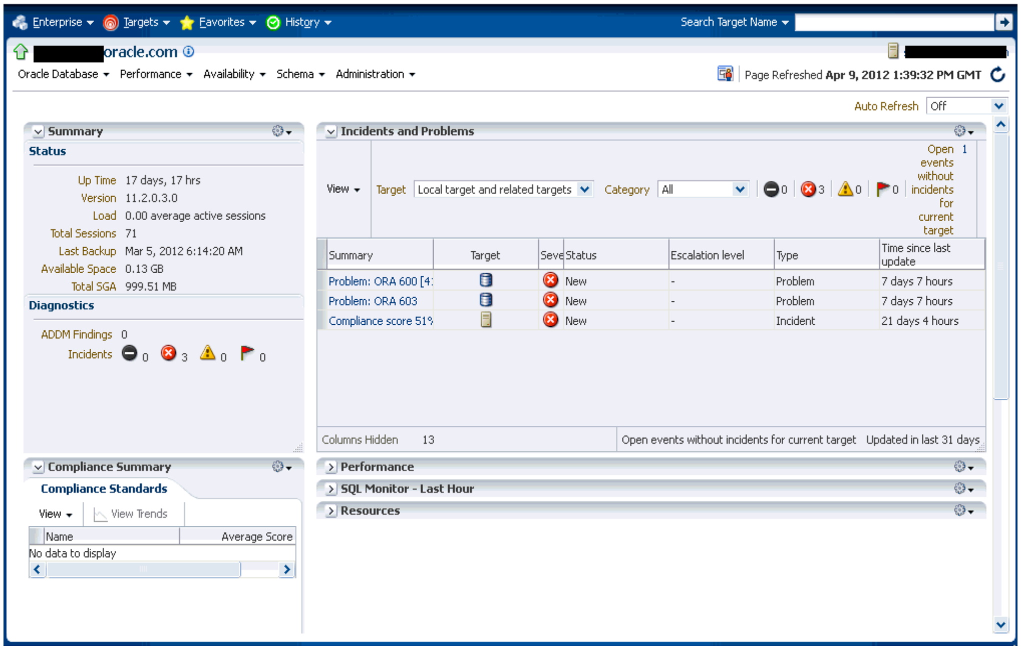
Compliance Summary

Name	Violations			Average Compliance Score (%)
	✖	⚠	⚠	
Security Recommendations For Oracle Products	9	0	0	81

Blackouts

Status	Submitted to	
	Group	Any Member

Target Homepages



[redacted]oracle.com [redacted]

Page Refreshed **Apr 9, 2012 1:39:32 PM GMT**

Auto Refresh Off

Summary

Status

Up Time	17 days, 17 hrs
Version	11.2.0.3.0
Load	0.00 average active sessions
Total Sessions	71
Last Backup	Mar 5, 2012 6:14:20 AM
Available Space	0.13 GB
Total SGA	999.51 MB

Diagnostics

ADDM Findings 0

Incidents ⊖ 0 ☒ 3 ⚠ 0 ⚑ 0

Incidents and Problems

Target Local target and related targets Category All ⊖ 0 ☒ 3 ⚠ 0 ⚑ 0 Open events without incidents for current target 1

Summary	Target	Seve	Status	Escalation level	Type	Time since last update
Problem: ORA 600 [4:		☒	New	-	Problem	7 days 7 hours
Problem: ORA 603		☒	New	-	Problem	7 days 7 hours
Compliance score 51%		☒	New	-	Incident	21 days 4 hours

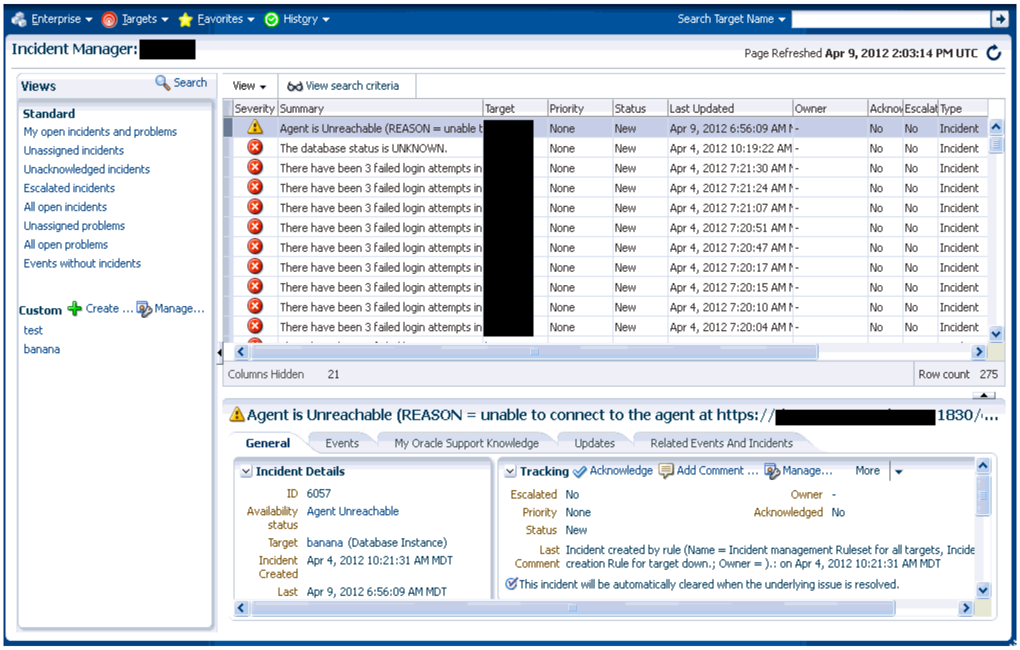
Columns Hidden 13 | Open events without incidents for current target Updated in last 31 days

Compliance Summary

Compliance Standards

Name	Average Score
No data to display	

Incident Manager (in context of a system or target)



Incident Manager: [redacted]

Page Refreshed **Apr 9, 2012 2:03:14 PM UTC**

Views

Standard

- My open incidents and problems
- Unassigned incidents
- Unacknowledged incidents
- Escalated incidents
- All open incidents
- Unassigned problems
- All open problems
- Events without incidents

Custom

- test
- banana

Severity	Summary	Target	Priority	Status	Last Updated	Owner	Acknov	Escalat	Type
⚠	Agent is Unreachable (REASON = unable t	[redacted]	None	New	Apr 9, 2012 6:56:09 AM M	-	No	No	Incident
☒	The database status is UNKNOWN.	[redacted]	None	New	Apr 4, 2012 10:19:22 AM	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:21:30 AM M	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:21:24 AM M	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:21:07 AM M	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:51 AM M	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:47 AM M	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:17 AM M	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:15 AM M	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:10 AM M	-	No	No	Incident
☒	There have been 3 failed login attempts in	[redacted]	None	New	Apr 4, 2012 7:20:04 AM M	-	No	No	Incident

Columns Hidden 21 | Row count 275

⚠ Agent is Unreachable (REASON = unable to connect to the agent at https://[redacted]1830/...

Incident Details

ID	6057
Availability status	Agent Unreachable
Target	banana (Database Instance)
Incident Created	Apr 4, 2012 10:21:31 AM MDT
Last	Apr 9, 2012 6:56:09 AM MDT

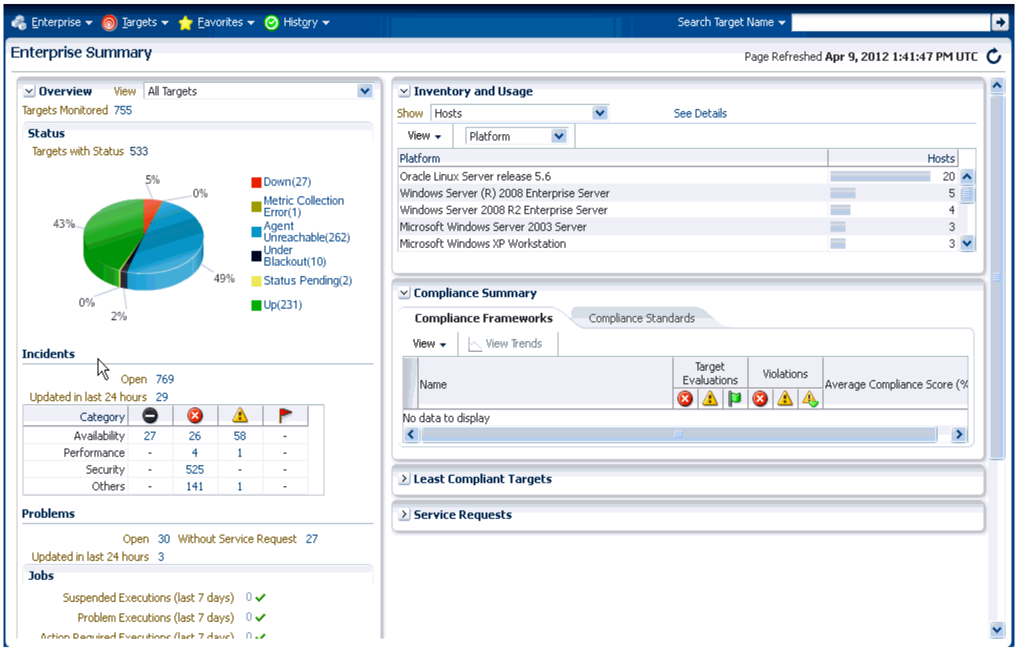
Tracking

Escalated	No	Owner	-
Priority	None	Acknowledged	No
Status	New		

Last Comment Incident created by rule (Name = Incident management Ruleset for all targets, Incide creation Rule for target down.; Owner =).: on Apr 4, 2012 10:21:31 AM MDT

✓ This incident will be automatically cleared when the underlying issue is resolved.

Enterprise Manager Console



Enterprise Summary

Page Refreshed **Apr 9, 2012 1:41:47 PM UTC**

Overview View All Targets

Targets Monitored 755

Status

Targets with Status 533

Incidents

Open 769

Updated in last 24 hours 29

Category	⊖	⊗	⚠	🚩
Availability	27	26	58	-
Performance	-	4	1	-
Security	-	525	-	-
Others	-	141	1	-

Problems

Open 30 Without Service Request 27

Updated in last 24 hours 3

Jobs

Suspended Executions (last 7 days) 0 ✓

Problem Executions (last 7 days) 0 ✓

Action Required Executions (last 7 days) 0 ✓

Inventory and Usage

Show Hosts

View Platform

Platform	Hosts
Oracle Linux Server release 5.6	20
Windows Server (R) 2008 Enterprise Server	5
Windows Server 2008 R2 Enterprise Server	4
Microsoft Windows Server 2003 Server	3
Microsoft Windows XP Workstation	3

Compliance Summary

Compliance Frameworks

Name	Target Evaluations			Violations			Average Compliance Score (%
	⊗	⚠	🏳	⊗	⚠	⚠	

No data to display

3.3.2 Searching for Incidents

You can search for incidents based on a variety of incident attributes such as the time incidents were last updated, target name, target type, or incident status.

1. Navigate to the Incident Manager page.

   From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. In the **Views** region located on the left, click **Search**.

   a. In the **Search** region, search for Incidents using the **Type** list and select **Incidents**.

   b. In the Criteria region, choose all the criteria that are appropriate. To add fields to the criteria, click **Add Fields...** and select the appropriate fields.

   c. After you have provided the appropriate criteria, click **Get Results**.

      Validate that the list of incidents match what you are looking for. If not, change the search criteria as needed.

   d. To view all the columns associated with this table, in the **View** menu, select **Columns**, then select **Show All**.

Searching for Incidents by Target Lifecycle Status

In addition to searching for incidents using high-level incident attributes, you can also perform more granular searches based on individual target lifecycle status. Briefly, lifecycle status is a target property that specifies a target's operational status. Status options for which you can search are:

- All
- Mission Critical
- Production

- Staging
- Test
- Development

For more discussion on lifecycle status, see Section 3.4.7, "Event Prioritization."

To search for incidents by target lifecycle status:

1. Navigate to the Incident Manager page.

   From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. In the **Views** region located on the left, click **Search**.
3. In the **Search** region, click **Add Fields**. A pop-up menu appears showing the available lifecycle statuses.
4. Choose on one or more of the lifecycle status options.
5. Enter any additional search criteria.
6. Click **Get Results**.

3.3.3 Setting Up Custom Views

Incident Manager also allows you to define custom views to help you gain quick access to the incidents and problems on which you need to focus. For example, you may define a view to display all critical database incidents that you own. By specifying and saving view preferences to display only those incident attributes that you are interested in Enterprise Manager will show only the list of matching incidents.

You can then search the incidents for only the ones with specific attributes, such as priority 1. The view allows easy access to pertinent incidents for daily triage. Accordingly, you can save the search criteria as a filter named "All priority 1 incidents for my targets". The view becomes available in the UI for immediate use and will be available anytime you log in to access the specific incidents. The last view you used will be the default view used on your next login.

Perform the following steps:

1. Navigate to the Incident Manager page.

   From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. In the **MyViews** region located on the left, click the create "+" icon.

   a. In the **Search** region, search for Incidents using the **Type** list and select **Incidents**.

   b. In the Criteria region, choose all the criteria that are appropriate. To add fields to the criteria, click **Add Fields...** and select the appropriate fields.

   c. After you have provided the appropriate criteria, click **Get Results**.

      Validate that the list of incidents match what you are looking for. If not, change the search criteria as needed.

   d. To view all the columns associated with this table, in the **View** menu, select **Columns**, then select **Show All**.

To select a subset of columns to display and also the order in which to display them, from the **View** menu, select **Columns**, then **Manage Columns**. A dialog displays showing a list of columns available to be added in the table.

e. Click the **Create View...** button.

f. Enter the view name. If you want other administrators to use this view, check the **Share** option.

g. Click **OK** to save the view.

> **Note:** From the View creation dialog, you can also mark the view as shared. See Section 3.3.4, "Sharing/Unsharing Custom Views" for more information.

3.3.4 Sharing/Unsharing Custom Views

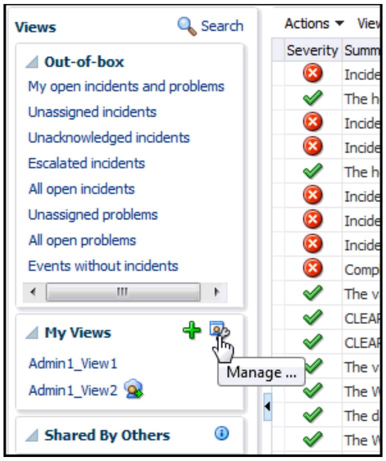
When you create your own views, they are private (only you can see them). Beginning with Enterprise Manager Release 12.1.0.4, you can share your private views with other administrators. When you share a view, all Enterprise Manager users will be able to use the view.

As mentioned previously, you are given the opportunity to share a view during the view creation process. If you have already created custom views, you can share them at any time.

1. Navigate to Incident Manager.

   From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. From the My Views region, click the Manage icon.



3. From the Manage Custom Views dialog, choose a custom view.

4. Click **Share** (or **Unshare** if the view is already shared and you want to unshare it.)

5. Click **Yes** to confirm the share/unshare operation.

3.3.5 Responding and Working on a Simple Incident

The following steps take you through one possible incident management scenario.

1. Navigate to Incident Manager.

From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. Use a view to filter the list of incidents. For example, you should use **My Open Incidents and Problems** view to see incidents and problems assigned to you. You can then sort the list by priority.
3. To work on an incident, select the incident. In the **General** tab, click **Acknowledge** to indicate that you are working on this incident, and to stop receiving repeat notifications for the incident.

   In addition to the acknowledging the incident, you can perform other incident management operations such as:

   - Adding a comment.
   - Managing the incident. See Section 3.3.6, "Responding to and Managing Multiple Incidents, Events and Problems in Bulk" for more information on incident management options.
   - Editing the summary.
   - Manually creating a ticket.
   - Suppressing/unsuppressing the incident.
   - Clearing the incident.

   Be aware that as you are working on an individual incident, new incidents might be coming in. Update the list of incidents by clicking the **Refresh** icon.
4. If the solution for the incident is unknown, use one or all of the following methods made available in the Incident page:

   - Use the **Guided Resolution** region and access any recommendations, diagnostic and resolution links available.
   - Check My Oracle Support Knowledge base for known solutions for the incident.
   - Study related incidents available through the Related Events and Incidents tab.
5. Once the solution is known and can be resolved right away, resolve the incident by using tools provided by the system, if possible.
6. In most cases, once the underlying cause has been fixed, the incident is cleared in the next evaluation cycle. However, in cases like log-based incidents, clear the incident.

Alternatively, you can work with incidents for a specific target from that target's home page. From the *target* menu, select **Monitoring** and then select **Incident Manager** to access incidents for that target (or group).

3.3.6 Responding to and Managing Multiple Incidents, Events and Problems in Bulk

There may be situations where you want to respond to multiple incidents in the same way. For example, you find that a cluster of incidents that are assigned to you are due to insufficient tablespace issues on several production databases. Your manager suggests that these tablespaces be transferred to a storage system being procured by another administrator. In this situation, you want to set all of the tablespace incidents to a customized resolution state "Waiting for Hardware." You also want to assign the incidents to the other administrator and add a comment to explain the scenario. In this situation, you want to update all of these incidents in bulk rather than individually.

To respond to incidents in bulk:

1. Navigate to Incident Manager.

   From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. Use a view to filter the list of incidents to the subset of incidents you want to work on. For example, you can use **My Open Incidents and Problems** view to see incidents and problems assigned to you. You can then sort the list by priority.

3. Select the incidents to which you want to respond. You can select multiple incidents by holding down the Control key and selecting individual incidents or you can hold down the Shift key and select the first and last incidents to select a contiguous block of incidents.

4. From the **Action** menu, choose the desired response action.

   - **Acknowledge**: Indicate that you have viewed the incidents. This option also stops any repeat notifications sent out for the incidents. This sets the *Acknowledged* flag to *Yes* and also makes you the owner of the incident

   - **Manage**: Allows you to perform a multi-action response to the incidents.

     – *Acknowledge*: If an incident is acknowledged, it will be implicitly assigned to the user who acknowledged it. When a user assigns an incident to himself, it is considered acknowledged. Once acknowledged, an incident cannot be unacknowledged. Acknowledgement also stops any repeat notifications for that incident

     – *Assign to*: Assign the incident(s) to the administrator who will take ownership of the incident.

     – *Prioritization*: The priority level of an incident can be set by selecting one of the out-of-the-box priority values: None, Urgent, Very High, High, Medium, Low

     – *Incident Status*: The resolution state for the incident can be set by selecting either Work in Progress or Resolved or to any custom status defined.

     – *Escalation Level*: Administrators can update incidents to set an escalation level: Level 1 through 5, in addition to the default value of None. An escalated issue can be de-escalated by setting the escalation to None. The appropriate *Escalation Level* depends on the IT procedures you have in place.

     – *Comment*: You can enter comments such as those you want to pass to the owner of the incident.

   - **Suppress**: Suppressing an incident stops corresponding notifications, and removes it from out-of-the-box views and default totals (such as those presented in the summary region). Suppression is typically performed when you want to defer action on the incident until a future time and in the meantime want to visually hide them from appearing in the console. Administrators can see suppressed incidents by explicitly searching for them such as performing a search on incidents where the search criteria includes the *Suppressed* search field

     Incidents can be suppressed until any of the following conditions are met:

     – Until the suppression is manually removed

     – Until specified date in the future

  - Until the severity state changes (incidents only)
  - Until it is closed
- **Clear**: Administrators can clear incidents or problems manually. For incidents, this applies only to incidents containing incidents that can be manually cleared.
- **Add Comment**: Users can add comments on incidents and events. Comments may be used for sharing information with other users or to provide tracking information on any actions being taken. Comments can be added even on closed issues.

> **Note:** The single action **Acknowledge** and **Clear** buttons are enabled for open incidents and can be used for multiple incident selection.

If any of the above actions applies only to a subset of selected incidents (for example, if an administrator tries to acknowledge multiple incidents, of which some are already acknowledged), the action will be performed only where applicable. The administrator will be informed of the success or failure of the action.

When an administrator selects any of these actions, a corresponding annotation is added to the incident for future reference.

5. Click **OK**. Enterprise Manager displays a process summary and confirmation dialogs.
6. Continue working with the incidents as required.

3.3.7 Searching My Oracle Support Knowledge

To access My Oracle Support Knowledge base entries from within Incident Manager, perform the following steps:

1. Navigate to Incident Manager.

   From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.
2. Select one of the standard views. Choose the appropriate incident or problem in the View table.
3. In the resulting details region, click **My Oracle Support Knowledge**.

   If your My Oracle Support (MOS) login credentials have been saved as MOS Preferred Credentials, you do not need to log in manually. If not, you will need to sign in to My Oracle Support. To save your MOS login information as Preferred Credentials.

   Setting MOS Preferred Credentials: From the **Setup** menu, select **Security** and then **Preferred Credentials**. From the My Oracle Support Preferred Credentials region, click **Set MOS Credentials**.
4. On the My Oracle Support page, click the **Knowledge** tab to browse the knowledge base.

   From this page, in addition to accessing formal Oracle documentation, you can also change the search string in to look for additional knowledge base entries.

3.3.8 Open Service Request (Problems-only)

There are times when you may need assistance from Oracle Support to resolve a *problem*. This procedure is not relevant for incidents or events.

To submit a service request (SR), perform the following steps:

1. Navigate to Incident Manager.

   From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. Use one of the views to find the problem or search for it or use one of your custom views. Select the appropriate problem from table.
3. Click on the **Support Workbench: Package Diagnostic** link.
4. Complete the workflow for opening an SR. Upon completing the workflow, a draft SR will have been created.
5. Sign in to My Oracle Support if you are not already signed in.
6. On the My Oracle Support page, click the **Service Requests** tab.
7. Click **Create SR** button.

3.3.9 Suppressing Incidents and Problems

There are times when it is convenient to hide an incident or problem from the list in the All Open Incidents page or the All Open Problems page. For example, you need to defer work on the incident until a future date (for example, until maintenance window). In order to avoid having it appear in the UI, you want to temporarily hide or suppress the incident until a future date. In order to find a suppressed incident, you must explicitly search for the incident using either the *Show all* or the *Only show suppressed* search option. In order to unhide a suppressed incident or problem, it must be manually unsuppressed.

To suppress an incident or problem:

1. Navigate to Incident Manager.

   From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. Select either the All Open Incidents view or the All Open Problems view.

   Choose the appropriate incident or problem. Click the **General** tab.

3. In the resulting details region, click **More**, then select **Suppress**.
4. On the resulting Suppress pop-up, choose the appropriate suppression type.

   Add a comment if desired.

5. Click **OK**.

3.3.10 Managing Workload Distribution of Incidents

Incident Manager enables you to manage incidents and problems to be addressed by your team.

Perform the following tasks:

1. Navigate to Incident Manager.

From the **Enterprise** menu on the Enterprise Manager home page, select **Monitoring**, then select **Incident Manager**.

2. Use the standard or custom views to identify the incidents for which your team is responsible. You may want to focus on unassigned and unacknowledged incidents and problems.
3. Review the list of incidents. This includes: determining person assigned to the incident, checking its status, progress made, and actions taken by the incident owner.
4. Add comments, change priority, reassign the incident as needed by clicking on the Manage button in the Incident Details region.

Example Scenario

The DBA manager uses Incident Manager to view all the incidents owned by his team. He ensures all of them are correctly assigned; if not, he reassigns and prioritizes them appropriately. He monitors the escalated events for their status and progress, adds comments as needed for the owner of the incident. In the console, he can view how long each of the incidents has been open. He also reviews the list of unassigned incidents and assigns them appropriately.

3.3.11 Reviewing Events on a Periodic Basis

Oracle recommends managing via incidents in order to focus on important events or groups of related events. Due to the variety and sheer number of events that can be generated, it is possible that not all important events will be covered by incidents. To help you find these important yet untreated events, Enterprise Manager provides the **Events without incidents** standard view.

Perform the following steps:

1. From the **Enterprise** menu, select **Monitoring**, then select **Incident Manager**.
2. In the Views region, click **Events without incidents**.
3. Select the desired event in the table. The event details display.
4. In the details area, choose **More** and then either **Create Incident** or **Add Event to Incident**.

Example Scenario

During the initial phase of Enterprise Manager uptake, every day the DBA manager reviews the events for the databases his team is responsible for and filters them to view only the ones which are not tracked by ticket or incident. He browses such events to ensure that none of them requires incidents to track the issue. If he feels that one such event requires an incident to track the issue, he creates an incident directly for this event.

3.3.11.1 Creating an Incident Manually

If an event of interest occurs that is not covered by any rule and you want to convert that event to an incident, perform the following:

1. Using an available view, find the event of interest.
2. Select the event in the table.
3. From the **More...** drop-down menu, choose **Create Incident...**
4. Enter the incident details and click **OK**.

5. Should you decide to work on the incident, set yourself as owner of the incident and update status to *Work in Progress*.

Example Scenario

As per the operations policy, the DBA manager has setup rules to create incidents for all critical issues for his databases. The remainder of the issues are triaged at the event level by one of the DBAs.

One of the DBA receives email for an "SQL Response" event (not associated with an incident) on the production database. He accesses the details of the event by clicking on the link in the email. He reviews the details of the event. This is an issue that needs to be tracked and resolved, so he opens an incident to track the resolution of the issue. He marks the status of the incident as "Work in progress".

3.4 Advanced Topics

The following sections discuss incident/event management features relating advanced applications or operational areas.

3.4.1 Automatic Diagnostic Repository (ADR): Incident Flood Control

ADR is a file-based repository that stores database diagnostic data such as traces, dumps, the alert log, and health monitor reports. ADR's unified directory structure and a unified set of tools enable customers and Oracle Support to correlate and analyze diagnostic data across multiple instances and Oracle products.

Like Enterprise Manager, ADR creates and tracks incidents and problems to allow you to resolve issues.

- A *problem* is a critical error in the database. Critical errors manifest as internal errors, such as ORA-00600, or other severe errors, such as ORA-07445 (operating system exception) or ORA-04031 (out of memory in the shared pool).
- An *incident* is a single occurrence of a problem. When a problem (critical error) occurs multiple times, an incident is created for each occurrence. Incidents are timestamped and tracked in ADR. When an incident occurs, ADR sends a diagnostic incident alert to Enterprise Manager.

3.4.1.1 Working with ADR Diagnostic Incidents Using Incident Manager

Each diagnostic incident recorded in the ADR is also recorded as an incident in Enterprise Manager, thus providing you with a unified view of ADR/Enterprise Manager incidents and problems from within Incident Manager. For the ADR diagnostic incidents, you can access Enterprise Manager Support Workbench to take further action, such as packaging a problem or raising a service request with Oracle Support.

3.4.1.2 Incident Flood Control

Prior to Enterprise Manager Release 12.1.0.4, there was no limit to the number of diagnostic incidents recorded for a single problem in Incident Manager. It is conceivable that a problem could generate dozens or perhaps hundreds of incidents in a short period of time. While incidents generated during the early stages of a problem may be useful, after a certain point the excess diagnostic data would provide little value and possibly slow down your efforts to diagnose and resolve the problem. Because diagnostic problems typically tend to be long-lived, a significant number of incidents could be generated over time. Also, depending on the size of your monitored environment, the diagnostic data may consume considerable system resources.

For these reasons, the Enterprise Manager applies flood control limits on the number of diagnostic incidents that can be raised for a given problem in Incident Manager. Flood-controlled incidents provide a way of informing you that a critical error is ongoing, without overloading the system with diagnostic data.

Beginning with Enterprise Manager Release 12.1.0.4, two limits are placed on the number of diagnostic incidents that can be raised for a given problem in Incident Manager. A problem is identified by a unique problem signature called a problem key and is associated with a single target.

Enterprise Manager Limits on Diagnostic Incidents

Enterprise Manager enforces two limits for diagnostic incidents:

- For any given *hour*, Enterprise Manager only records up to five (default value) diagnostic incidents for a given target and problem key combination.
- On any given *day*, Enterprise Manager only records up to 25 (default value) diagnostic incidents for a given problem key and target combination.

When either of these limits is reached, any diagnostic incidents for the same target/problem key combination will not be recorded until the corresponding hour or day is over. Diagnostic incident recording will commence once a new hour or day begins.

> **Note:** Hour and day calculations are based on UTC (or GMT).

These diagnostic incident limits only apply to Incident Manager and not to the underlying ADR. All incidents continue to be recorded in the ADR repository. Using Enterprise Manager Support Workbench, users can view all the incidents for a given problem at any time and take appropriate actions.

Enterprise Manager diagnostic incident limits are configurable. As mentioned earlier, the defaults for these two limits are set to 5 incidents per hour and 25 incidents per day. These defaults should not be changed unless there is a clear business reason to track all diagnostic incidents.

Changing Enterprise Manager Diagnostic Incident Limits

To update the diagnostic limits, execute the following SQL against the Enterprise Manager repository as the SYSMAN user using the appropriate limit values as shown in the following example.

Example 3–3 SQL Used to Change Diagnostic Incident Limits

```
exec  EM_EVENT_UTIL.SET_ADR_INC_LIMITS(5,25);
```

The PL/SQL shown in the following example prints out the current limits.

Example 3–4 SQL Used to Print Out Current Diagnostic Incident Limits

```
DECLARE
  l_adr_hour_limit NUMBER;
  l_adr_day_limit NUMBER;
BEGIN
      em_event_util. GET_ADR_INC_LIMITS
              (p_hourly_limit => l_adr_hour_limit,
               p_daily_limit => l_adr_day_limit);
      dbms_output.put_line(l_adr_hour_limit || '-' || l_adr_day_limit);
END;
```

Important: The Enterprise Manager incident limits are **in addition to** any diagnostic incident limits imposed by underlying applications such as Oracle database, Middleware and Fusion Applications. These limits are specific to each application. See the respective application documentation for more information.

3.4.2 Defining Custom Incident Statuses

As discussed in "Working with Incidents" on page 3-40, one of the primary incident workflow attributes is *status*. For most conditions, these predefined status attributes will suffice. However, the uniqueness of your monitoring and management environment may require an incident workflow requiring specialized incident states. To address this need, you can define custom states using the *create_resolution_state* EM CLI verb.

3.4.2.1 Creating a New Resolution State

```
emcli create_resolution_state
     -label="Label for display"
     -position="Display position"
     [-applies_to="INC|PBLM"]
```

This verb creates a new resolution state for describing the state of incidents or problems.

Important: This command can only be executed by Enterprise Manager Super Administrators.

The new state is always added between the *New* and *Closed* states. You must specify the exact position of this state in the overall list of states by using the `-position` option. The position can be between 2 and 98.

By default, the new state is applicable to both incidents and problems. The `-applies_to` option can be used to indicate that the state is applicable only to incidents or problems.

A success message is reported if the command is successful. An error message is reported if the change fails.

Examples

The following example adds a resolution state that applies to both incidents and problems at position 25.

```
emcli create_resolution_state  -label="Waiting for Ticket"
-position=25
```

The following example adds a resolution state that applies to problems only at position 35.

```
emcli create_resolution_state  -label="Waiting for SR"
-position=35 -applies_to=PBLM
```

3.4.2.2 Modifying an Existing Resolution State

You can chance the both the display label and the position of an existing state by using the *modify_resolution_state* verb.

```
emcli modify_resolution_state
        -label="old label of the state to be changed"
        -new_label="New label for display"
        -position="New display position"
        [-applies_to=BOTH]
```

This verb modifies an existing resolution state that describes the state of incidents or problems. As with the create_resolution_state verb, this command can only be executed by Super Administrators.

You can optionally indicate that the state should apply to both incidents and problems using the `-applies_to` option.

Examples

The following example updates the resolution state with old label "Waiting for TT" with a new label "Waiting for Ticket" and if necessary, changes the position to 25.

```
emcli modify_resolution_state  -label="Waiting for TT" -new_
label="Waiting for Ticket" -position=25
```

The following example updates the resolution state with the old label "SR Waiting" with a new label "Waiting for SR" and if necessary, changes the position to 35. It also makes the state applicable to incidents and problems.

```
emcli modify_resolution_state  -label="SR Waiting" -new_
label="Waiting for SR" -position=35 -applies_to=BOTH
```

3.4.3 Clearing Stateless Alerts for Metric Alert Event Types

For *metric alert* event types, an event (metric alert) is raised based on the metric threshold values. These metric alert events are called *stateful* alerts. For those metric alert events that are not tied to the state of a monitored system (for example, *snapshot too old*, or *resumable session suspended*), these alerts are called stateless alerts. Because stateless alerts are not cleared automatically, they need to be cleared manually. You can perform a bulk purge of stateless alerts using the *clear_stateless_alerts* EM CLI verb.

> **Note:** For large numbers of incidents, you can manually clear incidents in bulk. See "Responding to and Managing Multiple Incidents, Events and Problems in Bulk".

clear_stateless_alerts clears the stateless alerts associated with the specified target. The clearing must be manually performed as the Management Agent does not automatically clear stateless alerts. To find the metric internal name associated with a stateless alert, use the EM CLI *get_metrics_for_stateless_alerts* verb.

Format

```
emcli clear_stateless_alerts -older_than=number_in_days -target_type=target_type
-target_name=target_name [-include_members][-metric_internal_name=target_type_
metric:metric_name:metric_column] [-unacknowledged_only][-ignore_notifications]
[-preview]

[ ] indicates that the parameter is optional
```

Options

- **older_than**

  Specify the age of the alert in days. (Specify 0 for currently open stateless alerts.)

- **target_type**

  Internal target type identifier, such as host, oracle_database, and emrep.

- **target_name**

  Name of the target.

- **include_members**

  Applicable for composite targets to examine alerts belonging to members as well.

- **metric_internal_name**

  Metric to be cleaned up. Use the get_metrics_for_stateless_alerts verb to see a complete list of supported metrics for a given target type.

- **unacknowledged_only**

  Only clear alerts if they are not acknowledged.

- **ignore_notifications**

  Use this option if you do not want to send notifications for the cleared alerts. This may reduce the notification sub-system load.

- **ignore_notifications**

  Use this option if you do not want to send notifications for the cleared alerts. This may reduce the notification sub-system load.

- **preview**

  Shows the number of alerts to be cleared on the target(s).

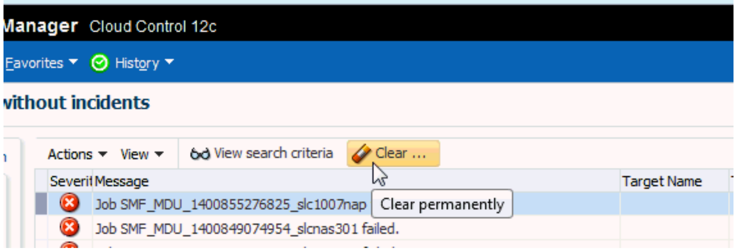
Example

The following example clears alerts generated from the database alert log over a week old. In this example, no notifications are sent when the alerts are cleared.

```
emcli clear_stateless_alerts -older_than=7 -target_type=oracle_database -tar  get_
name=database -metric_internal_name=oracle_database:alertLog:genericErrStack
-ignore_notifications
```

3.4.4 Automatically Clearing "Manually Clearable" Events

There are those events that clear automatically, such as CPU Utilization and those events that must be manually cleared, either through the Incident Manager UI or automatically via rule (such as Job Failure, or Log Metric events). Auto-clear events, as the term implies, are cleared automatically by Enterprise Manager once the underlying issue is resolved. In the case of CPU Utilization, the event CPU Utilization clears automatically once the percent utilization falls below the warning threshold. However, for those events that must be cleared manually, a user must intervene and clear the event using Incident Manager either by selecting the incident/event and clicking **Clear**, or creating an event rule to do the job (recommended method).

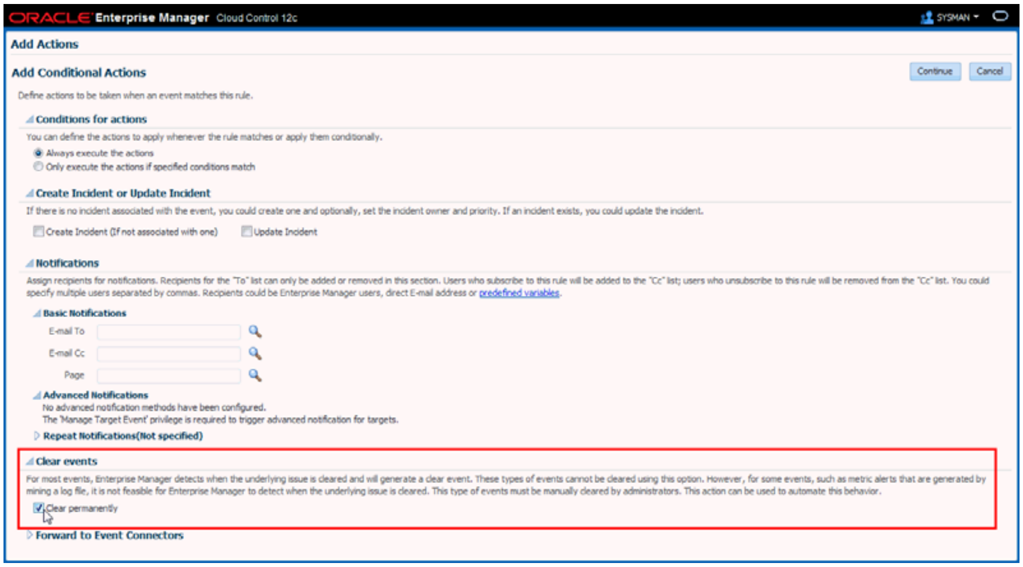


Job SMF_MDU_1400855276825_slc1007nap

Job SMF_MDU_1400849074954_slcnas301 failed.

As mentioned previously, an event rule automates the clearing of *manually clearable* events. Enterprise Manager provides a limited number of out-of-box rules that automatically clear *manually clearable* events, such as job failures or ADP events that remain open for seven days. However, to more accurately meet the needs of your monitoring environment, Oracle recommends creating your own event rules to automatically clear those *manually clearable* events that are most prevalent in your environment.

During the rule creation process, you can specify that an event be automatically cleared by selecting the **Clear Event** option while you are adding conditional actions.



Define actions to be taken when an event matches this rule.

You can define the actions to apply whenever the rule matches or apply them conditionally.

● Always execute the actions

○ Only execute the actions if specified conditions match

If there is no incident associated with the event, you could create one and optionally, set the incident owner and priority. If an incident exists, you could update the incident.

□ Create Incident (If not associated with one) □ Update Incident

Assign recipients for notifications. Recipients for the "To" list can only be added or removed in this section. Users who subscribe to this rule will be added to the "Cc" list; users who unsubscribe to this rule will be removed from the "Cc" list. You could specify multiple users separated by commas. Recipients could be Enterprise Manager users, direct E-mail address or predefined variables.

E-mail To

E-mail Cc

Page

No advanced notification methods have been configured.

The 'Manage Target Event' privilege is required to trigger advanced notification for targets.

For most events, Enterprise Manager detects when the underlying issue is cleared and will generate a clear event. These types of events cannot be cleared using this option. However, for some events, such as metric alerts that are generated by mining a log file, it is not feasible for Enterprise Manager to detect when the underlying issue is cleared. This type of events must be manually cleared by administrators. This action can be used to automate this behavior.

☑ Clear permanently

Getting Notified when the Event Clears

The event clearing action is an asynchronous operation, which means that when the rule action (clear) is initiated, the manually clearable event will be enqueued for clearing, but not actually cleared. Hence, an email notification sent upon rule execution will indicate that the event has not been cleared. Asynchronous clearing is by design as it reduces overall rule engine processing load and processing time. Subscribing to this event clearing rule with the intent to be notified when the event clears will be of little value. If you want to be notified when the event clears, you must create a new event rule and explicitly specify a *Clear* severity. In doing so, you will be notified once the event is actually cleared.

3.4.5 User-reported Events

Users may create (publish) events manually using the EM CLI verb *publsh_event*. A User-reported event is published as an event of the "User-reported event" class. Only users with Manage Target privilege can publish these events for a target. An error message is reported if the publish fails.

After an event is published with a severity other than CLEAR (see below), end-users with appropriate privileges can manually clear the event from the UI, or they can publish a new event using a severity level of CLEAR and the same details to report clearing of the underlying situation.

3.4.5.1 Format

```
emcli publish_event
        -target_name="Target name"
        -target_type="Target type internal name"
        -message="Message for the event"
        -severity="Severity level"
        -name="event name"
        [-key="sub component name"
         -context="name1=value1;name2=value2;.."
         -separator=context="alt. pair separator"
         -subseparator=context="alt. name-value separator"]

[ ] indicates that the parameter is optional
```

3.4.5.2 Options

- **target_name**

  Target name.

- target_type

  Target type name.

- message

  Message to associate for the event. The message cannot exceed 4000 characters.

- **severity**

  Numeric severity level to associate for the event. The supported values for severity level are as follows:

  "CLEAR"
  "MINOR_WARNING"
  "WARNING"
  "CRITICAL"
  "FATAL"

- **name**

  Name of the event to publish. The event name cannot exceed 128 characters.

  This is indicative of the nature of the event. Examples include "Disk Used Percentage," "Process Down," "Number of Queues," and so on. The name must be repeated and identical when reporting different severities for the same sequence of events. This should not have any identifying information about a specific event; for example, "Process xyz is down." To identify any specific components within a target that the event is about, see the key option below.

- **key**

  Name of the sub-component within a target this event is related to. Examples include a disk name on a host, name of a tablespace, and so forth. The key cannot exceed 256 characters.

- **context**

Additional context that can be published for a given event. This is a series of strings of format name:value separated by a semi-colon. For example, it might be useful to report the percentage size of a disk when reporting space issues on the disk. You can override the default separator ":" by using the sub-separator option, and the pair separator ";" by using the separator option.

The context names cannot exceed 256 characters, and the values cannot exceed 4000 characters.

- **separator**

  Set to override the default ";" separator. You typically use this option when the name or the value contains ";". Using "=" is not supported for this option.

- **subseparator**

  Set to override the default ":" separator between the name-value pairs. You typically use this option when the name or value contains ":". Using "=" is not supported for this option.

3.4.5.3 Examples

Example 1

The following example publishes a warning event for "my acme target" indicating that a HDD restore failed, and the failure related to a component called the "Finance DB machine" on this target.

```
emcli publish_event  -target_name="my acme target" -target_type="oracle_acme"
-name="HDD restore failed" -key="Finance DB machine" -message="HDD restoration
failed due to corrupt disk" -severity=WARNING
```

Example 2

The following example publishes a minor warning event for "my acme target" indicating that a HDD restore failed, and the failure related to a component called the "Finance DB machine" on this target. It specifies additional context indicating the related disk size and name using the default separators. Note the escaping of the \ in the disk name using an additional "\".

```
emcli publish_event  -target_name="my acme target" -target_type="oracle_acme"
-name="HDD restore failed" -key="Finance DB machine" -message="HDD restoration
failed due to corrupt disk" -severity=MINOR_WARNING -context="disk
size":800GB\;"disk name":\\uddo0111245
```

Example 3

The following example publishes a critical event for "my acme target" indicating that a HDD restore failed, and the failure related to a component called the "Finance DB machine" on this target. It specifies additional context indicating the related disk size and name. It uses alternate separators, because the name of the disk includes the ":" default separator.

```
emcli publish_event  -target_name="my acme target" -target_type="oracle_acme"
-name="HDD restore failed" -key="Finance DB machine" -message="HDD restoration
failed due to corrupt disk" -severity=CRITICAL -context="disk size"^800GB\;"disk
name"^\\sdd1245:2 -subseparator=context=^
```

3.4.6 Additional Rule Applications

Rules can be set up to perform more complicated tasks beyond straightforward notifications. The following tasks illustrate additional rule capabilities.

- Setting Up a Rule to Send Different Notifications for Different Severity States of an Event
- Creating a Rule to Notify Different Administrators Based on the Event Type
- Creating a Rule to Create a Ticket for Incidents
- Creating a Rule to Send SNMP Traps to Third Party Systems

3.4.6.1 Setting Up a Rule to Send Different Notifications for Different Severity States of an Event

Before you perform this task, ensure the DBA has set appropriate thresholds for the metric so that a critical metric alert is generated as expected.

Consider the following example:

The Administration Manager sets up a rule to page the specific DBA when a critical metric alert event occurs for a database in a production database group and to email the DBA when a warning metric alert event occurs for the same targets. This task occurs when a new group of databases is deployed and DBAs request to create appropriate rules to manage such databases.

Perform the following tasks to set appropriate thresholds:

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. On the Incident Rules - All Enterprise Rules page, highlight a rule set and click **Edit...**. (Rules are created in the context of a rule set. If there is no existing rule set to manage the newly added target, create a rule set.)
3. In the Edit Rule Set page, locate the Rules section. Click **Create...**
4. From the Select Type of Rule to Create dialog, choose **Incoming events and updates to events**. Click **Continue**.
5. Provide the rule details as follows:
   a. For Type, select **Metric Alerts** as the Type.
   b. In the criteria section, select **Severity**. From the drop-down list, check and **Critical** and **Warning** as the selected values. Click **Next**.
   c. On the Add Actions page, click **+Add**.

      In the Create Incident section, check the **Create Incident** option. Click **Continue**. The Add Action page displays with the new rule. Click **Next**.
   d. Specify a name for the rule and a description. Click **Next**.
   e. On the Review page, ensure your settings are correct and click **Continue**. A message appears informing you that the rule has been successfully created. Click **OK** to dismiss the message.

      Next, you need to create a rule to perform the notification actions.
6. From the Rules section on the Edit Rules page, click **Create**.
7. Select **Newly created incidents or updates to incidents** as the rule type and click **Continue**.
8. Check **Specific Incidents.**

9. Check **Severity** and from the drop-down option selector, check **Critical** and **Warning**. Click **Next**.
10. On the Add Actions page, click **Add**. The Conditional Actions page displays.
11. In the **Conditions for actions** section, choose **Only execute the actions if specified conditions match**.
12. From the **Incident matches the following criteria** list, choose **Severity** and then **Critical** from the drop-down option selector.
13. In the **Notifications** section, enter the DBA in the **Page** field. Click **Continue**. The Add Actions page displays.
14. Click **Add** to create a new action for the Warning severity.
15. In the **Conditions for actions** section, choose **Only execute the actions if specified conditions match**.
16. From the **Incident matches the following criteria** list, choose **Severity** and then **Warning** from the drop-down option selector.
17. In the **Notifications** section, enter the DBA in the **Email to** field. Click **Continue**. The Add Actions page displays with the two conditional actions. Click **Next**.
18. Specify a rule name and description. Click **Next**.
19. On the Review page, ensure your rules have been defined correctly and click **Continue**. The Edit Rule Set page displays.
20. Click **Save** to save your newly defined rules.

3.4.6.2 Creating a Rule to Notify Different Administrators Based on the Event Type

As per operations policy for production databases, the incidents that relate to application issues should go to the application DBAs and the incidents that relate to system parameters should go to the system DBAs. Accordingly, the respective incidents will be assigned to the appropriate DBAs and they should be notified by way of email.

Before you set up rules, ensure the following prerequisites are met:

- DBA has setup appropriate thresholds for the metric so that critical metric alert is generated as expected.
- Rule has been setup to create incident for all such events.
- Respective notification setup is complete, for example, global SMTP gateway, email address, and schedule for individual DBAs.

Perform the following steps:

1. Navigate to the Incident Rules page.

   From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. Search the list of enterprise rules matching the events from the production database.
3. On the Incident Rules - All Enterprise Rules page, highlight a rule set and click **Edit...**.

   Rules are created in the context of a rule set. If there is no existing rule set, create a rule set.
4. From the Edit Rule Set page (Rules tab), select the rule which creates the incidents for the metric alert events for the database. Click **Edit**

5. From the Select Events page, click **Next**.
6. From the Add Actions page, click **+Add**. The Add Conditional Actions page displays.
7. In the Notifications area, enter the email address of the DBA you want to be notified for this specific event type and click **Continue** to add the action. Enterprise Manager returns you to the Add Actions page.
8. Click **Next**.
9. On the Specify Name and Description page, enter an intuitive rule name and a brief description.
10. Click **Next**.
11. On the Review page, review the **Applies to**, **Actions** and **General** information for correctness .
12. Click **Continue** to create the rule.
13. Create/Edit additional rules to handle alternate additional administrator notifications according to event type.
14. Review the rules summary and make corrections as needed. Click **Save** to save your rule set changes.

3.4.6.3 Creating a Rule to Create a Ticket for Incidents

If your IT process requires a helpdesk ticket be created to resolve incidents, then you can use the helpdesk connector to associate the incident with a helpdesk ticket and have Enterprise Manager automatically open a ticket when the incident is created. Communication between Incident Manager and your helpdesk system is bidirectional, thus allowing you to check the changing status of the ticket from within Incident Manager. Enterprise Manager also allows you to link out to a Web-based third-part console directly from the ticket so that you can launch the console in context directly from the ticket.

For example, according to the operations policy of an organization, all critical incidents from a production database should be tracked by way of Remedy tickets. A rule is set up to create a Remedy ticket when a critical incident occurs for the database. When such an incident occurs, the ticket is generated by the rule, the incident is associated with the ticket, and the operation is logged for future reference to the updates of the incident. While viewing the details of the incident, the DBA can view the ticket ID and, using the attached URL link, access the Remedy to get the details about the ticket.

Before you perform this task, ensure the following prerequisites are met:

- Monitoring support has been set up.
- Remedy ticketing connector has been configured.

Perform the following steps:

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. On the Incident Rules - All Enterprise Rules page, select the appropriate rule set and click **Edit...**. (Rules are created in the context of a rule set. If there is no applicable rule set , create a new rule set.)
3. Select the appropriate rule that covers the incident conditions for which tickets should be generated and click **Edit...**
4. Click **Next** to proceed to the **Add Actions** page.

5. Click **+Add** to access the **Add Conditional Actions** page.
   a. Specify that a ticket should be generated for incidents covered by the rule.
   b. Specify the ticket template to be used.
6. Click **Continue** to return to the Add actions page.
7. On the Add Actions page, click **Next**.
8. On the Review page, click **Continue**.
9. On the Specify Name and Description page, click **Next**.
10. On the Review page, click **Continue**. A message displays indicating that the rule has been successfully modified. Click **OK** to close the message.
11. Repeat steps 3 through 10 until all appropriate rules have been edited.
12. Click **Save** to save your changes to the rule set.

3.4.6.4 Creating a Rule to Send SNMP Traps to Third Party Systems

As mentioned in Chapter 4, "Using Notifications," Enterprise Manager supports integration with third-party management tools through the SNMP. Sending SNMP traps to third party systems is a two-step process:

Step 1: Create an advanced notification method based on an SNMP trap.

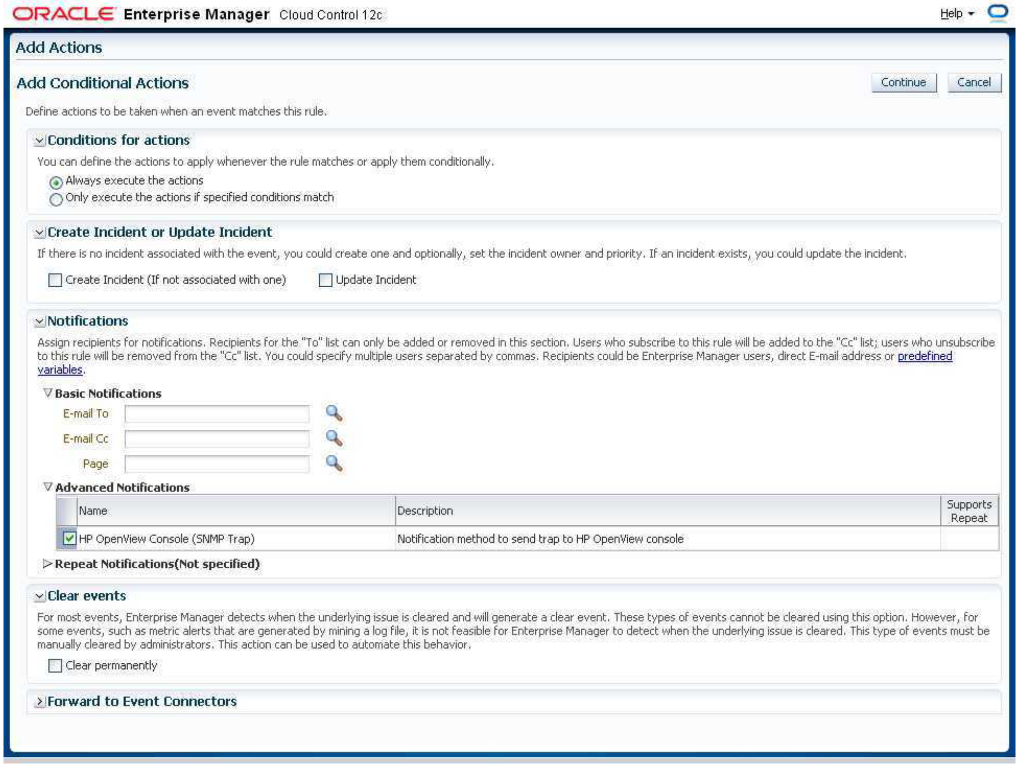
Step 2: Create an incident rule that invokes the SNMP trap notification method.

The following procedure assumes you have already created the SNMP trap notification method. For instruction on creating a notification method based on an SNMP trap, see "Sending SNMP Traps to Third Party Systems" on page 4-38.

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. On the Incident Rules - All Enterprise Rules page, click **Create Rule Set...**
3. Enter the rule set **Name**, a brief **Description**, and select the type of source object the rule **Applies to** (Targets).
4. Click on the **Rules** tab and then click **Create...**
5. On the Select Type of Rule to Create dialog, select **Incoming events and updates to events** and then click **Continue**.
6. On the Create New Rule : Select Events page, specify the criteria for the events for which you want to send SNMP traps and then click **Next**.

   > **Note:** You must create one rule per event type. For example, if you want to send SNMP traps for Target Availability events and Metric Alert events, you must specify two rules.

7. On the Create New Rule : Add Actions page, click **Add**. The Add Conditional Actions page displays.
8. In the Notifications section, under Advanced Notifications, select an existing SNMP trap notification method as shown in the following graphic.



ORACLE Enterprise Manager Cloud Control 12c

Add Actions

Add Conditional Actions

Define actions to be taken when an event matches this rule.

Conditions for actions

You can define the actions to apply whenever the rule matches or apply them conditionally.

● Always execute the actions
○ Only execute the actions if specified conditions match

Create Incident or Update Incident

If there is no incident associated with the event, you could create one and optionally, set the incident owner and priority. If an incident exists, you could update the incident.

□ Create Incident (If not associated with one) □ Update Incident

Notifications

Assign recipients for notifications. Recipients for the "To" list can only be added or removed in this section. Users who subscribe to this rule will be added to the "Cc" list; users who unsubscribe to this rule will be removed from the "Cc" list. You could specify multiple users separated by commas. Recipients could be Enterprise Manager users, direct E-mail address or predefined variables.

Basic Notifications

E-mail To

E-mail Cc

Page

Advanced Notifications

	Name	Description	Supports Repeat
☑	HP OpenView Console (SNMP Trap)	Notification method to send trap to HP OpenView console	

Repeat Notifications(Not specified)

Clear events

For most events, Enterprise Manager detects when the underlying issue is cleared and will generate a clear event. These types of events cannot be cleared using this option. However, for some events, such as metric alerts that are generated by mining a log file, it is not feasible for Enterprise Manager to detect when the underlying issue is cleared. This type of events must be manually cleared by administrators. This action can be used to automate this behavior.

□ Clear permanently

Forward to Event Connectors

For information on creating SNMP trap notification methods, see "Sending SNMP Traps to Third Party Systems" on page 4-38.

9. Click **Continue** to return to the Create New Rule : Add Actions page.
10. Click **Next** to go to the Create New Rule : Specify Name and Description page.
11. Specify a rule name and a concise description and then click **Next**.
12. Review the rule definition and then click **Continue** add the rule to the rule set. A message displays indicating the rule has been added to the rule set but has not yet been saved. Click **OK** to close the message.
13. Click **Save** to save the rule set. A confirmation is displayed. Click **OK** to close the message.

3.4.7 Event Prioritization

When working in a large enterprise, it is conceivable that when systems are under heavy load, a large number of incidents and events may be generated. All of these need to be processed in a timely and efficient manner in accordance with your business priorities. An effective prioritization scheme is needed to determine which events/incidents should be resolved first.

In order to determine which event/incidents are high priority, Enterprise Manager uses a prioritization protocol based on two incident/event attributes: Lifecycle Status of the target and the Incident/Event Type. Lifecycle Status is a target property that specifies a target's operational status. You can set/view a target's Lifecycle Status from the UI (from a target's **Target Setup** menu, select **Properties**). You can set target Lifecycle Status properties across multiple targets simultaneously by using the Enterprise Manager Command Line Interface (EM CLI) set_target_property_value verb.

A target's Lifecycle Status is set when it is added to Enterprise Manager for monitoring. At that time, you determine where in the prioritization hierarchy that target belongs—the highest level being "mission critical" and the lowest being "development."

Target Lifecycle Status

- Mission Critical (highest priority)
- Production
- Stage
- Test
- Development (lowest priority)

Incident/Event Type

- Availability events (highest priority)
- Non-informational events.
- Informational events

3.4.8 Root Cause Analysis (RCA) and Target Down Events

Root Cause Analysis (RCA) tries to identify the root causes of issues that cause operational events. Beginning with Enterprise Manager Could Control 12.1.0.3, Incident Manager automatically performs RCA over *target down events*, thus actively identifying whether the target down event is the cause or symptom of other target down events.

The term target down event specifically pertains to Target Availability events that are raised when the targets are detected to be down.

3.4.8.1 How RCA Works

RCA is an ongoing process that identifies whether a target down event is root cause or symptom. It uses the Causal Analysis Update attribute of the event to store the results of its analysis, i.e. identifying whether or not the target down event is root cause or symptom. Whenever a new target availability event comes in, RCA is automatically performed on the incoming event and existing target down events that are related to it. Based on the analysis, it updates the Causal Analysis Update attribute value if the incoming event is a target down event. It also updates the Causal Analysis Update attribute for the related target down events if there is a change.

Two types of target relationships are used for identifying the related targets: *dependency* and *containment*.

When one target depends on another target for its availability, dependency relationship exists between them. For example, J2EE application target depends on the WebLogic Server target over which it is deployed.

The causal analysis update attribute is used only for target down events (such as a Target Availability event for target down) and can have be assigned any one of the following values by the RCA process:

- *Symptom* -- The target down event has been caused by another target down event.
- *Cause* - The target down event has caused another target down event and it is not the symptom of any other target down event.

- *Root Cause* - The target down event has caused another target down event and it is not the symptom of any other target down event.
- *N/A* - Root cause analysis is not applicable to this event. Root cause analysis applies to target down events only.
- *Not a cause and not a symptom* - The target down event is not a root cause and not a symptom of other target down events. This is shown in Incident Manager as a dash (-).

The following rules describe the RCA process:

- **Rule 1**: Down event on a non-container target (a target that does not have members) is marked as the cause if a dependent target is down and it is not symptom of other target down events.

  Examples:

  - You have J2EE applications deployed on a standalone WebLogic Server. If both J2EE application and WebLogic Server targets are down, the WebLogic Server down event is the cause for the J2EE applications deployed on it.
  - You have a J2EE application deployed on couple of WebLogic Servers, which are part of a WebLogic Cluster. If one WebLogic Server is down along with its J2EE application, then the WebLogic Server down event is the cause of the J2EE application target down. This assumes the WebLogic Cluster is not down.
- **Rule 2**: Down event on a non-container target (a target that does not have members) is marked as a symptom if a target it depends on is down or if the target containing it is down.

  Examples:

  - You have a J2EE application deployed on a standalone WebLogic Server. If both J2EE application and WebLogic Server targets are down, J2EE application down event is the symptom of WebLogic Server being down.
  - You have a couple of WebLogic Servers which are part of a WebLogic Cluster. Each WebLogic Server has a J2EE application deployed on it. If the WebLogic Cluster is down, this means both WebLogic Servers are down. Consequently, the J2EE applications that are deployed on these servers are also down. The WebLogic Server down events would be marked as the causes of the WebLogic Cluster being down. See Rule 3 for details.
  - You have a couple of RAC database instance targets that are part of a cluster database target. If the cluster database is down, then all RAC instances are also down. The RAC instance down events would be marked as the causes of cluster database being down. See Rule 3 for details..
- **Rule 3**: Down event on a container target is marked as symptom down if all member targets are down and any target containing it is not down.

  Examples:

  - You have a couple of WebLogic Servers, which are part of a standalone WebLogic Cluster. A WebLogic Cluster down event would be marked as symptom, if both the WebLogic Servers are down.
  - You have a couple of RAC database instance targets that are part of a cluster database target. The cluster database target down event would be marked as a symptom, if both database instances are down.

- **Rule 4**: Down event on a container target is marked as symptom if the target containing it is down.

  Example:

  You have a couple of WebLogic Clusters that are part of a WebLogic Domain target. If the WebLogic domain is down, this means the WebLogic Clusters are also down. The WebLogic Cluster target down events would be the cause of WebLogic Domain being down. The WebLogic Domain down event would be marked as symptom.

3.4.8.2 Leveraging RCA Results in Incident Rule Sets

As described above, RCA is an ongoing process which results in marking target down events as *cause*, *symptom* or *neither* as new target down events come in and are processed. So a target down event may be marked as a cause or symptom as it comes in or after some time when RCA has analyzed additional event information.

Most datacenters automatically create incidents for target down events since these are important events that need to be resolved right away. This is recommended best practice and also implemented by the out-of-the-box rule sets. However, in terms of notifying response teams or creating trouble tickets, it is not desirable to do so for symptom incidents. Some datacenters may also choose to not create incidents for symptom events.

So the RCA results can be leveraged to do the following:

1. Notify or create tickets only for non-symptom events:

   This can be achieved in 2 ways:

   - Create two separate event rules , one event rule to create incidents for all relevant events, but take no further action (no notification or ticket creation) and another one to create incidents for non-symptom events only and also send notifications and create tickets. See "Creating Incidents On Non-symptom Events" on page 3-71 for instructions.

   - Create an event rule that creates incidents for all target down events.   Create another rule to update the incident priority, send notifications and create tickets only for incidents stemming from non-symptom events. Once the incident priority is set to say "Urgent", customer can also create additional incident rules to take additional actions on the Urgent priority incidents. See "Creating a Rule to Update Incident Priority for Non-symptom Events" on page 3-70.

2. Only create incidents after a suitable wait for events that are not initially marked as neither a cause nor a symptom:

   As mentioned previously, RCA is an iterative process whereby incoming target down events are continually being evaluated, resulting in updates to causal analysis state of existing events. Over a period of time (minutes), a target down event that was initially marked as a root cause may or may not remain a root cause depending on other incoming target down events. The original target down event may later be classified as a symptom.

   To avoid prematurely creating an incident and opening a ticket for an event which may later turn out to be a symptom event, you can set up your rules as follows:

   - In addition to the rules already defined in the previous step, create an additional event rule to act upon RCA updates to events and when the RCA update indicates that the event is marked as a symptom, lower the priority of the incident to "Low". This will also send an update to the ticket automatically.

This is recommended. See "Introducing a Time Delay" on page 3-73 for instructions.

OR

- To allow time for target down events to be reported, analyzed, and then acted upon (such as creating an incident or updating an incident), you can add a delay in the rule actions. This is useful when customer have some tolerance to take action after some minimum delay (typically 5 minutes).

3. Only create incidents for non-symptom events.

   Some datacenters may choose not to create any incidents for symptom events. This can be achieved by changing the rules to only create incidents for events marked as cause or neither a cause nor symptom. See "Creating Incidents On Non-symptom Events" on page 3-71 for instructions.

   Please note that, even in this approach, it is possible that an event that was originally marked as cause or neither a cause nor symptom, may be marked as a symptom when more information is received. Customers can use an approach similar to that of the second option in step 2 to build some delay in creating the incidents.

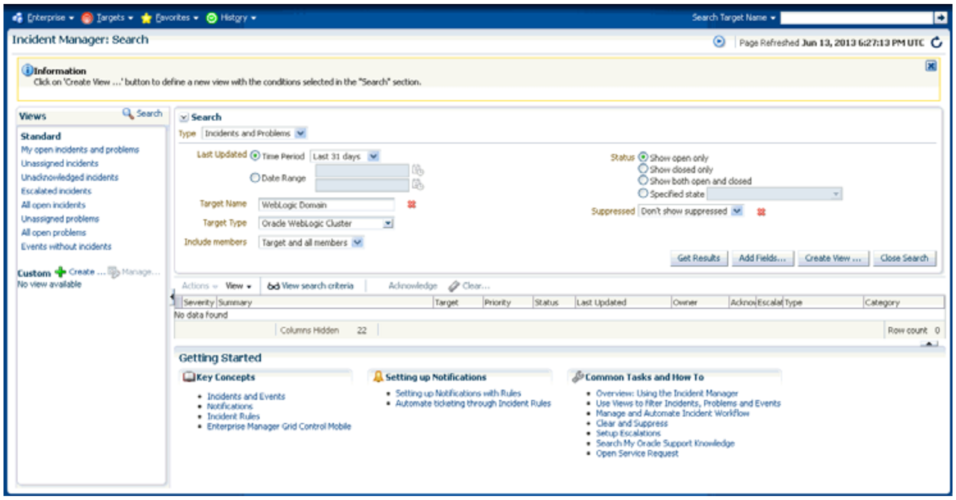
   Even with this, it is still feasible but a bit unlikely, that newer information shows up after the pre-set delay and ends up marking the event as symptom. So it is recommended to use the approach of setting incident priority and using that as a way to manage workflow.

3.4.8.3 Leveraging RCA Results in Incident Manager

You can use the RCA results to focus on the non-symptom incidents in Incident Manager. This involves using the Causal Analysis Update incident attribute when creating custom views.

1. From the **Enterprise** menu, select **Monitoring**, and then **Incidents**. The Indicent Manager page displays.

2. From the Views region, click **Create**. The Search page displays.



Information
Click on 'Create View ...' button to define a new view with the conditions selected in the "Search" section.

No view available

Type: Incidents and Problems

Last Updated: ● Time Period: Last 31 days ○ Date Range

Target Name: WebLogic Domain

Target Type: Oracle WebLogic Cluster

Include members: Target and all members

Status: ● Show open only ○ Show closed only ○ Show both open and closed ○ Specified state

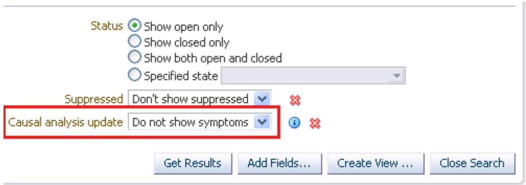
Suppressed: Don't show suppressed

Severity	Summary	Target	Priority	Status	Last Updated	Owner	Acknov	Escalat	Type	Category
No data found										

Columns Hidden 22

Row count 0

3. Click **Add Fields...** and then choose **Causal analysis update**. The Causal analysis update displays as additional search criteria.

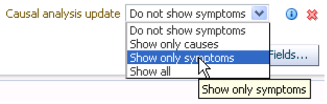


Status ● Show open only
○ Show closed only
○ Show both open and closed
○ Specified state

Suppressed: Don't show suppressed

Causal analysis update: Do not show symptoms

4. Choose 'Do Not Show Symptoms' from the list of available criteria. This will automatically exclude incidents that have been marked as 'symptom'. Incidents that are not marked as symptom or root cause will be included as long as it matches any other criteria you may have specified.



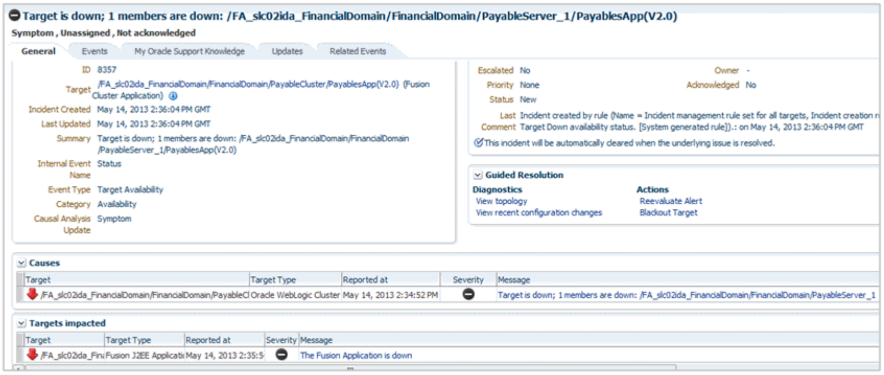
Causal analysis update: Do not show symptoms

5. Click **Create View**, enter a **View Name** when prompted, and then click **OK**.

Showing RCA Results in an Incident Detail

An incident that is a root cause or symptom will be identified prominently as part of the details of the incident in Incident Manager. In addition, in case the incident is a symptom, a **Causes** section will be added to identify the root cause(s) of the incident. In case the incident has, in turn, caused other target down incidents, an **Impacted Targets** section will also be added to show the targets that have been affected, that is. other targets that are down as a result of the original target down. The following figure shows the incident detail.

Figure 3–8   Incident that is a Root Cause



Target is down; 1 members are down: /FA_slc02ida_FinancialDomain/FinancialDomain/PayableServer_1/PayablesApp(V2.0)

Symptom , Unassigned , Not acknowledged

ID: 8357

Target: /FA_slc02ida_FinancialDomain/FinancialDomain/PayableCluster/PayablesApp(V2.0) (Fusion Cluster Application)

Incident Created: May 14, 2013 2:36:04 PM GMT

Last Updated: May 14, 2013 2:36:04 PM GMT

Summary: Target is down; 1 members are down: /FA_slc02ida_FinancialDomain/FinancialDomain /PayableServer_1/PayablesApp(V2.0)

Internal Event Name: Status

Event Type: Target Availability

Category: Availability

Causal Analysis Update: Symptom

Escalated: No

Owner: -

Priority: None

Acknowledged: No

Status: New

Last Comment: Incident created by rule (Name = Incident management rule set for all targets, Incident creation r Target Down availability status. [System generated rule]).: on May 14, 2013 2:36:04 PM GMT

This incident will be automatically cleared when the underlying issue is resolved.

Guided Resolution

Diagnostics	Actions
View topology	Reevaluate Alert
View recent configuration changes	Blackout Target

Causes

Target	Target Type	Reported at	Severity	Message
/FA_slc02ida_FinancialDomain/FinancialDomain/PayableCl	Oracle WebLogic Cluster	May 14, 2013 2:34:52 PM	⊖	Target is down; 1 members are down: /FA_slc02ida_FinancialDomain/FinancialDomain/PayableServer_1

Targets impacted

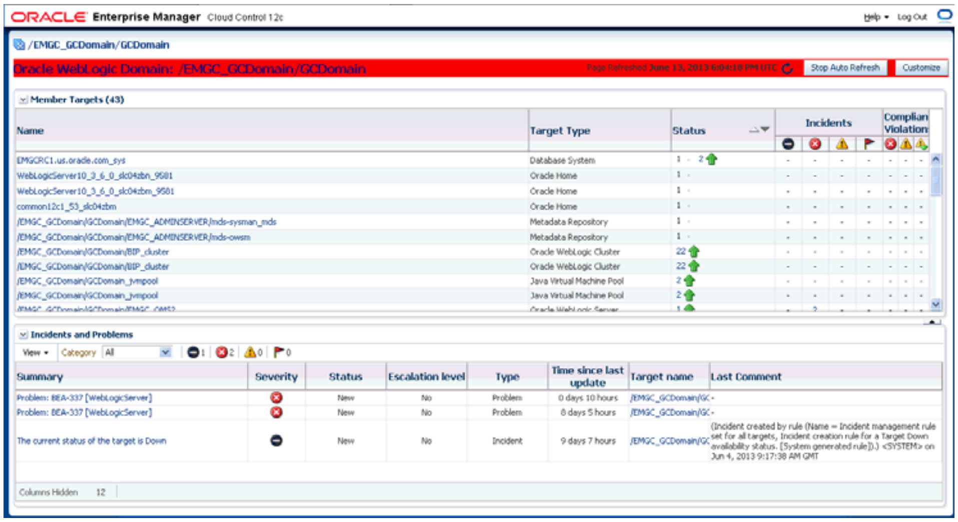
Target	Target Type	Reported at	Severity	Message
/FA_slc02ida_Fin	Fusion J2EE Applicati	May 14, 2013 2:35:5	⊖	The Fusion Application is down

3.4.8.4 Leveraging RCA Results in the System Dashboard

In the System Dashboard, you can use the RCA results to exclude symptom incidents from the Incidents table so administrators can focus their attention on incidents that are root cause or have not been caused by other target down events.

To exclude Symptom Incidents:

1. In the System Dashboard, click on the **View** option that is accessible from the upper left hand corner of the **Incidents and Problems** table.



/EMGC_GCDomain/GCDomain

Oracle WebLogic Domain: /EMGC_GCDomain/GCDomain

Page Refreshed June 13, 2013 6:04:18 PM UTC

Member Targets (43)

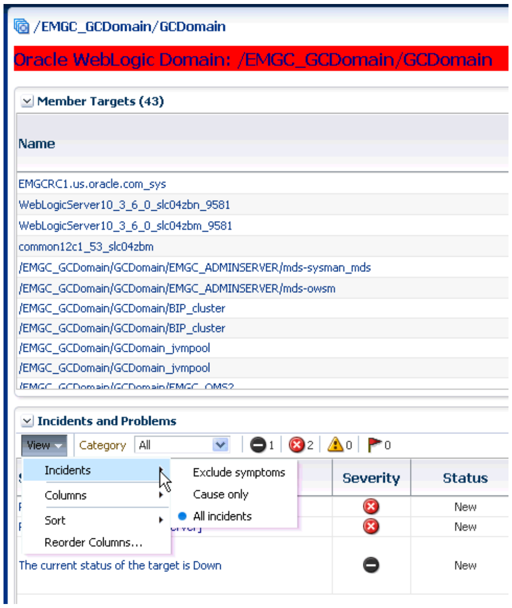
Name	Target Type	Status	Incidents				Complian Violation		
			⊖	⊗	⚠	⚑	⊗	⚠	⚠
EMGCRC1.us.oracle.com_sys	Database System	1 · 2 ⬆	-	-	-	-	-	-	-
WebLogicServer10_3_6_0_slc04zbn_9581	Oracle Home	1 ·	-	-	-	-	-	-	-
WebLogicServer10_3_6_0_slc04zbm_9581	Oracle Home	1 ·	-	-	-	-	-	-	-
common12c1_53_slc04zbm	Oracle Home	1 ·	-	-	-	-	-	-	-
/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/mds-sysman_mds	Metadata Repository	1 ·	-	-	-	-	-	-	-
/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/mds-owsm	Metadata Repository	1 ·	-	-	-	-	-	-	-
/EMGC_GCDomain/GCDomain/BIP_cluster	Oracle WebLogic Cluster	22 ⬆	-	-	-	-	-	-	-
/EMGC_GCDomain/GCDomain/BIP_cluster	Oracle WebLogic Cluster	22 ⬆	-	-	-	-	-	-	-
/EMGC_GCDomain/GCDomain_jvmpool	Java Virtual Machine Pool	2 ⬆	-	-	-	-	-	-	-
/EMGC_GCDomain/GCDomain_jvmpool	Java Virtual Machine Pool	2 ⬆	-	-	-	-	-	-	-

Incidents and Problems

Summary	Severity	Status	Escalation level	Type	Time since last update	Target name	Last Comment
Problem: BEA-337 [WebLogicServer]	⊗	New	No	Problem	0 days 10 hours	/EMGC_GCDomain/GC	-
Problem: BEA-337 [WebLogicServer]	⊗	New	No	Problem	8 days 5 hours	/EMGC_GCDomain/GC	-
The current status of the target is Down	⊖	New	No	Incident	9 days 7 hours	/EMGC_GCDomain/GC	(Incident created by rule (Name = Incident management rule set for all targets, Incident creation rule for a Target Down availability status. [System generated rule]).) <SYSTEM> on Jun 4, 2013 9:17:38 AM GMT

Columns Hidden 12

2. Choose the option to 'Exclude symptoms'. Alternatively, you can also choose the option 'Cause only' show only shows target down incidents that have been identified as cause of other target down incidents. Regardless of the option chosen, incidents that have not been marked as symptom or root cause will continue to be displayed.



/EMGC_GCDomain/GCDomain

Oracle WebLogic Domain: /EMGC_GCDomain/GCDomain

Member Targets (43)

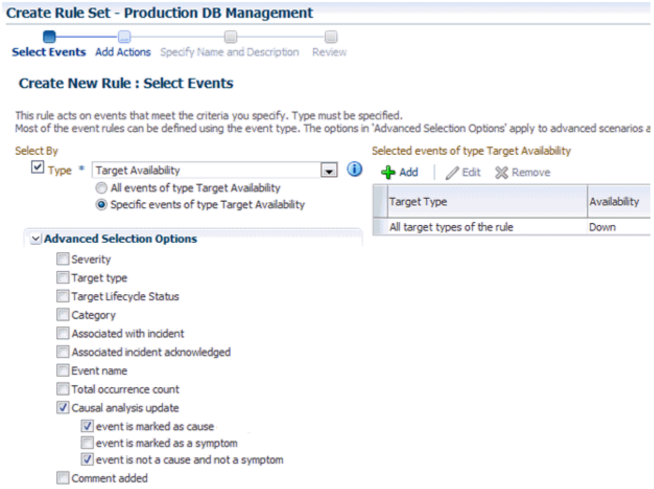
Name
EMGCRC1.us.oracle.com_sys
WebLogicServer10_3_6_0_slc04zbn_9581
WebLogicServer10_3_6_0_slc04zbm_9581
common12c1_53_slc04zbm
/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/mds-sysman_mds
/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/mds-owsm
/EMGC_GCDomain/GCDomain/BIP_cluster
/EMGC_GCDomain/GCDomain/BIP_cluster
/EMGC_GCDomain/GCDomain_jvmpool
/EMGC_GCDomain/GCDomain_jvmpool

Incidents and Problems

Summary	Severity	Status
	⊗	New
	⊗	New
The current status of the target is Down	⊖	New

3.4.8.5 Creating a Rule to Update Incident Priority for Non-symptom Events

1. Create an event rule to select only non-symptom events.



Create Rule Set - Production DB Management

Select Events — Add Actions — Specify Name and Description — Review

Create New Rule : Select Events

This rule acts on events that meet the criteria you specify. Type must be specified.
Most of the event rules can be defined using the event type. The options in 'Advanced Selection Options' apply to advanced scenarios a

Select By

☑ Type * Target Availability
○ All events of type Target Availability
● Specific events of type Target Availability

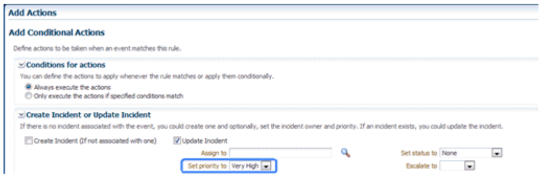
Selected events of type Target Availability

Target Type	Availability
All target types of the rule	Down

Advanced Selection Options

- □ Severity
- □ Target type
- □ Target Lifecycle Status
- □ Category
- □ Associated with incident
- □ Associated incident acknowledged
- □ Event name
- □ Total occurrence count
- ☑ Causal analysis update
  - ☑ event is marked as cause
  - □ event is marked as a symptom
  - ☑ event is not a cause and not a symptom
- □ Comment added

2. When adding an action, select the priority to be set for incidents associated with the non-symptom events selected above.



Add Actions

Add Conditional Actions

Define actions to be taken when an event matches this rule.

Conditions for actions

You can define the actions to apply whenever the rule matches or apply them conditionally.

● Always execute the actions
○ Only execute the actions if specified conditions match

Create Incident or Update Incident

If there is no incident associated with the event, you could create one and optionally, set the incident owner and priority. If an incident exists, you could update the incident.

□ Create Incident (If not associated with one) ☑ Update Incident

Assign to

Set priority to Very High

Set status to None

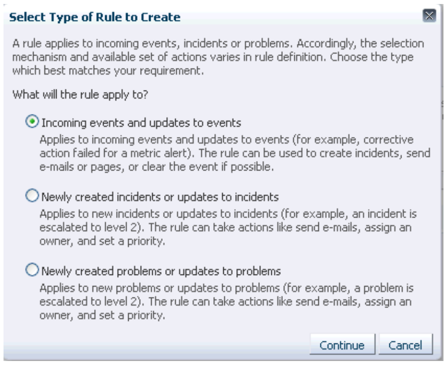
Escalate to

3.4.8.6 Creating Incidents On Non-symptom Events

You can leverage Incident Manager's RCA capability creating rule sets that generate incidents. For monitoring situations where a high number of *symptom* target down events are generated, but only a few non-symptom target down events, you can create rule sets that generate incidents and send notifications only for non-symptom events.

To create a rule set that creates incidents for non-symptom target down events:

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. Click **Create Rule Set...** You then create the rule as part of creating the rule set.
3. Select the rule set that will contain the new rule. Click **Edit...** in the Rules tab of the Edit Rule Set page, and then:
   1. Click **Create ...**
   2. Select "Incoming events and updates to events."



Select Type of Rule to Create ☒

A rule applies to incoming events, incidents or problems. Accordingly, the selection mechanism and available set of actions varies in rule definition. Choose the type which best matches your requirement.

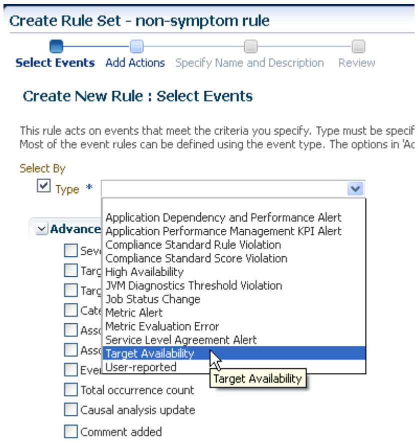
What will the rule apply to?

● Incoming events and updates to events
Applies to incoming events and updates to events (for example, corrective action failed for a metric alert). The rule can be used to create incidents, send e-mails or pages, or clear the event if possible.

○ Newly created incidents or updates to incidents
Applies to new incidents or updates to incidents (for example, an incident is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

○ Newly created problems or updates to problems
Applies to new problems or updates to problems (for example, a problem is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

3. Click **Continue**. The *Create New Rule : Select Events* dialog displays.



Create Rule Set - non-symptom rule

Create New Rule : Select Events

This rule acts on events that meet the criteria you specify. Type must be specif
Most of the event rules can be defined using the event type. The options in 'Ac

Select By

☑ Type *

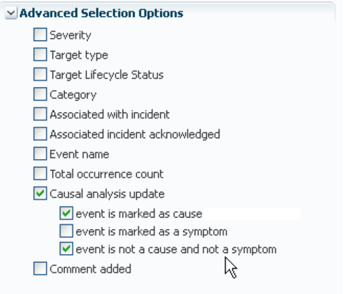
4. In the Advanced Selection Options region, choose *Causal analysis update*. Three causal event options display.

   event is marked as cause: A target down is considered a cause if other targets depending on it are down.

   event is marked as a symptom: A target down is considered a symptom if a target it depends on is also down.

   event is not a cause and not a symptom: A target down is neither a cause or symptom.

   By selecting one or more options, you can filter out extraneous target down events and focus on those target availability events that pertain to targets with interdependencies. To create an incident for only non-symptom events, choose *event is marked as cause* and *event is not a cause and not a symptom*.



Advanced Selection Options

☐ Severity
☐ Target type
☐ Target Lifecycle Status
☐ Category
☐ Associated with incident
☐ Associated incident acknowledged
☐ Event name
☐ Total occurrence count
☑ Causal analysis update
☑ event is marked as cause
☐ event is marked as a symptom
☑ event is not a cause and not a symptom
☐ Comment added

Click **Next**.

5. On the *Create New Rule : Add Actions* page, click **Add**. The *Add Conditional Actions* page displays.
6. In the *Create Incident or Update Incident* region, choose **Create Incident**.
7. Specify the remaining assignment and notification details and click **Continue**.
8. Complete the remaining *Create Rule Set* wizard pages. See "Creating a Rule Set" on page 3-33 for more information on creating rule sets.

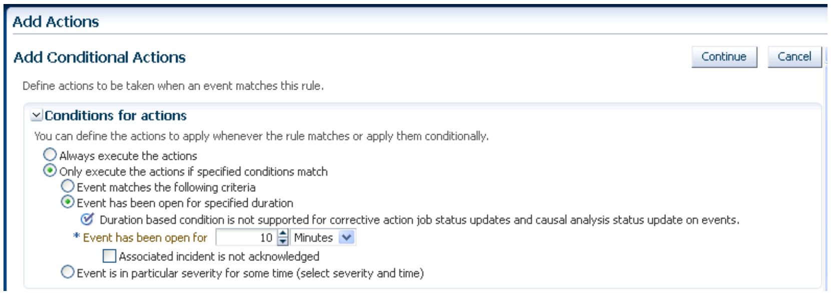
3.4.8.7 Introducing a Time Delay

As mentioned previously, Incident Manager RCA is an iterative process whereby incoming target down events are continually being evaluated, resulting in updates to causal analysis states. Over a period of time (minutes), a root cause may or may not remain a root cause depending on incoming target down events. The original target down event may later be classified as a symptom. To allow time for target down events to be reported, analyzed, and then acted upon (such as creating an incident), you can define an event evaluation time delay when creating a rule set.

In the previous example, where incidents are created for non-symptom events, without a time delay in the rule, there could potentially be an incident created for a non-symptom event that eventually becomes a symptom.

To add a time delay to the rule:

1. From the *Create Rule Set* wizard *Add Actions* page, click **Add** or **Edit** (modify an existing rule). The *Add Conditional Actions* page displays.
2. In the *Conditions for Actions* region, choose **Only execute the actions if specified conditions match**. A list of conditions displays.
3. Choose **Event has been open for specified duration**.
4. Specify the desired time delay.



Add Actions

Add Conditional Actions

Define actions to be taken when an event matches this rule.

Conditions for actions

You can define the actions to apply whenever the rule matches or apply them conditionally.

○ Always execute the actions
● Only execute the actions if specified conditions match
○ Event matches the following criteria
● Event has been open for specified duration
Duration based condition is not supported for corrective action job status updates and causal analysis status update on events.
* Event has been open for 10 Minutes
☐ Associated incident is not acknowledged
○ Event is in particular severity for some time (select severity and time)

5. Click **Continue** and complete the remaining steps in the wizard.

3.5 Moving from Enterprise Manager 10/11g to 12c

Enterprise Manager 12c incident management functionality leverages your existing pre-12c monitoring setup out-of-box. Migration is seamless and transparent. For example, if your Enterprise Manager 10/11g monitoring system sends you emails based on specific monitoring conditions, you will continue to receive those emails without interruption. To take advantage of 12c features, however, you may need to perform additional migration tasks.

> **Important:** Alerts that were generated pre-12c will still be available. For example, critical metric alerts will be available as critical incidents.

Rules

When you migrate to Enterprise Manger 12c, all of your existing notification rules are automatically converted to rules. Technically, they are converted to event rules first with incidents automatically being created for each event rule.

In general, event rules allow you to define which events should become incidents. However, they also allow you to take advantage of the Enterprise Manager's increased monitoring flexibility.

For more information on rule migration, see the following documents:

- Appendix A, " Overview of Notification in Enterprise Manager Cloud Control" section "Migrating Notification Rules to Rule Sets" in the *Enterprise Manager Cloud Control Upgrade Guide*.
- Chapter 29 "Updating Rules" in the *Enterprise Manager Cloud Control Upgrade Guide*.

Privilege Requirements

The *Create Enterprise Rule Set* resource privilege is now required in order to edit/create enterprise rule sets and rules contained within. The exception to this is migrated notification rules. When pre-12c notification rules are migrated to event rules, the original notification rule owners will still be able to edit their own rules without having been granted the Create Enterprise Rule Set resource privilege. However, they must be granted the *Create Enterprise Rule Set* resource privilege if they wish to create new rules. Enterprise Manager Super Administrators, by default, can edit and create rule sets.

Monitoring: Common Tasks

The following sections provide "how-to" examples illustrating common tasks for incident/monitoring setup and usage.

- "Setting Up an Email Gateway" on page 3-76
- "Sending Email for Metric Alerts" on page 3-78
- "Sending SNMP Traps for Metric Alerts" on page 3-82
- "Sending Events to an Event Connector" on page 3-87
- "Sending Email to Different Email Addresses for Different Periods of the Day" on page 3-91

Setting Up an Email Gateway

Task

In order for Enterprise Manager to send email notifications to administrators, it must access an available email gateway within your organization. The instructions below step you through the process of configuring Enterprise Manager to use a designated email gateway.

User Roles

- Enterprise Manager Administrator

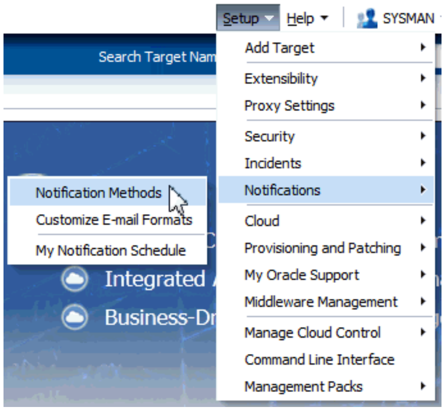
Prerequisites

- User must have Super Administrator privileges.

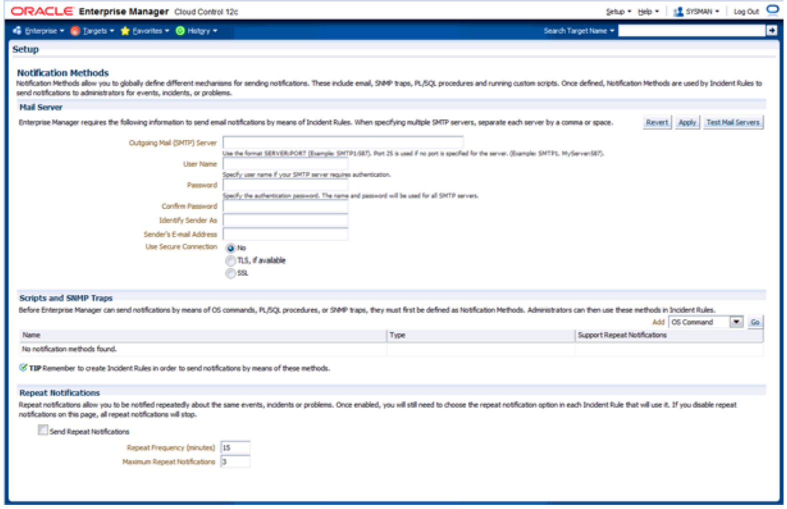
  For more information, see "Setting Up a Mail Server for Notifications" on page 4-2.

How to do it:

1. From the **Setup** menu, select **Notifications**, then select **Notification Methods**.



   The Notification Methods page displays.



Setup

Notification Methods

Notification Methods allow you to globally define different mechanisms for sending notifications. These include email, SNMP traps, PL/SQL procedures and running custom scripts. Once defined, Notification Methods are used by Incident Rules to send notifications to administrators for events, incidents, or problems.

Mail Server

Enterprise Manager requires the following information to send email notifications by means of Incident Rules. When specifying multiple SMTP servers, separate each server by a comma or space. Revert Apply Test Mail Servers

Outgoing Mail (SMTP) Server
Use the format SERVER:PORT (Example: SMTP1:587). Port 25 is used if no port is specified for the server. (Example: SMTP1, MyServer:587).
User Name
Specify user name if your SMTP server requires authentication.
Password
Specify the authentication password. The name and password will be used for all SMTP servers.
Confirm Password
Identify Sender As
Sender's E-mail Address
Use Secure Connection ● No ○ TLS, if available ○ SSL

Scripts and SNMP Traps

Before Enterprise Manager can send notifications by means of OS commands, PL/SQL procedures, or SNMP traps, they must first be defined as Notification Methods. Administrators can then use these methods in Incident Rules.

Add OS Command Go

Name	Type	Support Repeat Notifications
No notification methods found.		

TIP Remember to create Incident Rules in order to send notifications by means of these methods.

Repeat Notifications

Repeat notifications allow you to be notified repeatedly about the same events, incidents or problems. Once enabled, you will still need to choose the repeat notification option in each Incident Rule that will use it. If you disable repeat notifications on this page, all repeat notifications will stop.

□ Send Repeat Notifications

Repeat Frequency (minutes) 15
Maximum Repeat Notifications 3

2. Enter the requisite parameters. The following examples illustrate valid parameter values.

- **Outgoing Mail (SMTP) Server -** smtp01.example.com:587, smtp02.example.com
- **User Name -** myadmin
- **Password -** ******
- **Confirm Password -** ******
- **Identify Sender As -** Enterprise Manager
- **Sender's Email Address -** mgmt_rep@example.com
- **Use Secure Connection** - *No*: Email is not encrypted. *SSL*: Email is encrypted using the Secure Sockets Layer protocol. *TLS, if available*: Email is encrypted using the Transport Layer Security protocol if the mail server supports TLS. If the server does not support TLS, the email is automatically sent as plain text.

3. Ensure Enterprise Manager can connect to the specified email gateway. Click **Test Mail Servers**. Enterprise Manager displays a success/failure message. Click **OK** to return to the Notification Methods page.
4. Once Enterprise Manager verifies that it can successfully connect to your email gateway, click **Apply**.

What you have accomplished:

At this point, you have configured Enterprise Manager to use your corporate email gateway. Enterprise Manager can now notify registered users while monitoring conditions within your managed environment.

What's next?

"Defining E-mail Addresses" on page 4-5

"Setting Up a Notification Schedule" on page 4-6

"Setting Up E-mail for Yourself" on page 4-5

"Setting Up E-mail for Other Administrators" on page 4-9

Sending Email for Metric Alerts

Task

Configure Enterprise Manager to send email to administrators when a metric alert threshold is reached. In this example, you want to send an email notification when a metric alert is raised when CPU Utilization reaches Critical severity.

User Roles

- IT Operator/Manager
- Enterprise Manager Administrator

Prerequisites

- Set up an Email Gateway that allows Enterprise Manager to send email to administrators.

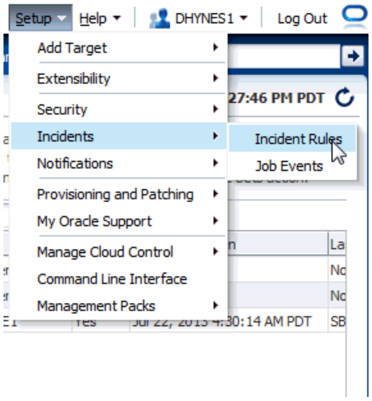
  For more information, see "Setting Up a Mail Server for Notifications" on page 4-2.
- Metric thresholds have been set for CPU Utilization.
- User's Enterprise Manager account has been granted the appropriate privileges to manage incidents from his managed system.

  For information, see "Setting Up Administrators and Privileges" on page 3-26.
- User's Enterprise Manager account has notification preferences (email and schedule). This is required not just for the administrator who is creating/editing a rule, but also for any user who is being notified as a result of the rule action.

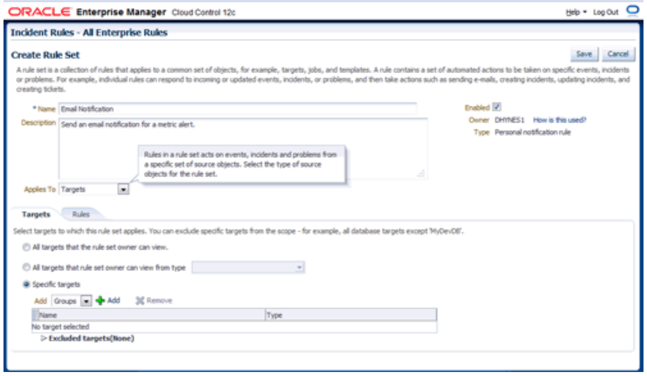
  For more information, see "Setting Up a Notification Schedule" on page 4-6.

How to do it:

1. From the **Setup** menu, select **Incidents,** then select **Incident Rules.**



2. Click **Create Rule Set.**
3. Enter a name and description for the rule set.



Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name: Email Notification

Description: Send an email notification for a metric alert.

Rules in a rule set acts on events, incidents and problems from a specific set of source objects. Select the type of source objects for the rule set.

Applies To: Targets

Enabled: ☑

Owner: DHYNES1 How is this used?

Type: Personal notification rule

Select targets to which this rule set applies. You can exclude specific targets from the scope - for example, all database targets except 'MyDevDB'.

○ All targets that the rule set owner can view.

○ All targets that rule set owner can view from type

● Specific targets

Add: Groups

Name	Type
No target selected	

4. In the Targets tab, select **All targets that the rule set owner can view**.

Alternative: *Having the rule set apply to specific targets/group.*

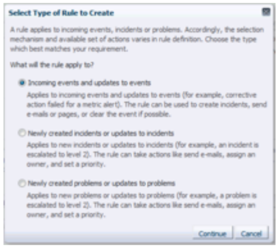
Although we have chosen to have the rule set apply to all targets in this example, alternatively, you can have a rule set apply only to specific targets or groups.

To do this:

1. From the Targets tab, select **Specific targets**.
2. From the Add drop-down menu, choose **Groups** or **Targets**
3. Click **Add**. The Target selector dialog displays.
4. Either search for a target/group name or select one from the table.
5. Click **Select** once you have chosen the targets/groups of interest. The dialog closes and the targets appear in the Specific Targets list.

---

5. In the Rules tab, click **Create.** The Select Type of Rule to Create dialog appears.



Select Type of Rule to Create

A rule applies to incoming events, incidents or problems. Accordingly, the selection mechanism and available set of actions varies in rule definition. Choose the type which best matches your requirement.

What will the rule apply to?

● Incoming events and updates to events

Applies to incoming events and updates to events (for example, corrective action failed for a metric alert). The rule can be used to create incidents, send e-mails or pages, or clear the event if possible.

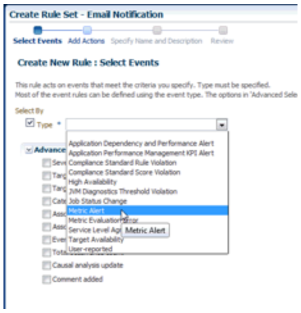
○ Newly created incidents or updates to incidents

Applies to new incidents or updates to incidents (for example, an incident is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

○ Newly created problems or updates to problems

Applies to new problems or updates to problems (for example, a problem is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

6. Select **Incoming events and updates to events,** and click **Continue.**
7. On the Select Events page, set the criteria for events based on which the rule should act. In this case, choose **Metric Alert** from the drop down list.


Select Events
Add Actions
Specify Name and Description
Review
Advance
Application Dependency and Performance Alert
Application Performance Management KPI Alert
Compliance Standard Rule Violation
Compliance Standard Score Violation
High Availability
JVM Diagnostics Threshold Violation
Job Status Change
Metric Alert
Metric Evaluation Error
Service Level Agr
Target Availability
User-reported
Metric Alert
Causal analysis update
Comment added

Create Rule Set - Email Notification

Create New Rule : Select Events

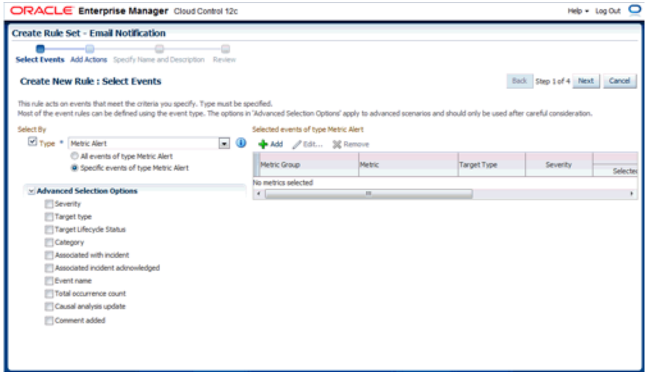
This rule acts on events that meet the criteria you specify. Type must be specified. Most of the event rules can be defined using the event type. The options in 'Advanced Sele

Select By

☑ Type *

Click **Next.**

8. Select the **Specific events of type Metric Alert** option. A metric selection area displays:



Create Rule Set - Email Notification

Create New Rule : Select Events

This rule acts on events that meet the criteria you specify. Type must be specified.
Most of the event rules can be defined using the event type. The options in 'Advanced Selection Options' apply to advanced scenarios and should only be used after careful consideration.

Select By

☑ Type * Metric Alert

○ All events of type Metric Alert
● Specific events of type Metric Alert

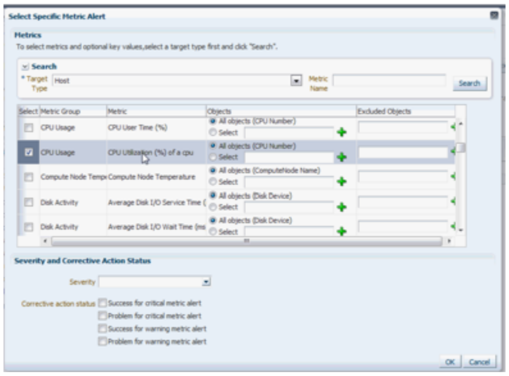
Advanced Selection Options

□ Severity
□ Target type
□ Target Lifecycle Status
□ Category
□ Associated with incident
□ Associated incident acknowledged
□ Event name
□ Total occurrence count
□ Causal analysis update
□ Comment added

Selected events of type Metric Alert

Metric Group	Metric	Target Type	Severity	Selecte
No metrics selected				

In this example, we only want to send notifications for CPU % Utilization greater reaches the defined Critical threshold.



Select Specific Metric Alert

Metrics

To select metrics and optional key values,select a target type first and click "Search".

Search

* Target Type: Host

Metric Name:

Select	Metric Group	Metric	Objects	Excluded Objects
□	CPU Usage	CPU User Time (%)	● All objects (CPU Number) ○ Select	
☑	CPU Usage	CPU Utilization (%) of a cpu	● All objects (CPU Number) ○ Select	
□	Compute Node Temp	Compute Node Temperature	● All objects (ComputeNode Name) ○ Select	
□	Disk Activity	Average Disk I/O Service Time (	● All objects (Disk Device) ○ Select	
□	Disk Activity	Average Disk I/O Wait Time (ms	● All objects (Disk Device) ○ Select	

Severity and Corrective Action Status

Severity:

Corrective action status:
□ Success for critical metric alert
□ Problem for critical metric alert
□ Success for warning metric alert
□ Problem for warning metric alert

9. Choose Severity **Critical** from the drop down menu.

   Click **OK**.

10. Click **Next**.

11. On the Add Actions page, click **Add** and add actions to be taken by the rule. In the Notifications section, enter the email addresses where the notifications must be send. Click **Next.**

    Multiple conditional actions can be specified and evaluated sequentially (top down) in the order you add them.

Alternative: *Sending email notifications to mailing list.*

In addition to specifying email addresses, you may also specify defined Enterprise Manager administrators. Mailing distribution lists can also be specified to notify entire categories of users. Using mailing lists allows you to change who gets notified without having to update individual rule sets.

---

12. On the Specify Name and Description page, enter a name and description for the rule. Click **Next.**

13. On the review page, review the details, and click **Continue.**

14. On the Create Rule Set page, click **Save.**

What you have accomplished:

At this point, you have created a new rule set that will send an administrator email a notification whenever the CPU Utilization reaches the Critical metric threshold. To subscribe to this rule set, see "Subscribing to Receive Email from a Rule" on page 3-39 for further instructions.

What's Next?

- How Do I Set Up Email Notifications for Other Administrators
- Add/Update/Delete Email Addresses and Define a Notification Schedule
- "Responding and Working on a Simple Incident" on page 3-46

Sending SNMP Traps for Metric Alerts

Task

You want to configure Enterprise Manager to send event information (for example, a metric alert) via SNMP trap to an HP Openview console. This is done in two phases

1. Create a notification method to send the SNMP Trap
2. Create an incident rule to send an SNMP trap when a metric alert is raised.

User Roles

- Enterprise Manager Administrator

Prerequisites

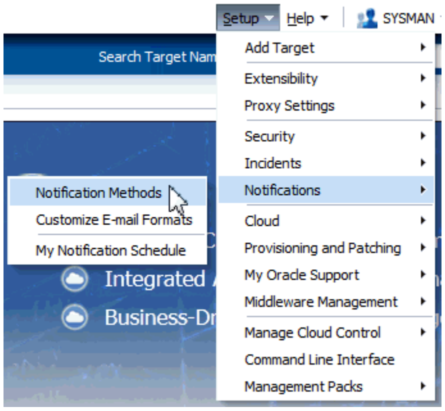
- User must have Super Administrator privileges.

  For more information, see "Setting Up a Mail Server for Notifications" on page 4-2.

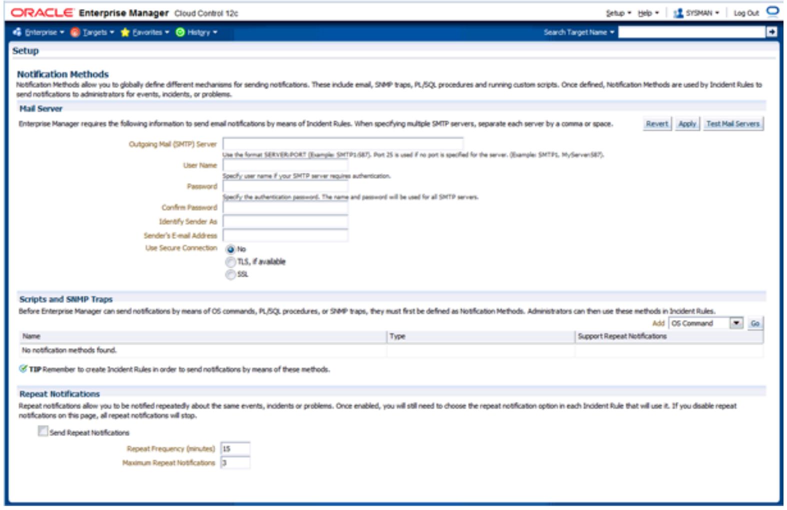
How to do it:

Create a notification method based on an SNMP Trap.

1. From the **Setup** menu, select **Notifications**, then select **Notification Methods**.



The Notification Methods page displays.



Notification Methods

Notification Methods allow you to globally define different mechanisms for sending notifications. These include email, SNMP traps, PL/SQL procedures and running custom scripts. Once defined, Notification Methods are used by Incident Rules to send notifications to administrators for events, incidents, or problems.

Mail Server

Enterprise Manager requires the following information to send email notifications by means of Incident Rules. When specifying multiple SMTP servers, separate each server by a comma or space.

Outgoing Mail (SMTP) Server

Use the format SERVER:PORT (Example: SMTP1:587). Port 25 is used if no port is specified for the server. (Example: SMTP1, MyServer:587).

User Name

Specify user name if your SMTP server requires authentication.

Password

Specify the authentication password. The name and password will be used for all SMTP servers.

Confirm Password

Identify Sender As

Sender's E-mail Address

Use Secure Connection ● No ○ TLS, if available ○ SSL

Scripts and SNMP Traps

Before Enterprise Manager can send notifications by means of OS commands, PL/SQL procedures, or SNMP traps, they must first be defined as Notification Methods. Administrators can then use these methods in Incident Rules.

Name	Type	Support Repeat Notifications
No notification methods found.		

TIP Remember to create Incident Rules in order to send notifications by means of these methods.

Repeat Notifications

Repeat notifications allow you to be notified repeatedly about the same events, incidents or problems. Once enabled, you will still need to choose the repeat notification option in each Incident Rule that will use it. If you disable repeat notifications on this page, all repeat notifications will stop.

□ Send Repeat Notifications

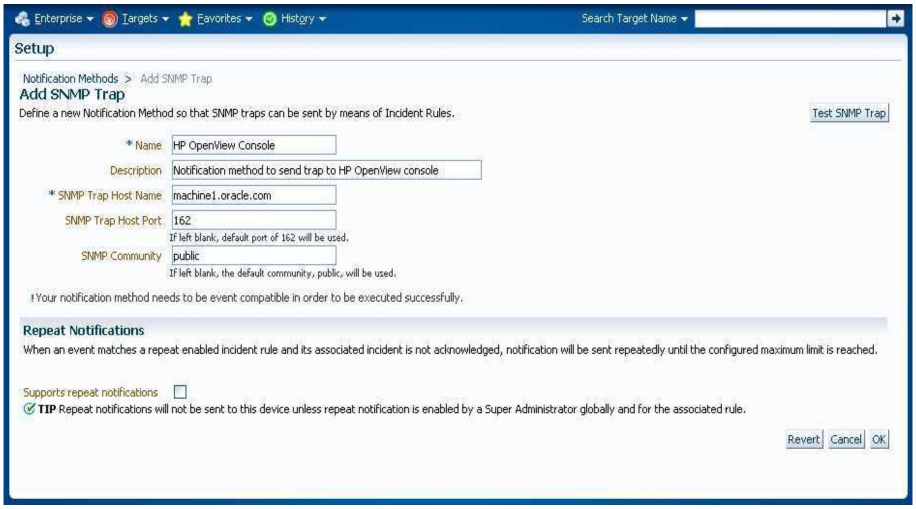
Repeat Frequency (minutes) 15

Maximum Repeat Notifications 3

2. From the **Add** drop-down menu, choose **SNMP Trap** and then click **Go**. The Add SNMP Trap page displays.

   You must provide the name of the host (machine) on which the SNMP master agent is running and other details as shown in the following graphic.

   The following examples illustrate valid parameter values.



Add SNMP Trap

Define a new Notification Method so that SNMP traps can be sent by means of Incident Rules.

* Name: HP OpenView Console

Description: Notification method to send trap to HP OpenView console

* SNMP Trap Host Name: machine1.oracle.com

SNMP Trap Host Port: 162
If left blank, default port of 162 will be used.

SNMP Community: public
If left blank, the default community, public, will be used.

! Your notification method needs to be event compatible in order to be executed successfully.

Repeat Notifications

When an event matches a repeat enabled incident rule and its associated incident is not acknowledged, notification will be sent repeatedly until the configured maximum limit is reached.

Supports repeat notifications □

✓ **TIP** Repeat notifications will not be sent to this device unless repeat notification is enabled by a Super Administrator globally and for the associated rule.

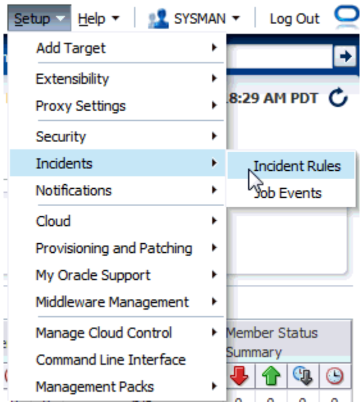
3. Click **Test SNMP Trap** to validate the SNMP trap settings. Enterprise Manager displays a success/failure message. Click **OK** to return to the Add SNMP Trap page.

4. Click **OK** to return to the Notification Methods page.

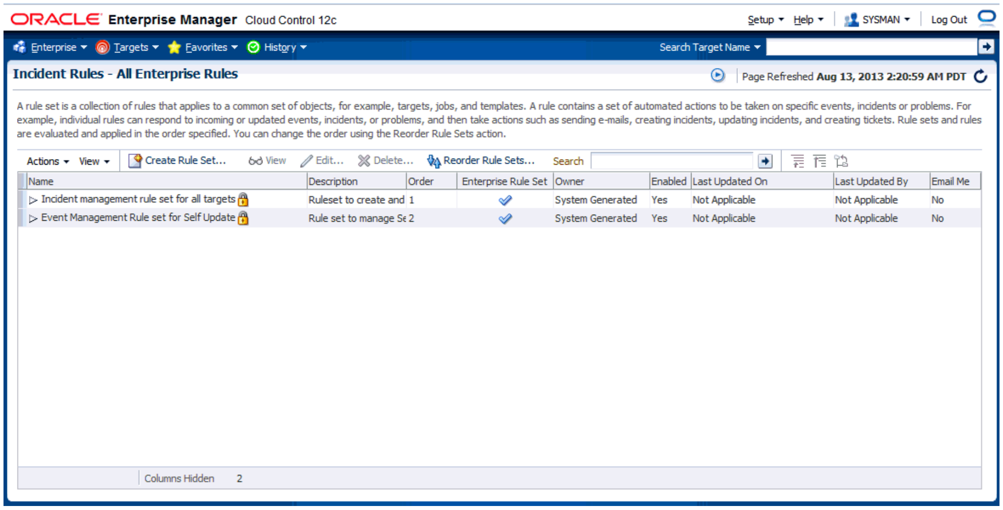
5. Click **OK** to add the new SNMP Trap-based notification method.

Create an incident rule to send an SNMP trap when a metric alert is raised.

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.



   The Incident Rules - All Enterprise Rules page displays.



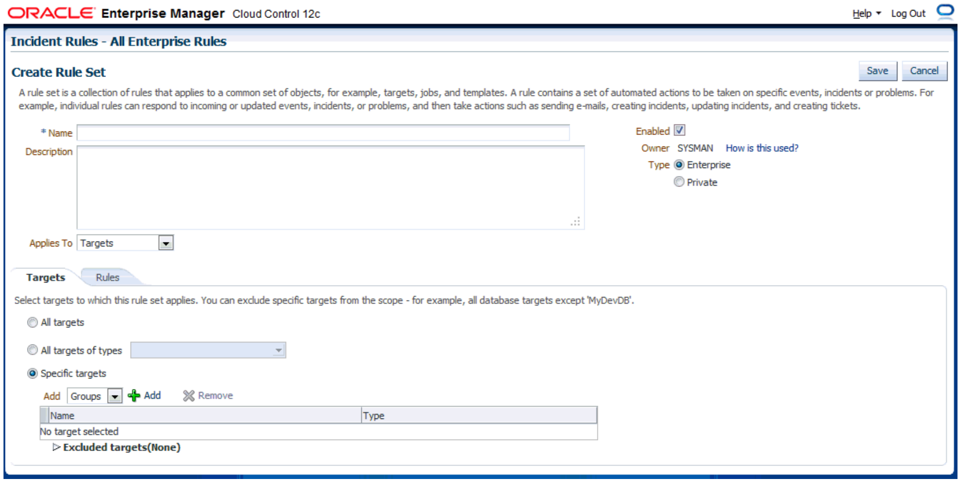
Incident Rules - All Enterprise Rules

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. Rule sets and rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule Sets action.

Name	Description	Order	Enterprise Rule Set	Owner	Enabled	Last Updated On	Last Updated By	Email Me
▷ Incident management rule set for all targets	Ruleset to create and	1	✓	System Generated	Yes	Not Applicable	Not Applicable	No
▷ Event Management Rule set for Self Update	Rule set to manage Se	2	✓	System Generated	Yes	Not Applicable	Not Applicable	No

Columns Hidden 2

2. On the Incident Rules - All Enterprise Rules page, click **Create Rule Set...** The Create Rule Set page displays.



Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name

Description

Applies To Targets

Enabled ☑

Owner SYSMAN How is this used?

Type ● Enterprise ○ Private

Select targets to which this rule set applies. You can exclude specific targets from the scope - for example, all database targets except 'MyDevDB'.

○ All targets

○ All targets of types

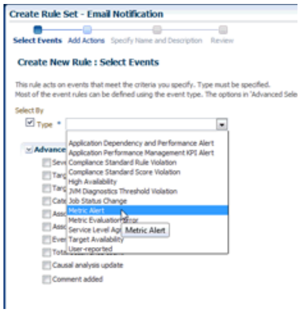
● Specific targets

Add Groups

Name	Type
No target selected	

▷ Excluded targets(None)

3. Enter the rule set **Name**, a brief **Description**, and select the type of source object the rule **Applies to** (Targets).
4. Click on the **Rules** tab and then click **Create...**
5. On the Select Type of Rule to Create dialog, select **Incoming events and updates to events** and then click **Continue**.
6. On the Select Events page, set the criteria for events based on which the rule should act. In this case, choose **Metric Alert** from the drop down list.



Create Rule Set - Email Notification

Create New Rule : Select Events

This rule acts on events that meet the criteria you specify. Type must be specified.
Most of the event rules can be defined using the event type. The options in 'Advanced Sele

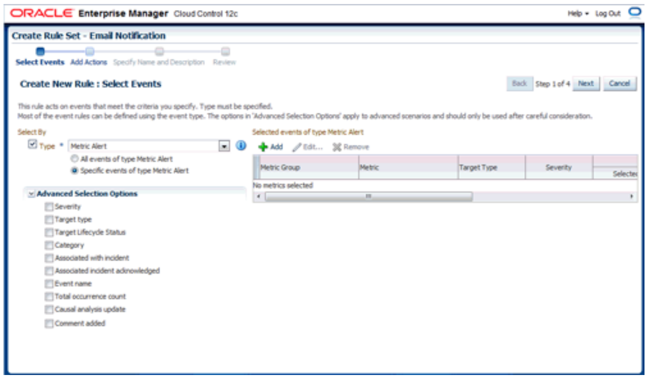
Select By

☑ Type *

Select Events
Add Actions
Specify Name and Description
Review
Advance
Application Dependency and Performance Alert
Application Performance Management KPI Alert
Compliance Standard Rule Violation
Compliance Standard Score Violation
High Availability
JVM Diagnostics Threshold Violation
Job Status Change
Metric Alert
Metric Evaluation Error
Service Level Agr
Target Availability
User-reported
Metric Alert
□ Causal analysis update
□ Comment added

Click **Next.**

7. Select the **Specific events of type Metric Alert** option. A metric selection area displays:



ORACLE Enterprise Manager Cloud Control 12c
Help
Log Out
Select Events
Add Actions
Specify Name and Description
Review
Back
Next
Cancel
Add
Edit...
Remove

Create Rule Set - Email Notification

Create New Rule : Select Events

Step 1 of 4

This rule acts on events that meet the criteria you specify. Type must be specified.
Most of the event rules can be defined using the event type. The options in 'Advanced Selection Options' apply to advanced scenarios and should only be used after careful consideration.

Select By

☑ Type * Metric Alert

○ All events of type Metric Alert

● Specific events of type Metric Alert

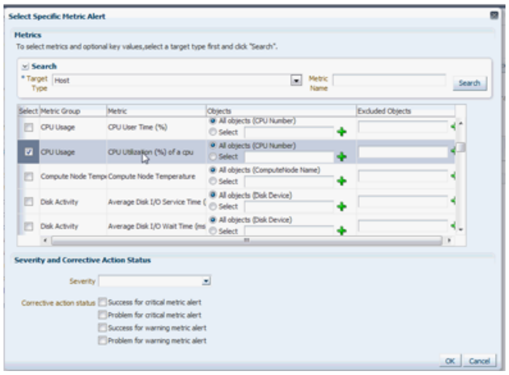
Advanced Selection Options

□ Severity
□ Target type
□ Target Lifecycle Status
□ Category
□ Associated with incident
□ Associated incident acknowledged
□ Event name
□ Total occurrence count
□ Causal analysis update
□ Comment added

Selected events of type Metric Alert

Metric Group	Metric	Target Type	Severity	Selected
No metrics selected				

In this example, we only want to send notifications for CPU % Utilization greater reaches the defined Critical threshold.



Select Specific Metric Alert

Metrics

To select metrics and optional key values,select a target type first and click "Search".

Search

* Target Type: Host

Metric Name:

Select	Metric Group	Metric	Objects	Excluded Objects
□	CPU Usage	CPU User Time (%)	● All objects (CPU Number) ○ Select	
☑	CPU Usage	CPU Utilization (%) of a cpu	● All objects (CPU Number) ○ Select	
□	Compute Node Tempe	Compute Node Temperature	● All objects (ComputeNode Name) ○ Select	
□	Disk Activity	Average Disk I/O Service Time (	● All objects (Disk Device) ○ Select	
□	Disk Activity	Average Disk I/O Wait Time (ms	● All objects (Disk Device) ○ Select	

Severity and Corrective Action Status

Severity

Corrective action status
□ Success for critical metric alert
□ Problem for critical metric alert
□ Success for warning metric alert
□ Problem for warning metric alert

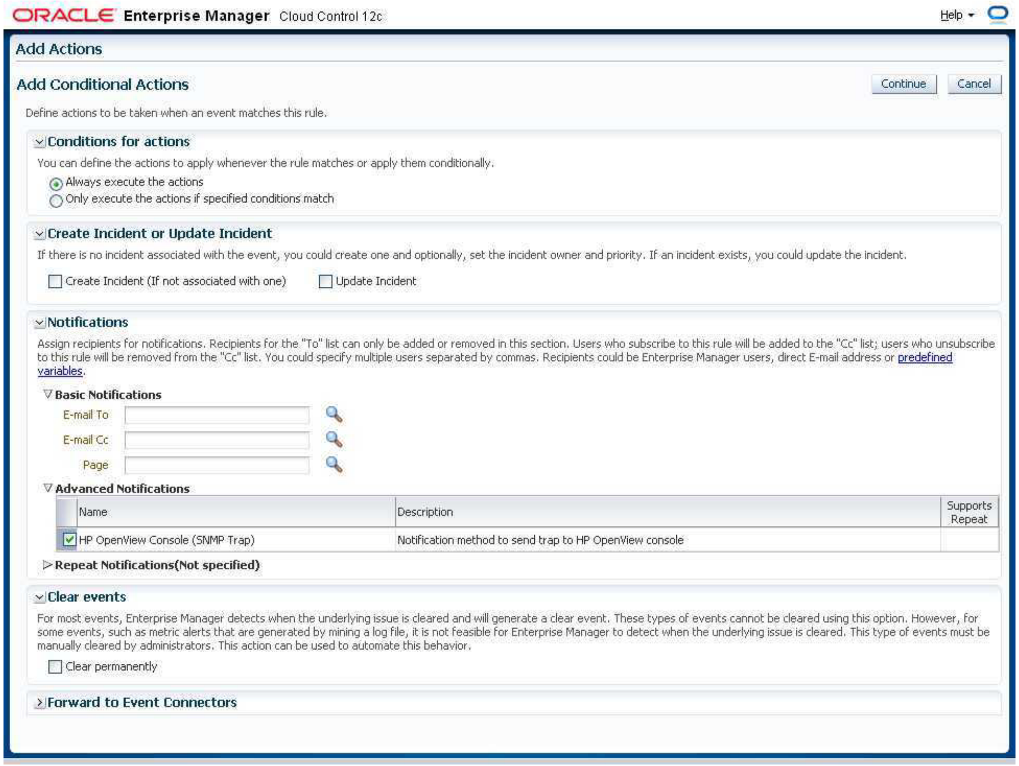
8. Choose Severity **Critical** from the drop down menu.

   Click **OK**.

9. Click **Next**.

10. On the Create New Rule : Add Actions page, click **Add**. The Add Conditional Actions page displays.

11. In the Notifications section, under Advanced Notifications, select an existing SNMP trap notification method as shown in the following graphic.



Add Actions

Add Conditional Actions

Define actions to be taken when an event matches this rule.

Conditions for actions

You can define the actions to apply whenever the rule matches or apply them conditionally.

● Always execute the actions
○ Only execute the actions if specified conditions match

Create Incident or Update Incident

If there is no incident associated with the event, you could create one and optionally, set the incident owner and priority. If an incident exists, you could update the incident.

□ Create Incident (If not associated with one) □ Update Incident

Notifications

Assign recipients for notifications. Recipients for the "To" list can only be added or removed in this section. Users who subscribe to this rule will be added to the "Cc" list; users who unsubscribe to this rule will be removed from the "Cc" list. You could specify multiple users separated by commas. Recipients could be Enterprise Manager users, direct E-mail address or predefined variables.

Basic Notifications

E-mail To

E-mail Cc

Page

Advanced Notifications

	Name	Description	Supports Repeat
☑	HP OpenView Console (SNMP Trap)	Notification method to send trap to HP OpenView console	

Repeat Notifications(Not specified)

Clear events

For most events, Enterprise Manager detects when the underlying issue is cleared and will generate a clear event. These types of events cannot be cleared using this option. However, for some events, such as metric alerts that are generated by mining a log file, it is not feasible for Enterprise Manager to detect when the underlying issue is cleared. This type of events must be manually cleared by administrators. This action can be used to automate this behavior.

□ Clear permanently

Forward to Event Connectors

For information on creating SNMP trap notification methods, see "Sending SNMP Traps to Third Party Systems" on page 4-38.

12. Click **Continue** to return to the Create New Rule : Add Actions page.

13. Click **Next** to go to the Create New Rule : Specify Name and Description page.

14. Specify a rule name and a concise description and then click **Next**.

15. Review the rule definition and then click **Continue** add the rule to the rule set. A message displays indicating the rule has been added to the rule set but has not yet been saved. Click **OK** to close the message.

16. Click **Save** to save the rule set. A confirmation is displayed. Click **OK** to close the message.

What you have accomplished:

At this point, you have created an incident rule set that instructs Enterprise Manager to send an SNMP trap to a third-party system whenever a metric alert is raised (%CPU Utilization).

What's next?

- "Subscribing to Receive Email from a Rule" on page 3-39
- "Searching for Incidents" on page 3-44

Sending Events to an Event Connector

Task

You want to send event information from Enterprise Manager to IBM Tivoli Netcool/OMNIbus using a connector. To do so, you must create an incident rule that invokes the IBM Tivoli Netcool/OMNIbus Connector connector.

User Roles

- System Administrator
- IT Operator

Prerequisites

- User must have the Create Enterprise Rule Set resource privilege and at least View privileges on the targets where events are to be forward to Netcool/OMNIbus.

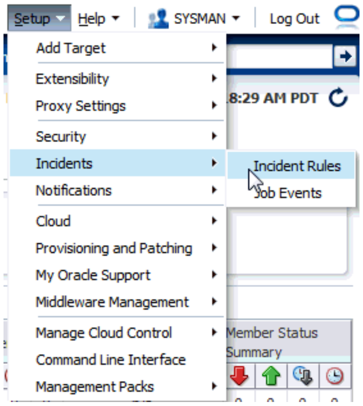
  For more information, see "Setting Up a Mail Server for Notifications" on page 4-2.

- The IBM Tivoli Netcool/OMNIbus connector must be installed and configured.

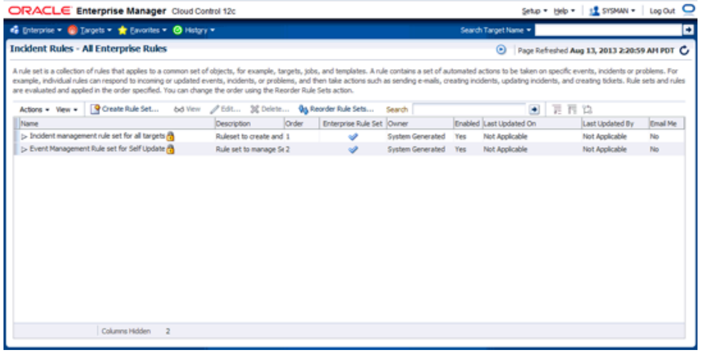
  For more information, see the Oracle® Enterprise Manager IBM Tivoli Netcool/OMNIbus Connector Installation and Configuration Guide.

How to do it:

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.



The Incident Rules - All Enterprise Rules page displays.

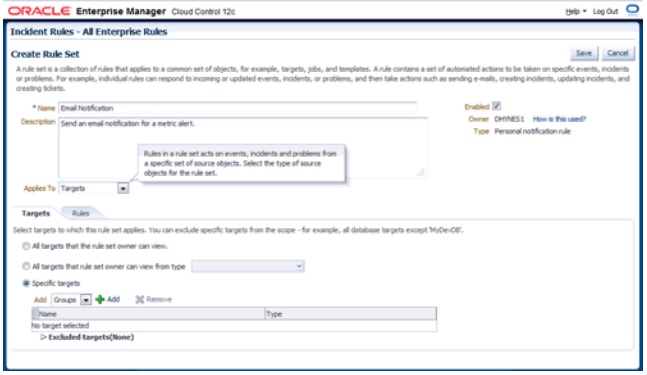


A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets. Rule sets and rules are evaluated and applied in the order specified. You can change the order using the Reorder Rule Sets action.

Name	Description	Order	Enterprise Rule Set	Owner	Enabled	Last Updated On	Last Updated By	Email Me
▷ Incident management rule set for all targets	Ruleset to create and	1	✓	System Generated	Yes	Not Applicable	Not Applicable	No
▷ Event Management Rule set for Self Update	Rule set to manage Sε	2	✓	System Generated	Yes	Not Applicable	Not Applicable	No

2. Click **Create Rule Set.**

3. Enter a name and description for the rule set.



Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name: Email Notification

Description: Send an email notification for a metric alert.

Rules in a rule set acts on events, incidents and problems from a specific set of source objects. Select the type of source objects for the rule set.

Applies To: Targets

Enabled: ☑

Owner: DHYNES1 How is this used?

Type: Personal notification rule

Select targets to which this rule set applies. You can exclude specific targets from the scope - for example, all database targets except 'MyDevDB'.

○ All targets that the rule set owner can view.

○ All targets that rule set owner can view from type

● Specific targets

Add: Groups

No target selected

▷ Excluded targets(None)

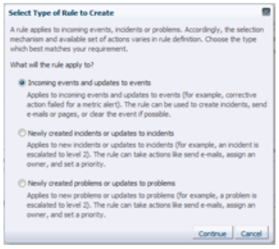
4. In the Targets tab, select **All targets that the rule set owner can view**.

Having the rule set apply to specific targets/groups: Although we have chosen to have the rule set apply to all targets in this example, you can alternatively have a rule set apply only to specific targets or groups.

To do this:

1. From the Targets tab, select **Specific targets**.
2. From the Add drop-down menu, choose **Groups** or **Targets**
3. Click **Add**. The Target selector dialog displays.
4. Either search for a target/group name or select one from the table.
5. Click **Select** once you have chosen the targets/groups of interest. The dialog closes and the targets appear in the Specific Targets list.

5. In the Rules tab, click **Create.** The Select Type of Rule to Create dialog appears.



Select Type of Rule to Create

A rule applies to incoming events, incidents or problems. Accordingly, the selection mechanism and available set of actions varies in rule definition. Choose the type which best matches your requirement.

What will the rule apply to?

● Incoming events and updates to events

Applies to incoming events and updates to events (for example, corrective action failed for a metric alert). The rule can be used to create incidents, send e-mails or pages, or clear the event if possible.

○ Newly created incidents or updates to incidents

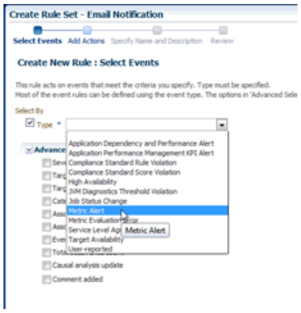
Applies to new incidents or updates to incidents (for example, an incident is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

○ Newly created problems or updates to problems

Applies to new problems or updates to problems (for example, a problem is escalated to level 2). The rule can take actions like send e-mails, assign an owner, and set a priority.

6. Select **Incoming events and updates to events,** and click **Continue.**

7. On the Select Events page, set the criteria for events based on which the rule should act. In this case, choose **Metric Alert** from the drop down list.



Select Events
Add Actions
Specify Name and Description
Review
Advance
Application Dependency and Performance Alert
Application Performance Management KPI Alert
Compliance Standard Rule Violation
Compliance Standard Score Violation
High Availability
JVM Diagnostics Threshold Violation
Job Status Change
Metric Alert
Metric Evaluation Error
Service Level Agr
Target Availability
User-reported
Metric Alert
Causal analysis update
Comment added

Create Rule Set - Email Notification

Create New Rule : Select Events

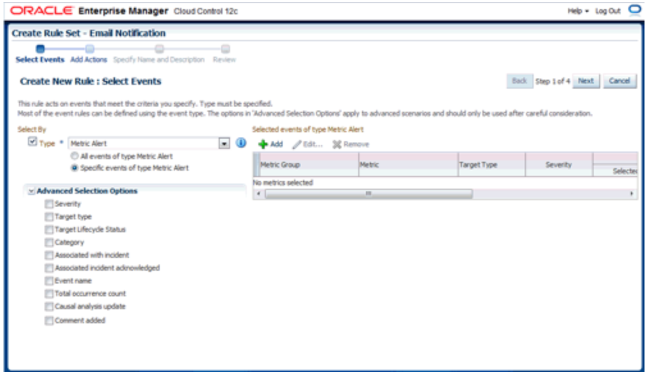
This rule acts on events that meet the criteria you specify. Type must be specified. Most of the event rules can be defined using the event type. The options in 'Advanced Sele

Select By

☑ Type *

Click **Next.**

8. Select the **Specific events of type Metric Alert** option. A metric selection area displays:


ORACLE Enterprise Manager Cloud Control 12c
Help
Log Out
Select Events
Add Actions
Specify Name and Description
Review
Back
Next
Cancel
Add
Edit...
Remove

Create Rule Set - Email Notification

Create New Rule : Select Events

Step 1 of 4

This rule acts on events that meet the criteria you specify. Type must be specified.
Most of the event rules can be defined using the event type. The options in 'Advanced Selection Options' apply to advanced scenarios and should only be used after careful consideration.

Select By

☑ Type * Metric Alert

○ All events of type Metric Alert

● Specific events of type Metric Alert

Advanced Selection Options

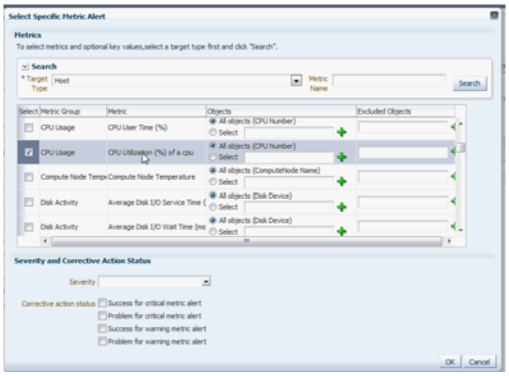
- □ Severity
- □ Target type
- □ Target Lifecycle Status
- □ Category
- □ Associated with incident
- □ Associated incident acknowledged
- □ Event name
- □ Total occurrence count
- □ Causal analysis update
- □ Comment added

Selected events of type Metric Alert

Metric Group	Metric	Target Type	Severity	Selected

No metrics selected

In this example, we only want to send notifications for CPU % Utilization greater reaches the defined Critical threshold.



Select Specific Metric Alert

Metrics

To select metrics and optional key values,select a target type first and click "Search".

Search

* Target Type Host

Metric Name

Select	Metric Group	Metric	Objects	Excluded Objects
□	CPU Usage	CPU User Time (%)	● All objects (CPU Number) ○ Select	
☑	CPU Usage	CPU Utilization (%) of a cpu	● All objects (CPU Number) ○ Select	
□	Compute Node Temp	Compute Node Temperature	● All objects (ComputeNode Name) ○ Select	
□	Disk Activity	Average Disk I/O Service Time (	● All objects (Disk Device) ○ Select	
□	Disk Activity	Average Disk I/O Wait Time (ms	● All objects (Disk Device) ○ Select	

Severity and Corrective Action Status

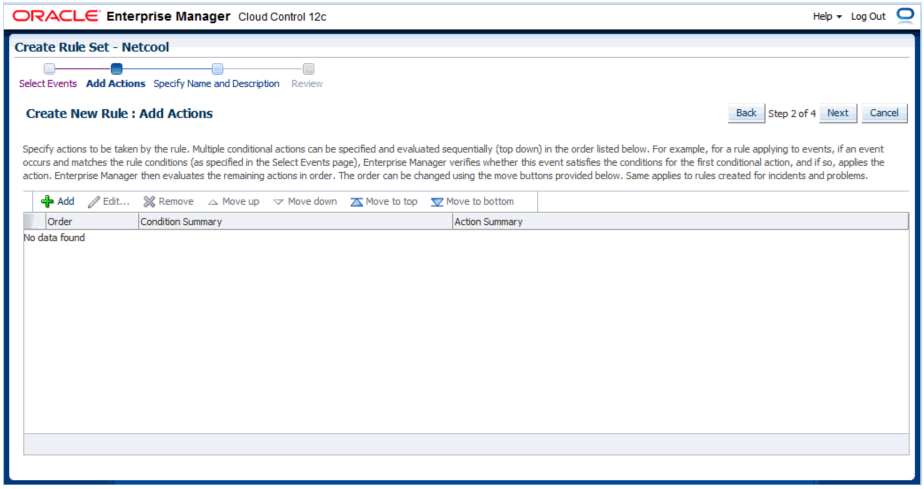
Severity

Corrective action status
□ Success for critical metric alert
□ Problem for critical metric alert
□ Success for warning metric alert
□ Problem for warning metric alert

9. Choose Severity **Critical** from the drop down menu.

   Click **OK**.

10. Click **Next**. The Add Actions page displays.



Create Rule Set - Netcool

Create New Rule : Add Actions

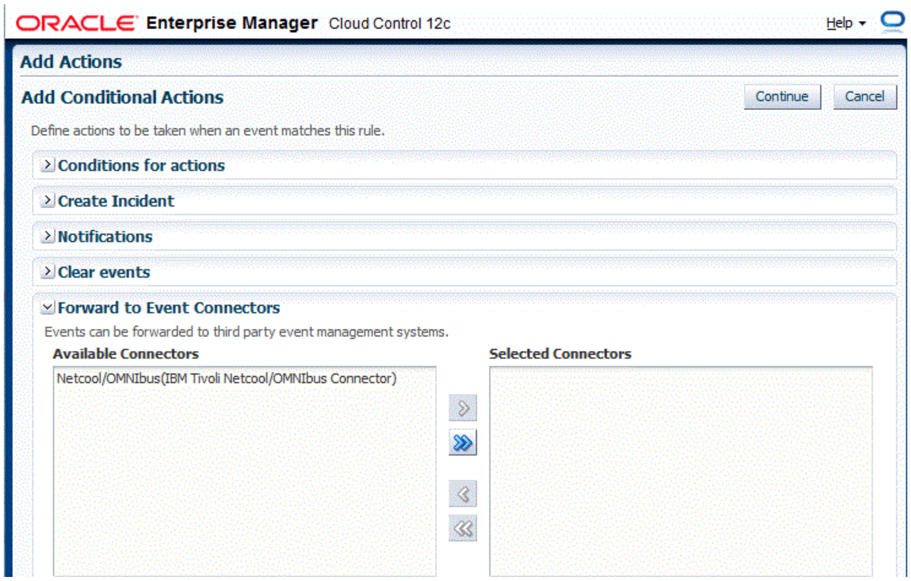
Step 2 of 4

Specify actions to be taken by the rule. Multiple conditional actions can be specified and evaluated sequentially (top down) in the order listed below. For example, for a rule applying to events, if an event occurs and matches the rule conditions (as specified in the Select Events page), Enterprise Manager verifies whether this event satisfies the conditions for the first conditional action, and if so, applies the action. Enterprise Manager then evaluates the remaining actions in order. The order can be changed using the move buttons provided below. Same applies to rules created for incidents and problems.

Order	Condition Summary	Action Summary

No data found

11. Click **Add**. The Add Conditional Actions page displays.



Define actions to be taken when an event matches this rule.

Events can be forwarded to third party event management systems.

Netcool/OMNIbus(IBM Tivoli Netcool/OMNIbus Connector)

12. Select one or more connector instances listed in the Forward to Event Connectors section and, click > button to add the connector to the Selected Connectors list and then click **Continue**.
13. The Add Actions page appears again and lists the new action.
14. Click **Next**. The Specify Name and Description page displays.
15. Enter a name and description for the rule, then click **Next**. The Review page displays.
16. Click **Continue** if everything appears correct.

    An information pop-up appears that states, "Rule has been successfully added to the current rule set. Newly added rules are not saved until the Save button is clicked."

    You can click **Back** and make corrections to the rule if necessary.

What you have accomplished:

At this point, you have created a rule that invokes the IBM Tivoli Netcool/OMNIbus Connector connector when a metric alert is raised.

What’s next?

"Subscribing to Receive Email from a Rule" on page 3-39

Sending Email to Different Email Addresses for Different Periods of the Day

Task

Your worldwide IT department operates 24/7. Support responsibility rotates to different data centers across the globe depending on the time of day. When Enterprise Manager sends an email notification, you want it sent to the administrator currently on duty (normal work day), which in this situation changes depending on the time of day.

There are four adminstrators to handle Enterprise Manager notification:

- ADMIN_ASIA
- ADMIN_EU
- ADMIN_UK
- ADMIN_US

You want the notifications to be sent to specific administrators during their normal work hours.

User Roles

- System Administrator
- IT Operator

Prerequisites

- Email addresses have been defined for all administrators you want to send email nofifications.

  For more information, see "Defining E-mail Addresses" on page 4-5.
- You must have Super Administrator privileges.
- All administrators who are to receive email notifications have been defined.

How to do it:

1. From the **Setup** menu, select **Notifications**, then select **My Notification Schedule**.

   The Notification Schedule page displays.
2. Specify the administrator who's notification schedule you wish to edit and click **Change**. The selected administrator's notification schedule displays. You can click the search icon (magnifying glass) for a list of available administrators.
3. Click **Edit Schedule Definition**. The Edit Schedule Definition: Time Period page displays. The Edit Existing Schedule option is chosen by default. If necessary, modify the rotation schedule.
4. Click **Continue**. The Edit Schedule Definition: Email Addresses page displays.
5. Follow the instructions on the Edit Schedule Definition: Email Addresses page to adjust the administrator's notification schedule as required.
6. Click **Finish** once the notification schedule changes for the selected administrator are have been made. You are returned to the Notification Schedule page.
7. Repeat this process (steps two through six) for each administrator until all four administrators' notification schedules are in sync with their normal workdays.

What you have accomplished:

You have created a notification schedule where administrators in different time zones across the globe are only sent alert notifications during their assigned work hours.

What's next?

"Subscribing to Receive Email from a Rule" on page 3-39

4 Using Notifications

The notification system allows you to notify Enterprise Manager administrators when specific incidents, events, or problems arise.

> **Note:** This chapter assumes that you are familiar with incident management. For information about monitoring and managing your IT infrastructure via incident management, see Chapter 3, "Using Incident Management".

As an integral part of the management framework, notifications can also perform actions such as executing operating system commands (including scripts) and PL/SQL procedures when specific incidents, events, or problems occur. This capability allows you to automate IT practices. For example, if an incident (such as monitoring of the operational (up/down) status of a database) arises, you may want the notification system to automatically open an in-house trouble-ticket using an OS script so that the appropriate IT staff can respond in a timely manner.

By using Simple Network Management Protocol (SNMP) traps, the Enterprise Manager notification system also allows you to send traps to SNMP-enabled third-party applications such as HP OpenView for events published in Enterprise Manager. Some administrators may want to send third-party applications a notification when a certain metric has exceeded a threshold.

This chapter covers the following:

- Passing Information to a PL/SQL Procedure

4.1 Setting Up Notifications

All Enterprise Manager administrators can set up e-mail notifications for themselves. Super Administrators also have the ability to set up notifications for other Enterprise Manager administrators.

4.1.1 Setting Up a Mail Server for Notifications

Before Enterprise Manager can send e-mail notifications, you must first specify the Outgoing Mail (SMTP) servers to be used by the notification system. Once set, you can then define e-mail notifications for yourself or, if you have Super Administrator privileges, you can also define notifications for other Enterprise Manager administrators.

You specify the Outgoing Mail (SMTP) server on the Notification Methods page (Figure 4–1). To display the Notification Methods page, from the **Setup** menu, select **Notifications**, then select **Notification Methods**.

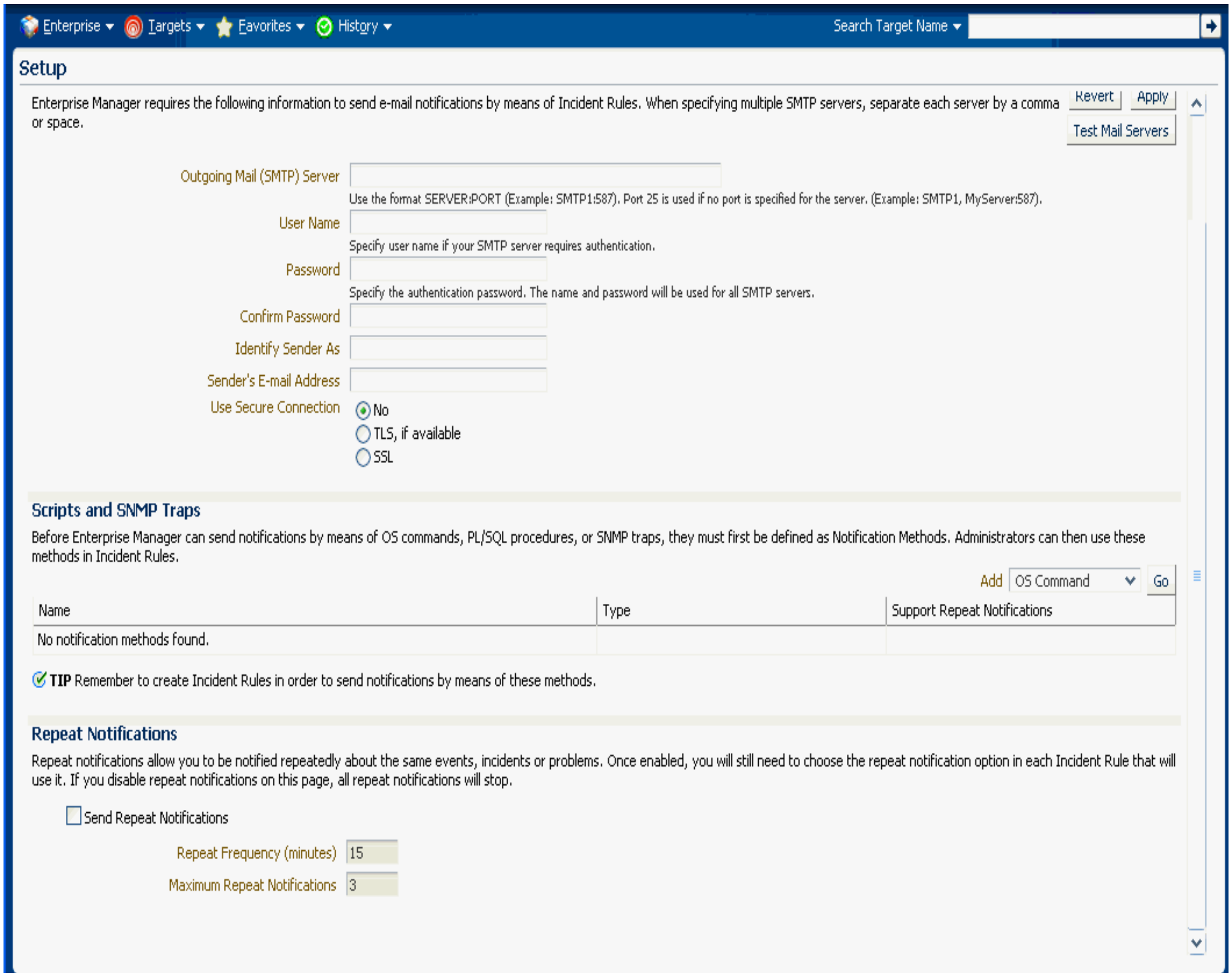
> **Note:** You must have Super Administrator privileges in order to configure the Enterprise Manager notifications system. This includes:
>
> - Setting up the SMTP server
> - Defining notification methods
> - Customizing notification email formats

Specify one or more outgoing mail server names, the mail server authentication credentials (User Name, Password, and Confirm Password), if required, the name you want to appear as the sender of the notification messages, and the e-mail address you want to use to send your e-mail notifications. This address, called the Sender's Mail Address, must be a valid address on each mail server that you specify. A message will be sent to this e-mail address if any problem is encountered during the sending of an e-mail notification. Example 4–1 shows sample notification method entries.

Example 4–1 Mail Server Settings

- **Outgoing Mail (SMTP) Server -** smtp01.example.com:587, smtp02.example.com
- **User Name -** myadmin
- **Password -** ******
- **Confirm Password -** ******
- **Identify Sender As -** Enterprise Manager
- **Sender's E-mail Address -** mgmt_rep@example.com
- **Use Secure Connection** - *No*: E-mail is not encrypted. *SSL*: E-mail is encrypted using the Secure Sockets Layer protocol. *TLS, if available*: E-mail is encrypted using the Transport Layer Security protocol if the mail server supports TLS. If the server does not support TLS, the e-mail is automatically sent as plain text.

Figure 4–1 Defining a Mail Server



Setup

Enterprise Manager requires the following information to send e-mail notifications by means of Incident Rules. When specifying multiple SMTP servers, separate each server by a comma or space.

Outgoing Mail (SMTP) Server

Use the format SERVER:PORT (Example: SMTP1:587). Port 25 is used if no port is specified for the server. (Example: SMTP1, MyServer:587).

User Name

Specify user name if your SMTP server requires authentication.

Password

Specify the authentication password. The name and password will be used for all SMTP servers.

Confirm Password

Identify Sender As

Sender's E-mail Address

Use Secure Connection ● No ○ TLS, if available ○ SSL

Scripts and SNMP Traps

Before Enterprise Manager can send notifications by means of OS commands, PL/SQL procedures, or SNMP traps, they must first be defined as Notification Methods. Administrators can then use these methods in Incident Rules.

Name	Type	Support Repeat Notifications
No notification methods found.		

✓ **TIP** Remember to create Incident Rules in order to send notifications by means of these methods.

Repeat Notifications

Repeat notifications allow you to be notified repeatedly about the same events, incidents or problems. Once enabled, you will still need to choose the repeat notification option in each Incident Rule that will use it. If you disable repeat notifications on this page, all repeat notifications will stop.

□ Send Repeat Notifications

Repeat Frequency (minutes) 15

Maximum Repeat Notifications 3

Note: The e-mail address you specify on this page is not the e-mail address to which the notification is sent. You will have to specify the e-mail address (where notifications will be sent) from the Password and E-mail page. From the **Setup** menu, choose **MyPreferences** and then **Enterprise Manager Password & E-mail**.

As standard practice, each user should have their own e-mail address.

After configuring the e-mail server, click **Test Mail Servers** to verify your e-mail setup. You should verify that an e-mail message was received by the e-mail account specified in the **Sender's E-mail Address** field.

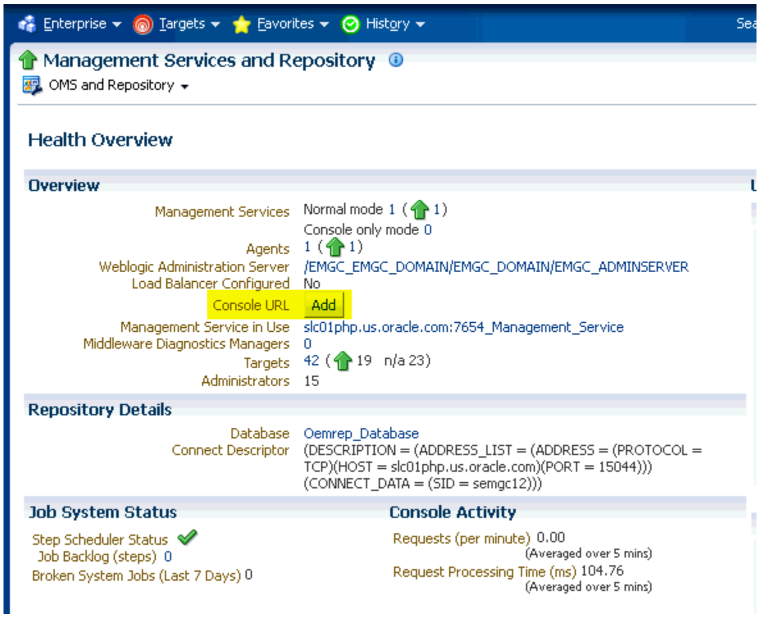
Defining multiple mail servers will improve the reliability of e-mail notification delivery. E-mail notifications will be delivered if at least one e-mail server is up. The notification load is balanced across multiple e-mail servers by the OMS, which switches through them (servers are allocated according to availability) after 20 e-mails have been sent. Switching is controlled by the *oracle.sysman.core.notification.emails_per_connection* emoms property.

Setting the Cloud Control Console URL when Using an SLB

If you have a multi-OMS environment with a Server Load Balancer (SLB) configured for the OMS instances, you should update the console URL to ensure that any emails from Enterprise Manager direct you to the Enterprise Manager console through the SLB URL and not the specific OMS URL from which the email may have originated.

To change the console URL:

1. From the **Setup** menu, select **Manage Cloud Control**, and then **Health Overview**. The Management Services and Repository page displays.
2. On the Management Services and Repository page, in the Overview section, click **Add/Edit** against the *Console URL* label.



Health Overview

Overview

Management Services	Normal mode 1 (1) Console only mode 0
Agents	1 (1)
Weblogic Administration Server	/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_ADMINSERVER
Load Balancer Configured	No
Console URL	Add
Management Service in Use	slc01php.us.oracle.com:7654_Management_Service
Middleware Diagnostics Managers	0
Targets	42 (19 n/a 23)
Administrators	15

Repository Details

Database	Oemrep_Database
Connect Descriptor	(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = slc01php.us.oracle.com)(PORT = 15044)))(CONNECT_DATA = (SID = semgc12)))

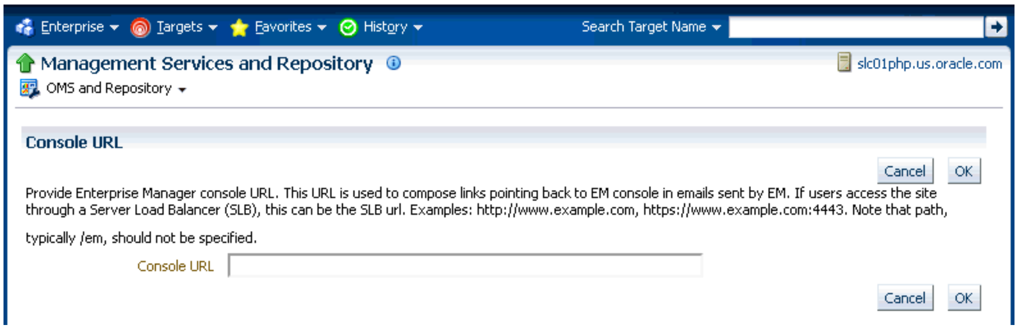
Job System Status

Step Scheduler Status ✓
Job Backlog (steps) 0
Broken System Jobs (Last 7 Days) 0

Console Activity

Requests (per minute) 0.00
(Averaged over 5 mins)
Request Processing Time (ms) 104.76
(Averaged over 5 mins)

The *Console URL* page displays.



Console URL

Provide Enterprise Manager console URL. This URL is used to compose links pointing back to EM console in emails sent by EM. If users access the site through a Server Load Balancer (SLB), this can be the SLB url. Examples: http://www.example.com, https://www.example.com:4443. Note that path, typically /em, should not be specified.

Console URL

3. Modify the Console URL to the SLB URL.

   Examples:

   http://www.example.com

   https://www.example.com:4443.

   Note that path, typically */em*, should not be specified.
4. Click **OK**.

4.1.2 Setting Up E-mail for Yourself

If you want to receive notifications by e-mail, you will need to specify your e-mail address(s) in the Password & E-mail page (from the Setup menu, select **MyPreferences**, then select **Enterprise Manager Password & E-mail**). In addition to defining notification e-mail addresses, you associate the notification message format (long, short, pager) to be used for your e-mail address.

Setting up e-mail involves three steps:

Step 1: Define an e-mail addresses.

Step 2: Set up a Notification Schedule.

Step 3: Subscribe to incident rules in order to receive e-mails.

4.1.2.1 Defining E-mail Addresses

An e-mail address can have up to 128 characters. There is no upper limit with the number of e-mail addresses.

To add an e-mail address:

1. From *username* drop-down menu, select **Enterprise Manager Password & E-mail**.
2. Click **Add Another Row** to create a new e-mail entry field in the **E-mail Addresses** table.
3. Specify the e-mail associated with your Enterprise Manager account. All e-mail notifications you receive from Enterprise Manager will be sent to the e-mail addresses you specify.

   For example, `user1@myco.com`

   Select the *E-mail Type* (message format) for your e-mail address. *E-mail (Long)* sends a HTML formatted e-mail that contains detailed information. Example 4–2 shows a typical notification that uses the long format.

   E-mail (Short) and *Pager(Short)* (Example 4–3) send a concise, text e-mail that is limited to a configurable number of characters, thereby allowing the e-mail be received as an SMS message or page. The content of the message can be sent entirely in the subject, entirely in the body or split across the subject and body.

   For example, in the last case, the subject could contain the severity type (for example, Critical) and the target name. The body could contain the time the severity occurred and the severity message. Since the message length is limited, some of this information may be truncated. If truncation has occurred there will be an ellipsis end of the message. *Pager(Short)* addresses are used for supporting the paging feature in incident rules. Note that the incident rules allow the rule author to designate some users to receive a page for critical issues.
4. Click **Apply** to save your e-mail address.

Example 4–2   Long E-mail Notification for Metric Alerts

```
Target type=Host
Target name=machine6140830.example.com
Message=Filesystem / has 54.39% available space, fallen below warning (60) or
critical (30) threshold.
Severity=Warning
Event reported time=Apr 28, 2011 2:33:55 PM PDT
Event Type=Metric Alert
Event name=Filesystems:Filesystem Space Available (%)
Metric Group=Filesystems
```

```
Metric=Filesystem Space Available (%)
Metric value=54.39
Key Value=/
Key Column 1=Mount Point
Rule Name=NotifRuleSet1,Event rule1
Rule Owner=SYSMAN
```

Example 4–3 Short E-mail Notification for Alerts

```
Subject is :
EM:Unreachable Start:myhost
Body is :
Nov 16, 2006 2:02:19 PM EST:Agent is Unreachable (REASON = Connection refused)
but the host is UP
```

More about E-mail(Short) and Pager(Short) Formats

Enterprise Manager does not directly support message services such as paging or SMS, but instead relies on external gateways to, for example, perform the conversion from e-mail to page. Beginning with Enterprise Manager 12c, the notification system allows you to tag e-mail addresses explicitly as 'page' or 'e-mail'. Explicit system differentiation between these two notification methods allows you to take advantage of the multiple action capability of incident rules. For example, the e-mail versus page distinction is required in order to send you an e-mail if an event severity is 'warning' or page you if the severity is 'critical'. To support this capability, a Pager format has been made available that sends an abbreviated version of the short format e-mail.

Note: To receive a Page, an administrator should be added to the Page Notification option in the Incident Rule.

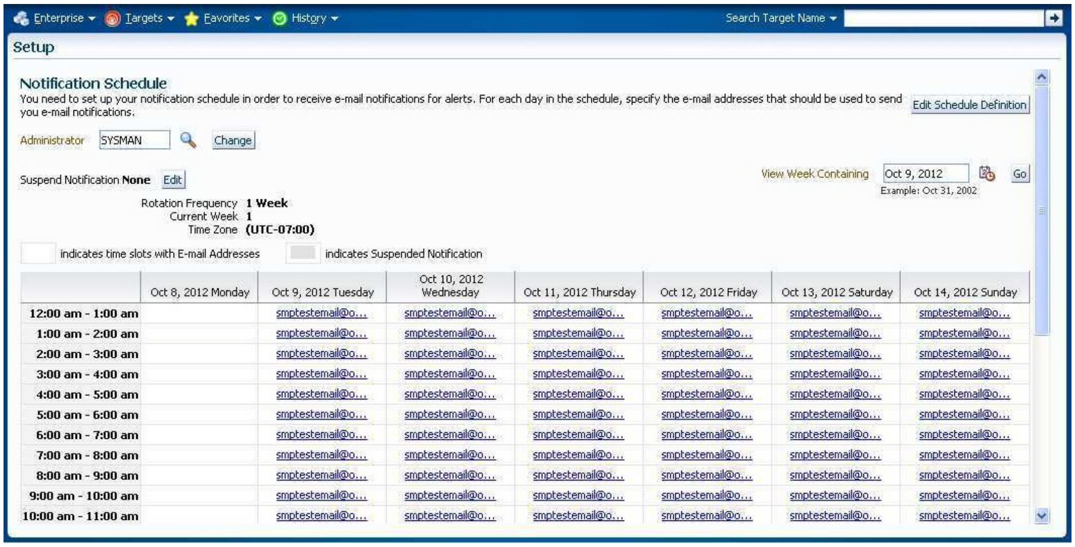
4.1.2.2 Setting Up a Notification Schedule

Once you have defined your e-mail notification addresses, you will need to define a notification schedule. For example, if your e-mail addresses are user1@myco.com, user2@myco.com, user3@myco.com, you can choose to use one or more of these e-mail addresses for each time period in your notification schedule. Only e-mail addresses that have been specified with your user preferences (**Enterprise Manager Password and Email** page) can be used in the notification schedule.

Note: When you enter e-mail addresses for the first time, a 24x7 weekly notification schedule is set automatically. You can then review and modify the schedule to suit your monitoring needs.

A notification schedule is a repeating schedule used to specify your on-call schedule—the days and time periods and e-mail addresses that should be used by Enterprise Manager to send notifications to you. Each administrator has exactly one notification schedule. When a notification needs to be sent to an administrator, Enterprise Manager consults that administrator's notification schedule to determine the e-mail address to be used. Depending on whether you are Super Administrator or a regular Enterprise Manager administrator, the process of defining a notification schedule differs slightly.

Figure 4–2 Notification Schedule Page



Notification Schedule

You need to set up your notification schedule in order to receive e-mail notifications for alerts. For each day in the schedule, specify the e-mail addresses that should be used to send you e-mail notifications.

Administrator SYSMAN

Suspend Notification **None**

View Week Containing Oct 9, 2012

Example: Oct 31, 2002

Rotation Frequency **1 Week**
Current Week **1**
Time Zone **(UTC-07:00)**

□ indicates time slots with E-mail Addresses ▨ indicates Suspended Notification

	Oct 8, 2012 Monday	Oct 9, 2012 Tuesday	Oct 10, 2012 Wednesday	Oct 11, 2012 Thursday	Oct 12, 2012 Friday	Oct 13, 2012 Saturday	Oct 14, 2012 Sunday
12:00 am - 1:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
1:00 am - 2:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
2:00 am - 3:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
3:00 am - 4:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
4:00 am - 5:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
5:00 am - 6:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
6:00 am - 7:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
7:00 am - 8:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
8:00 am - 9:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
9:00 am - 10:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...
10:00 am - 11:00 am		smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...	smptestemail@o...

If you are a regular Enterprise Manager administrator and are defining your own notification schedule:

1. From **Setup** menu, select **Notifications**, then select **My Notification Schedule**.
2. Follow the directions on the Notification Schedule page to specify when you want to receive e-mails.

4.1.2.3 Subscribe to Receive E-mail for Incident Rules

An incident rule is a user-defined rule that specifies the criteria by which notifications should be sent for specific events that make up the incident. An incident rule set, as the name implies, consists of one or more rules associated with the same incident.

When creating an incident rule, you specify criteria such as the targets you are interested in, the types of events to which you want the rule to apply. Specifically, for a given rule, you can specify the criteria you are interested in and the notification methods (such as e-mail) that should be used for sending these notifications. For example, you can set up a rule that when any database goes down or any database backup job fails, e-mail should be sent and the "log trouble ticket" notification method should be called. Or you can define another rule such that when the CPU or Memory Utilization of any host reach critical severities, SNMP traps should be sent to another management console.

Notification flexibility is further enhanced by the fact that with a single rule, you can perform multiple actions based on specific conditions. Example: When monitoring a condition such as machine memory utilization, for an incident severity of 'warning' (memory utilization at 80%), send the administrator an e-mail, if the severity is 'critical' (memory utilization at 99%), page the administrator immediately.

You can subscribe to a rule you have already created.

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. On the Incident Rules - All Enterprise Rules page, click on the rule set containing incident escalation rule in question and click **Edit...** Rules are created in the context of a rule set.

   Note: In the case where there is no existing rule set, create a rule set by clicking **Create Rule Set...** You then create the rule as part of creating the rule set.

3. In the Rules section of the Edit Rule Set page, highlight the escalation rule and click **Edit...**.
4. Navigate to the Add Actions page.
5. Select the action that escalates the incident and click **Edit...**
6. In the Notifications section, add the DBA to the **E-mail cc** list.
7. Click **Continue** and then navigate back to the **Edit Rule Set** page and click **Save**.

Out-of-Box Incident Rules

Enterprise Manager comes with two incident rule sets that cover the most common monitoring conditions, they are:

- Incident Management Ruleset for All Targets
- Event Management Ruleset for Self Update

If the conditions defined in the out-of-box incident rules meet your requirements, you can simply subscribe to receive e-mail notifications for the conditions defined in the rule using the subscribe procedure shown in the previous section.

The out-of-box incident rule set for all targets does not generate emails for *warning* alerts by default.

Creating Your Own Incident Rules

You can define your own custom rules. The following procedure documents the process of incident rule creation for non-Super Administrators.

To create your own incident rule:

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.

   The Incident Rules page displays. From this page you can create a new rule set, to which you can add new rules. Alternatively, if you have the requisite permissions, you can add new rules to existing

2. Click **Create Rule Set...**

   The create rule set page displays.

3. Specify the **Name**, **Description**, and the **Targets** to which the rules set should apply.
4. Click the **Rules** tab, then click **Create**.
5. Choose the incoming incident, event or problem to which you want the rule to apply. See "Setting Up Rule Sets" for more information.
6. Click **Continue**.

   Enterprise Manager displays the Create Incident Rule pages. Enter the requisite information on each page to create your incident rule.

7. Follow the wizard instructions to create your rule.

   Once you have completed defining your rule, the wizard returns you to the create rule set page.

8. Click **Save** to save the incident rule set.

4.1.3 Setting Up E-mail for Other Administrators

If you have Super Administrator privileges, you can set up e-mail notifications for other Enterprise Manager administrators. To set up e-mail notifications for other Enterprise Manager administrators, you need to:

Step 1: Ensure Each Administrator Account has an Associated E-mail Address

Each administrator to which you want to send e-mail notifications must have a valid e-mail address.

1. From the **Setup** menu, select **Security** and then **Administrators**.
2. For each administrator, define an e-mail address. This sets up a 24x7 notification schedule for this user that uses all the e-mail addresses specified. By default, this adds the *Email ID* with type set to *Email Long*. It is not possible to specify the *Email Type* option here.

Enterprise Manager also allows you to specify an administrator address when editing an administrator's notification schedule.

Step 2: Define Administrators' Notification Schedules

Once you have defined e-mail notification addresses for each administrator, you will need to define their respective notification schedules. Although a default 24x7 notification schedule is created when you specify an e-mail address for the first time, you should review and edit the notification schedule as needed.

1. From the **Setup** menu, select **Notifications**, then select **Notification Schedule**.

   From the vertical navigation bar, click Schedules (under Notification). The Notification Schedule page appears.
2. Specify the administrator who's notification schedule you wish to edit and click **Change**.
3. Click **Edit Schedule Definition**. The Edit Schedule Definition: Time Period page appears. If necessary, modify the rotation schedule.
4. Click **Continue**. The Edit Schedule Definition: E-mail Addresses page appears.
5. Follow the directions on the Edit Schedule Definition: E-mail Addresses page to modify the notification schedule.
6. Click **Finish** when you are done.
7. Repeat steps three through seven for each administrator.

Step 3: Assign Incident Rules to Administrators

With the notification schedules set, you now need to assign the appropriate incident rules for each designated administrator.

1. From the **Setup** menu, select **Incidents**, then select **Incident Rules**.
2. Select the desired **Ruleset** and click **Edit**.
3. Click on the **Rules** tab, select the desired rule and click **Edit**.
4. Click **Add Actions**, select desire action and click **Edit**.
5. Enter the **Administrator** name on either **E-mail To** or **E-mail Cc** field in the **Basic Notification** region.
6. Click **Continue**, click **Next**, click **Next**, click **Continue**, and finally click **Save**.

4.1.4 E-mail Customization

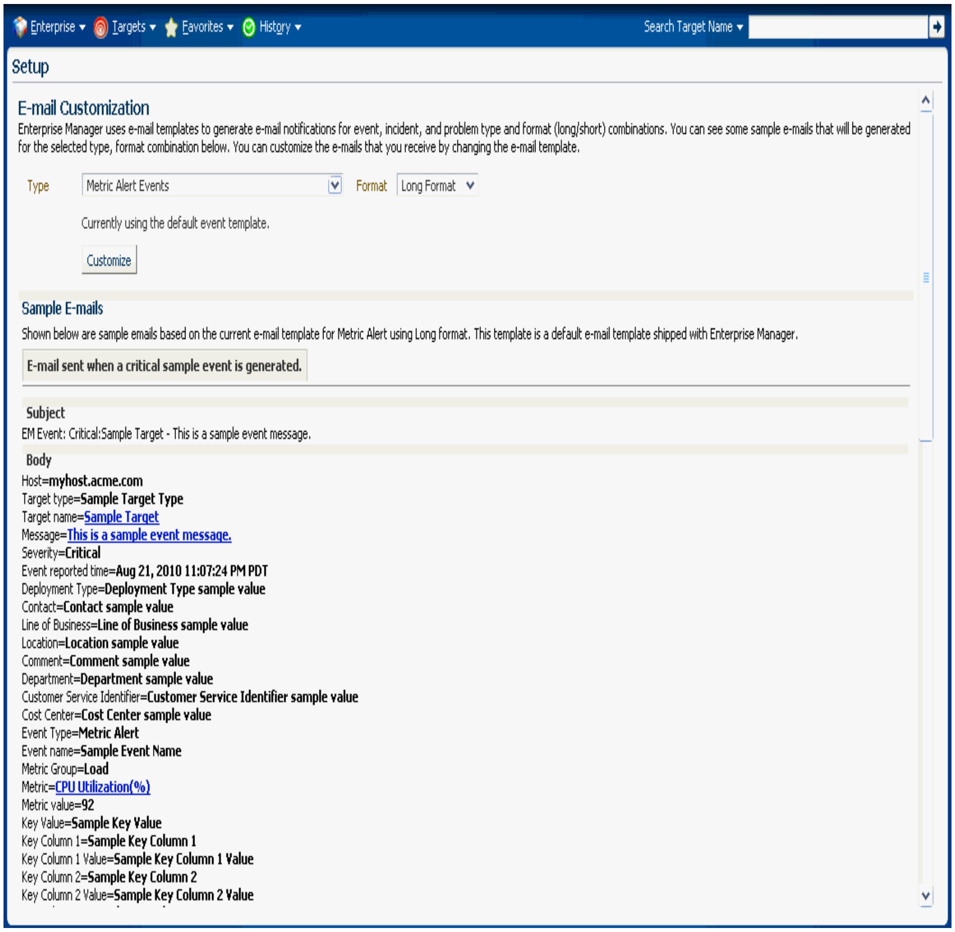
Enterprise Manager allows Super Administrators to customize global e-mail notifications for the following types: All events, incidents, problems, and specific event types installed. You can alter the default behavior for all events by customizing *Default Event Email Template*. In addition, you can further customize the behavior for a specific event type by customizing the template for the event type. For instance, you can customize the *Metric Alert Events* template for the metric alert event type. Using predefined building blocks (called attributes and labels) contained within a simple script, Super Administrators can customize alert e-mails by selecting from a wide variety of information content.

To customize an e-mail:

1. From the **Setup** menu, select **Notifications,** then select **Customize Email Formats**.
2. Choose the **Type** and **Format**.
3. Click **Customize**. The Customize Email Template page displays.

From the Customize E-mail Template page, you can modify the content of the e-mail template Enterprise Manager uses to generate e-mail notifications. Extensive information on script formatting, syntax, and options is available from the Edit E-mail Template page via imbedded assistance and online help.

Figure 4–3   E-mail Customization



Setup

E-mail Customization

Enterprise Manager uses e-mail templates to generate e-mail notifications for event, incident, and problem type and format (long/short) combinations. You can see some sample e-mails that will be generated for the selected type, format combination below. You can customize the e-mails that you receive by changing the e-mail template.

Type: Metric Alert Events   Format: Long Format

Currently using the default event template.

Sample E-mails

Shown below are sample emails based on the current e-mail template for Metric Alert using Long format. This template is a default e-mail template shipped with Enterprise Manager.

E-mail sent when a critical sample event is generated.

Subject

EM Event: Critical:Sample Target - This is a sample event message.

Body

Host=**myhost.acme.com**
Target type=**Sample Target Type**
Target name=**Sample Target**
Message=**This is a sample event message.**
Severity=**Critical**
Event reported time=**Aug 21, 2010 11:07:24 PM PDT**
Deployment Type=**Deployment Type sample value**
Contact=**Contact sample value**
Line of Business=**Line of Business sample value**
Location=**Location sample value**
Comment=**Comment sample value**
Department=**Department sample value**
Customer Service Identifier=**Customer Service Identifier sample value**
Cost Center=**Cost Center sample value**
Event Type=**Metric Alert**
Event name=**Sample Event Name**
Metric Group=**Load**
Metric=**CPU Utilization(%)**
Metric value=**92**
Key Value=**Sample Key Value**
Key Column 1=**Sample Key Column 1**
Key Column 1 Value=**Sample Key Column 1 Value**
Key Column 2=**Sample Key Column 2**
Key Column 2 Value=**Sample Key Column 2 Value**

4.1.4.1 E-mail Customization Reference

The following reference summarizes the semantics and component syntax of the pseudo-language used to define e-mails. The pseudo-language provides you with a simple, yet flexible way to customize e-mail notifications. The following is a summary of pseudo-language conventions/limitations:

- You can add comments (or any free-form text) using separate lines beginning with "--" or at end of lines.
- You can use attributes.
- You can use IF & ELSE & ENDIF control structures. You can also use multiple conditions using "AND" or "OR". Nested IF statements are not supported.
- You can insert spaces for formatting purposes. Spaces at the beginning of a line will be ignored in the actual e-mail. To insert spaces at the beginning of a line, use the [SP] attribute.
- Use "/" to escape and "[" or "]" if you want to add attribute names, operators, or IF clauses to the actual e-mail.
- HTML is not supported.

Reserved Words and Operators

The following table lists all reserved words and operators used when modifying e-mail scripts.

Table 4–1 Reserved Words and Operators

Reserved Word/Operator	Description
IF, ELSIF, ENDIF, ELSE	Used in IF-ELSE constructs.
AND, OR	Boolean operators – used in IF-ELSE constructs only.
NULL	To check NULL value for attributes - used in IF-ELSE constructs only.
|	Pipe operator – used to show the first non-NULL value in a list of attributes. For example: `METRIC_NAME|SEVERITY`
EQ, NEQ	Equal and Not-Equal operators – applicable to NULL, STRING and NUMERIC values.
/	Escape character – used to escape reserved words and operators. Escape characters signify that what follows the escape character takes an alternative interpretation.
[,]	Delimiters used to demarcate attribute names and IF clauses.

Syntax Elements

Literal Text

You can specify any text as part of the e-mail content. The text will be displayed in the e-mail and will not be translated if the Oracle Management Services (OMS) language setting is changed. For example, ‘my Oracle Home’ appears as ‘my Oracle Home’ in the generated e-mail.

Predefined Attributes

Predefined attributes/labels will be substituted with actual values in a specific context. To specify a predefined attribute/label, use the following syntax:

```
[PREDEFINED_ATTR]
```

Attribute names can be in either UPPER or LOWER case. The parsing process is case-insensitive.

A pair of square brackets is used to distinguish predefined attributes from literal text. For example, for a job e-mail notification, the actual job name will be substituted for `[EXECUTION_STATUS]`. For a metric alert notification, the actual metric column name will be substituted for `[METIRC_COLUMN]`.

You can use the escape character “/” to specify words and not have them interpreted as predefined labels/attributes. For example, "`/[NEW/]`” will not be considered as the predefined attribute `[NEW]` when parsed.

Operators

`EQ, NEQ` – for text and numeric values

`NULL`- for text and numeric values

`GT, LT, GE, LE` – for numeric values

Control Structures

The following table lists acceptable script control structures.

Table 4–2 Control Structures

Control Structure	Description
Pipe "|"	Two or more attributes can be separated by ‘|’ character. For example, `[METRIC_NAME|SEVERITY]` In this example, only the applicable attribute within the current alert context will be used (replaced by the actual value) in the e-mail. If more than one attribute is applicable, only the left-most attribute is used.

Table 4–2 (Cont.) Control Structures

<table>
<tr><th>Control Structure</th><th>Description</th></tr>
<tr><td>IF</td><td>

Allows you to make a block of text conditional. Only one level of IF and ELSIF is supported. Nested IF constructs are not supported.

All attributes can be used in IF or ELSIF evaluation using EQ/NEQ operators on NULL values. Other operators are allowed for “SEVERITY” and “REPEAT_COUNT” only.

Inside the IF block, the values need to be contained within quotation marks “ ”. Enterprise Manager will extract the attribute name and its value based on the position of “EQ” and other key words such as “and”, “or”. For example,

```
[IF REPEAT_COUNT EQ “1” AND SEVERITY EQ “CRITICAL”
THEN]
```

The statement above will be true when the attributes of the alert match the following condition:

- Attribute Name: REPEAT_COUNT
- Attribute Value: 1
- Attribute Name: SEVERITY
- Attribute Value: CRITICAL

Example IF Block:

```
[IF EXECUTION_STATUS NEQ NULL]
       [JOB_NAME_LABEL]=[EXECUTION_STATUS]
       [JOB_OWNER_LABEL]=[JOB_OWNER]
[ENDIF]

[IF SEVERITY_CODE EQ CRITICAL ]
       [MTRIC_NAME_LABEL]=[METRIC_GROUP]
       [METRIC_VALUE_LABEL]=[METRIC_VALUE]
       [TARGET_NAME_LABEL]=[TARGET_NAME]
       [KEY_VALUES]
[ENDIF]
```

Example IF and ELSEIF Block:

```
[IF SEVERITY_CODE EQ CRITICAL]
           statement1

[ELSIF SEVERITY_CODE EQ WARNING]
           statement2

[ELSIF SEVERITY_CODE EQ CLEAR]
           statement3

[ELSE]
           statement4

[ENDIF]
```

</td></tr>
</table>

Comments

You can add comments to your script by prefacing a single line of text with two hyphens "--". For example,

```
-- Code added on 8/3/2009
    [IF REPEAT_COUNT NEQ NULL]
    . . .
```

Comments may also be placed at the end of a line of text.

```
[IF SEVERITY_SHORT EQ W] -- for Warning alert
```

HTML Tags in Customization Content

Use of HTML tags is not supported.

When Enterprise Manager parses the e-mail script, it will convert the "<" and ">" characters of HTML tags into encoded format (&lt; and &gt;). This ensures that the HTML tag is not treated as HTML by the destination system.

Examples

E-mail customization template scripts support three main operators.

- Comparison operators: EQ/NEQ/GT/LT/GE/LE
- Logic operators: AND/OR
- Pipeline operator: |

4.1.5 Setting Up Repeat Notifications

Repeat notifications allow administrators to be notified repeatedly until an incident is either acknowledged or the number of **Maximum Repeat Notifications** has been reached. Enterprise Manager supports repeat notification for all notification methods (e-mail, OS command, PL/SQL procedure, and SNMP trap).

Configuring Repeat Notifications Globally

To enable repeat notifications for a notification method (globally), select the **Send Repeat Notifications** option on the Notification Methods page . In addition to setting the maximum number of repeat notifications, you can also set the time interval at which the notifications are sent.

> **Important:** For Oracle database versions 10 and higher, it is recommend that no modification be made to *aq_tm_processes* init.ora parameter. If, however, this parameter must be modified, its value should be at least one for repeat notification functionality. If the Enterprise Manager Repository database version is 9.2, the *aq_tm_processes* init.ora parameter must be set to at least one to enable repeat notification functionality.

Configuring Repeat Notifications Via Incident Rules

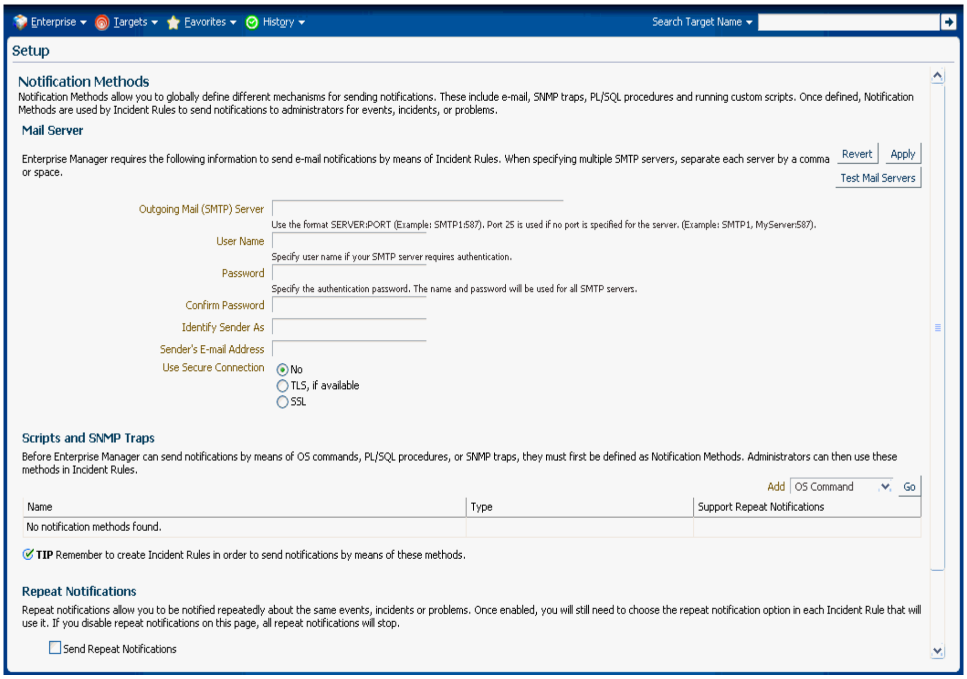
Setting repeat notifications globally at the notification method level may not provide sufficient flexibility. For example, you may want to have different repeat notification settings based on event type. Enterprise Manager accomplishes this by allowing you to set repeat notifications for individual incident rule sets or individual rules within a rule set. Repeat notifications set at the rule level take precedence over those defined at the notification method level.

> **Important:** Repeat notifications will only be sent if the **Send Repeat Notifications** option is enabled in the Notification Methods page.

Non-E-mail Repeat Notifications

For non-e-mail repeat notifications (PL/SQL, OS command, and SNMP trap notification methods), you must enable each method to support repeat notifications. You can select **Supports Repeat Notifications** option when adding a new notification method or by editing an existing method.

Figure 4–4 Enabling Repeat Notification for an OS Command Notification Method



Setup

Notification Methods

Notification Methods allow you to globally define different mechanisms for sending notifications. These include e-mail, SNMP traps, PL/SQL procedures and running custom scripts. Once defined, Notification Methods are used by Incident Rules to send notifications to administrators for events, incidents, or problems.

Mail Server

Enterprise Manager requires the following information to send e-mail notifications by means of Incident Rules. When specifying multiple SMTP servers, separate each server by a comma or space.

Outgoing Mail (SMTP) Server

Use the format SERVER:PORT (Example: SMTP1:587). Port 25 is used if no port is specified for the server. (Example: SMTP1, MyServer:587).

User Name

Specify user name if your SMTP server requires authentication.

Password

Specify the authentication password. The name and password will be used for all SMTP servers.

Confirm Password

Identify Sender As

Sender's E-mail Address

Use Secure Connection ● No ○ TLS, if available ○ SSL

Scripts and SNMP Traps

Before Enterprise Manager can send notifications by means of OS commands, PL/SQL procedures, or SNMP traps, they must first be defined as Notification Methods. Administrators can then use these methods in Incident Rules.

Add OS Command Go

Name	Type	Support Repeat Notifications
No notification methods found.		

✓ **TIP** Remember to create Incident Rules in order to send notifications by means of these methods.

Repeat Notifications

Repeat notifications allow you to be notified repeatedly about the same events, incidents or problems. Once enabled, you will still need to choose the repeat notification option in each Incident Rule that will use it. If you disable repeat notifications on this page, all repeat notifications will stop.

□ Send Repeat Notifications

4.2 Extending Notification Beyond E-mail

Notification Methods are the mechanisms by which notifications are sent. Enterprise Manager Super Administrators can set up e-mail notifications by configuring the 'e-mail' notification method. Most likely this would already have been set up as part of the Oracle Management Service installation.

Enterprise Manager Super Administrators can also define other custom notification methods. For example, event notifications may need to be forwarded to a 3rd party trouble-ticketing system. Assuming APIs to the third-party trouble-ticketing system are available, a custom notification method can be created to call a custom OS script that has the appropriate APIs. The custom notification method can be named in a user-friendly fashion, for example, "Log trouble ticket". Once the custom method is defined, whenever an administrator needs to send alerts to the trouble-ticketing system, he simply needs to invoke the now globally available notification method called "Log trouble ticket".

Custom notification methods can be defined based on any custom OS script, any custom PL/SQL procedure, or by sending SNMP traps. A fourth type of notification method (Java Callback) exists to support Oracle internal functionality and cannot be created or edited by Enterprise Manager administrators.

Only Super Administrators can define OS Command, PL/SQL, and SNMP Trap notification methods. However, any Enterprise Manager administrator can add these notification methods (once defined by the Super Administrator) as actions to their incident rules.

Through the Notification Methods page, you can:

- Set up the outgoing mail servers if you plan to send e-mail notifications through incident rules
- Create other custom notification methods using OS and PL/SQL scripts and SNMP traps.
- Set global repeat notifications.

4.3 Sending Notifications Using OS Commands and Scripts

Notification system can invoke a custom script when an incident rule matches the OS Command advanced notification action. A custom script receives notifications for matching events, incidents and problem through environment variables.

The length of any environment variable's value is limited to 512 characters by default. Configure emoms property named *oracle.sysman.core.notification.oscmd.max_env_var_length* for changing the default limit.

Important: Notification methods based on OS commands must be configured by an administrator with Super Administrator privileges.

Running OS Command Scripts: Running an OS command such as "sudo" for receiving notifications will fail because the command does not have read permission of the OMS account. The OMS account must have read permission over the OS command in order to send notifications.

To overcome the permissions problem, embed the command in a wrapper script that is readable by the OMS administrator account. Once the command is contained within the wrapper script, you then specify this script in place of the OS command.

Registering a Custom Script

In order to use a custom script, you must first register the script with the notification system. This is performed in four steps:

1. Define your OS command or script.
2. Deploy the script on each Management Service host.
3. Register your OS Command or Script as a new Notification Method.
4. Assign the notification method to an incident rule.

Step 1: Define your OS command or script.

You can specify an OS command or script that will be called by the notification system when an incident rule matches the OS Command advanced notification action. You can use incident, event, or problem context information, corrective action execution status and job execution status within the body of the script. Passing this contextual information to OS commands/scripts allows you to customize automated responses specific event conditions. For example, if an OS script opens a trouble ticket for an in-house support trouble ticket system, you will want to pass severity levels (critical, warning, and so on) to the script to open a trouble ticket with the appropriate details and escalate the problem. For more information on passing specific types of information to OS Command or Scripts, see:

- "Passing Event, Incident, Problem Information to an OS Command or Script" on page 4-60
- "Passing Corrective Action Execution Status to an OS Command or Script" on page 4-50
- "Passing Job Execution Status to an OS Command or Script" on page 4-54

Step 2: Deploy the script on each Management Service host.

You must deploy the OS Command or Script on each Management Service host machine that connects to the Management Repository. The OS Command is run as the user who started the Management Service. The OS Command or Script should be deployed on the same location on each Management Service host machine.

> **Important:** Both scripts and OS Commands should be specified using absolute paths. For example, /u1/bin/logSeverity.sh.

The command is run by the user who started the Management Service. If an error is encountered during the running of the OS Command, the Notification System can be instructed to retry the sending of the notification to the OS Command by returning an exit code of 100. The procedure is initially retried after one minute, then two minutes, then three minutes, eventually progressing to 30 minutes. From here, the procedure is retried every 30 minutes until the notification is a 24 hours old. The notification will be then be purged.

Example 4–4 shows the parameter in emoms.properties that controls how long the OS Command can execute without being killed by the Management Service. This prevents OS Commands from running for an inordinate length of time and blocks the delivery of other notifications. By default the command is allowed to run for 30 seconds before it is killed. The *oracle.sysman.core.notification.os_cmd_timeout* emoms property can be configured to change the default timeout value.

Example 4–4 Changing the oracle.sysman.core.notification.os_cmd_timeout emoms Property

```
emctl set property -name oracle.sysman.core.notification.os_cmd_timeout value 30
```

Step 3: Register your OS Command or Script as a new Notification Method.

Add this OS command as a notification method that can be called in incident rules. Log in as a Super Administrator. From the **Setup** menu, select **Notifications**, then select **Notification Methods**. From this page, you can define a new notification based on the 'OS Command' type. See "Sending Notifications Using OS Commands and Scripts".

The following information is required for each OS command notification method:

- Name
- Description

  Both Name and Description should be clear and intuitive so that the function of the method is clear to other administrators.

- OS Command

You must enter the full path of the OS command or script in the OS command field (for example, `/u1/bin/myscript.sh`). For environments with multiple Management Services, the path must be exactly the same on each machine that has a Management Service. Command line parameters can be included after the full path (for example, /u1/bin/myscript.sh arg1 arg2).

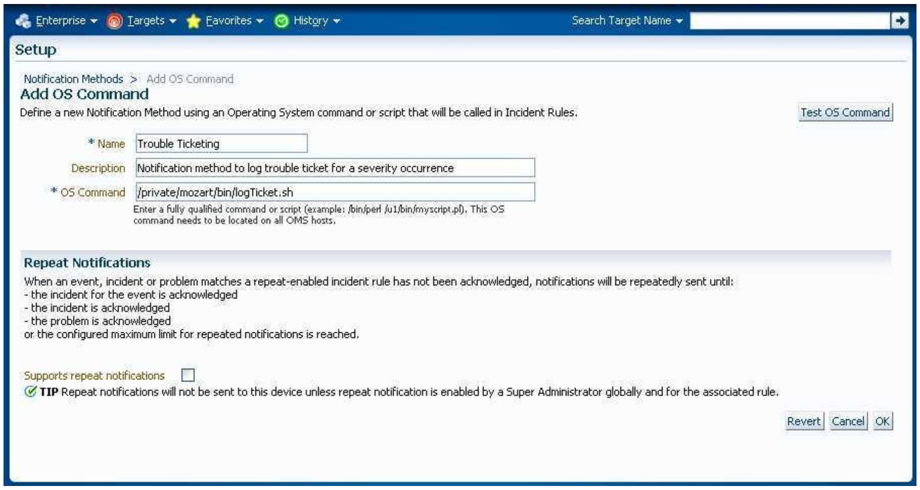
Example 4–5 shows information required for the notification method.

Example 4–5 OS Command Notification Method

```
Name Trouble Ticketing
Description Notification method to log trouble ticket for a severity occurrence
OS Command /private/mozart/bin/logTicket.sh
```

> **Note:** There can be more than one OS Command configured per system.

Figure 4–5 Notification Method: Add OS Command



Add OS Command

Define a new Notification Method using an Operating System command or script that will be called in Incident Rules.

* Name: Trouble Ticketing

Description: Notification method to log trouble ticket for a severity occurrence

* OS Command: /private/mozart/bin/logTicket.sh

Enter a fully qualified command or script (example: /bin/perl /u1/bin/myscript.pl). This OS command needs to be located on all OMS hosts.

Repeat Notifications

When an event, incident or problem matches a repeat-enabled incident rule has not been acknowledged, notifications will be repeatedly sent until:
- the incident for the event is acknowledged
- the incident is acknowledged
- the problem is acknowledged
or the configured maximum limit for repeated notifications is reached.

Supports repeat notifications □

✓ **TIP** Repeat notifications will not be sent to this device unless repeat notification is enabled by a Super Administrator globally and for the associated rule.

Step 4: Assign the notification method to an incident rule.

You can edit an existing rule (or create a new instance rule), then go to the Methods page. From the **Setup** menu, choose **Incidents** and then **Incident Rules**. The Incident Rules page provides access to all available rule sets.

For detailed reference information on passing event, incident, and problem information to an OS Command or script, see "Passing Event, Incident, Problem Information to an OS Command or Script" on page 4-60.

4.3.1 Script Examples

The sample OS script shown in Example 4–6 appends environment variable entries to a log file. In this example, the script logs a severity occurrence to a file server. If the file server is unreachable then an exit code of 100 is returned to force the Oracle Management Service Notification System to retry the notification

Example 4–6 Sample OS Command Script

```
#!/bin/ksh
```

```
LOG_FILE=/net/myhost/logs/event.log
if test -f $LOG_FILE
then
echo $TARGET_NAME $MESSAGE $EVENT_REPORTED_TIME >> $LOG_FILE
else
   exit 100
fi
```

Example 4–7 shows an OS script that logs alert information for both incidents and events to the file 'oscmdNotify.log'. The file is saved to the /net/myhost/logs directory.

Example 4–7 Alert Logging Scripts

```
#!/bin/sh
#
  LOG_FILE=/net/myhost/logs/oscmdNotify.log

  echo '-------------' >> $LOG_FILE

  echo 'issue_type=' $ISSUE_TYPE >> $LOG_FILE
  echo 'notif_type=' $NOTIF_TYPE >> $LOG_FILE
  echo 'message=' $MESSAGE >> $LOG_FILE
  echo 'message_url'  = $MESSAGE_URL >>$LOG_FILE
  echo 'severity=' $SEVERITY >> $LOG_FILE
  echo 'severity_code'  = $SEVERITY_CODE >>$LOG_FILE
  echo 'ruleset_name=' $RULESET_NAME >> $LOG_FILE
  echo 'rule_name=' $RULE_NAME >> $LOG_FILE
  echo 'rule_owner=' $RULE_OWNER >> $LOG_FILE
  echo 'repeat_count=' $REPEAT_COUNT >> $LOG_FILE
  echo 'categories_count'  = $CATEGORIES_COUNT >>$LOG_FILE
  echo 'category_1'  = $CATEGORY_1 >>$LOG_FILE
  echo 'category_2'  = $CATEGORY_2 >>$LOG_FILE
  echo 'category_code_1'  = $CATEGORY_CODE_1 >>$LOG_FILE
  echo 'category_code_2'  = $CATEGORY_CODE_2 >>$LOG_FILE
  echo 'category_codes_count'  = $CATEGORY_CODES_COUNT >>$LOG_FILE

# event
if [ $ISSUE_TYPE -eq 1 ]
then
  echo 'host_name=' $HOST_NAME >> $LOG_FILE
  echo 'event_type=' $EVENT_TYPE >> $LOG_FILE
  echo 'event_name=' $EVENT_NAME >> $LOG_FILE
  echo 'event_occurrence_time=' $EVENT_OCCURRENCE_TIME >> $LOG_FILE
  echo 'event_reported_time=' $EVENT_REPORTED_TIME >> $LOG_FILE
  echo 'sequence_id=' $SEQUENCE_ID >> $LOG_FILE
  echo 'event_type_attrs=' $EVENT_TYPE_ATTRS >> $LOG_FILE
  echo 'source_obj_name=' $SOURCE_OBJ_NAME >> $LOG_FILE
  echo 'source_obj_type=' $SOURCE_OBJ_TYPE >> $LOG_FILE
  echo 'source_obj_owner=' $SOURCE_OBJ_OWNER >> $LOG_FILE
  echo 'target_name'  = $TARGET_NAME >>$LOG_FILE
  echo 'target_url'  = $TARGET_URL >>$LOG_FILE
  echo 'target_owner=' $TARGET_OWNER >> $LOG_FILE
  echo 'target_type=' $TARGET_TYPE >> $LOG_FILE
  echo 'target_version=' $TARGET_VERSION >> $LOG_FILE
  echo 'lifecycle_status=' $TARGET_LIFECYCLE_STATUS >> $LOG_FILE
  echo 'assoc_incident_escalation_level'  = $ASSOC_INCIDENT_ESCALATION_LEVEL
>>$LOG_FILE
  echo 'assoc_incident_id'  = $ASSOC_INCIDENT_ID >>$LOG_FILE
  echo 'assoc_incident_owner'  = $ASSOC_INCIDENT_OWNER >>$LOG_FILE
  echo 'assoc_incident_acknowledged_by_owner'  = $ASSOC_INCIDENT_ACKNOWLEDGED_BY_
OWNER >>$LOG_FILE
  echo 'assoc_incident_acknowledged_details'  = $ASSOC_INCIDENT_ACKNOWLEDGED_
DETAILS >>$LOG_FILE
  echo 'assoc_incident_priority'  = $ASSOC_INCIDENT_PRIORITY >>$LOG_FILE
  echo 'assoc_incident_status'  = $ASSOC_INCIDENT_STATUS >>$LOG_FILE
  echo 'ca_job_status'  = $CA_JOB_STATUS >>$LOG_FILE
  echo 'event_context_attrs'  = $EVENT_CONTEXT_ATTRS >>$LOG_FILE
  echo 'last_updated_time'  = $LAST_UPDATED_TIME >>$LOG_FILE
  echo 'sequence_id'  = $SEQUENCE_ID >>$LOG_FILE
  echo 'test_date_attr_noref'  = $TEST_DATE_ATTR_NOREF >>$LOG_FILE
  echo 'test_raw_attr_noref'  = $TEST_RAW_ATTR_NOREF >>$LOG_FILE
  echo 'test_str_attr1'  = $TEST_STR_ATTR1 >>$LOG_FILE
  echo 'test_str_attr2'  = $TEST_STR_ATTR2 >>$LOG_FILE
  echo 'test_str_attr3'  = $TEST_STR_ATTR3 >>$LOG_FILE
  echo 'test_str_attr4'  = $TEST_STR_ATTR4 >>$LOG_FILE
  echo 'test_str_attr5'  = $TEST_STR_ATTR5 >>$LOG_FILE
  echo 'test_str_attr_ref'  = $TEST_STR_ATTR_REF >>$LOG_FILE
  echo 'total_occurrence_count'  = $TOTAL_OCCURRENCE_COUNT >>$LOG_FILE
fi

# incident
if [ $ISSUE_TYPE -eq 2 ]
then
  echo 'action_msg=' $ACTION_MSG >> $LOG_FILE
  echo 'incident_id=' $INCIDENT_ID >> $LOG_FILE
  echo 'incident_creation_time=' $INCIDENT_CREATION_TIME >> $LOG_FILE
  echo 'incident_owner=' $INCIDENT_OWNER >> $LOG_FILE
echo 'incident_acknowledged_by_owner'  = $INCIDENT_ACKNOWLEDGED_BY_OWNER >>$LOG_
FILE
  echo 'incident_status'  = $INCIDENT_STATUS >>$LOG_FILE
  echo 'last_modified_by=' $LAST_MODIFIED_BY >> $LOG_FILE
  echo 'last_updated_time=' $LAST_UPDATED_TIME >> $LOG_FILE
  echo 'assoc_event_count=' $ASSOC_EVENT_COUNT >> $LOG_FILE
  echo 'adr_incident_id=' $ADR_INCIDENT_ID >> $LOG_FILE
  echo 'occurrence_count=' $OCCURRENCE_COUNT >> $LOG_FILE
  echo 'escalated=' $ESCALATED >> $LOG_FILE
  echo 'escalated_level=' $ESCALATED_LEVEL >> $LOG_FILE
  echo 'priority=' $PRIORITY >> $LOG_FILE
  echo 'priority_code'  = $PRIORITY_CODE >>$LOG_FILE
  echo 'ticket_id=' $TICKET_ID >> $LOG_FILE
  echo 'ticket_status=' $TICKET_STATUS >> $LOG_FILE
  echo 'ticket_url=' $TICKET_ID_URL >> $LOG_FILE
  echo 'total_duplicate_count=' $TOTAL_DUPLICATE_COUNT >> $LOG_FILE
  echo 'source_count=' $EVENT_SOURCE_COUNT >> $LOG_FILE
  echo 'event_source_1_host_name'  = $EVENT_SOURCE_1_HOST_NAME >>$LOG_FILE
  echo 'event_source_1_target_guid'  = $EVENT_SOURCE_1_TARGET_GUID >>$LOG_FILE
  echo 'event_source_1_target_name'  = $EVENT_SOURCE_1_TARGET_NAME >>$LOG_FILE
  echo 'event_source_1_target_owner'  = $EVENT_SOURCE_1_TARGET_OWNER >>$LOG_FILE
  echo 'event_source_1_target_type'  = $EVENT_SOURCE_1_TARGET_TYPE >>$LOG_FILE
  echo 'event_source_1_target_url'  = $EVENT_SOURCE_1_TARGET_URL >>$LOG_FILE
  echo 'event_source_1_target_lifecycle_status'  = $EVENT_SOURCE_1_TARGET_
LIFECYCLE_STATUS >>$LOG_FILE
  echo 'event_source_1_target_version'  = $EVENT_SOURCE_1_TARGET_VERSION >>$LOG_
FILE
fi
exit 0
```

Example 4–8 shows a script that sends an alert to an HP OpenView console from Enterprise Manager Cloud Control. When a metric alert is triggered, the Enterprise

Manager Cloud Control displays the alert. The HP OpenView script is then called, invoking opcmsg and forwarding the information to the HP OpenView management server.

Example 4–8 HP OpenView Script

```
/opt/OV/bin/OpC/opcmsg severity="$SEVERITY" app=OEM msg_grp=Oracle msg_
text="$MESSAGE" object="$TARGET_NAME"
```

4.3.2 Migrating pre-12c OS Command Scripts

This section describes how to map pre-12c OS Command notification shell environment variables to 12c OS Command shell environment variables.

Note: Policy Violations are no longer supported beginning with the Enterprise Manager 12*c* release.

4.3.2.1 Migrating Metric Alert Event Types

Following table is the mapping for the OS Command shell environment variables when the event_type is metric_alert.

Table 4–3 Pre-12c/12c metric_alert Environment Variable Mapping

Pre-12c Environment Variable	Corresponding 12c Environment Variables
ACKNOWLEDGED	ASSOC_INCIDENT_ACKNOWLEDGED_BY_OWNER
ACKNOWLEDGED_BY	ASSOC_INCIDENT_OWNER
CYCLE_GUID	CYCLE_GUID
HOST	HOST_NAME
KEY_VALUE	Note: See detail description below.
KEY_VALUE_NAME	Note: See detail description below
MESSAGE	MESSAGE
METRIC	METRIC_COLUMN
NOTIF_TYPE	NOTIF_TYPE; use the map in section 2.3.5
REPEAT_COUNT	REPEAT_COUNT
RULE_NAME	RULESET_NAME
RULE_OWNER	RULE_OWNER
SEVERITY	SEVERITY
TARGET_NAME	TARGET_NAME
TARGET_TYPE	TARGET_TYPE
TIMESTAMP	EVENT_REPORTED_TIME
METRIC_VALUE	VALUE
VIOLATION_CONTEXT	EVENT_CONTEXT_ATTRS
VIOLATION_GUID	SEVERITY_GUID
POLICY_RULE	No mapping, Obsolete as of Enterprise Manager 12c release.

To obtain KEY_VALUE_NAME and KEY_VALUE, perform the following steps.

- If $NUM_KEYS variable is null, then $KEY_VALUE_NAME and $KEY_VALUE are null.
- If $NUM_KEYS equals 1

  KEY_VALUE_NAME=$KEY_COLUMN_1

  KEY_COLUMN_1_VALUE
- If $NUM_KEYS is greater than 1

  KEY_VALUE_NAME="$KEY_COLUMN_1;$KEY_COLUMN_2;..;KEY_COLUMN_x"

  KEY_VALUE="$KEY_COLUMN_1_VALUE;$KEY_COLUMN_2_VALUE;..;KEY_COLUMN_x_VALUE "

  Where x is the value of $NUM_KEYS and ";" is the separator.

4.3.2.2 Migrating Target Availability Event Types

Following table is the mapping for the OS Command shell environment variables when the event_type is 'target_availability'.

Table 4–4 pre-12c/12c target_availability Environment Variable Mappings

Pre-12c Environment Variable	Corresponding 12c Environment Variables
TARGET_NAME	TARGET_NAME
TARGET_TYPE	TARGET_TYPE
METRIC	Status
CYCLE_GUID	CYCLE_GUID
VIOLATION_CONTEXT	EVENT_CONTEXT_ATTRS
SEVERITY	TARGET_STATUS
HOST	HOST_NAME
MESSAGE	MESSAGE
NOTIF_TYPE	NOTIF_TYPE; use the map in section 2.3.5
TIMESTAMP	EVENT_REPORTED_TIME
RULE_NAME	RULESET_NAME
RULE_OWNER	RULE_OWNER
REPEAT_COUNT	REPEAT_COUNT
KEY_VALUE	""
KEY_VALUE_NAME	""

4.3.2.3 Migrating Job Status Change Event Types

Following table is the mapping for the OS Command shell environment variables when the event_type is 'job_status_change'.

Table 4–5 pre-12c/12c job_status_change Environment Variable Mappings

Pre-12c Environment Variable	Corresponding 12c Environment Variables
JOB_NAME	SOURCE_OBJ_NAME
JOB_OWNER	SOURCE_OBJ_OWNER
JOB_TYPE	SOURCE_OBJ_SUB_TYPE
JOB_STATUS	EXECUTION_STATUS
NUM_TARGETS	1 if $ TARGET_NAME is not null, 0 otherwise
TARGET_NAME1	TARGET_NAME
TARGET_TYPE1	TARGET_TYPE
TIMESTAMP	EVENT_REPORTED_TIME
RULE_NAME	RULESET_NAME
RULE_OWNER	RULE_OWNER

4.3.2.4 Migrating Corrective Action-Related OS Scripts

Refer to section "Migrating Metric Alert Event Types" for mapping the following environment variables while receiving notifications for corrective actions.

KEY_VALUE

KEY_VALUE_NAME

METRIC

METRIC_VALUE

RULE_NAME

RULE_OWNER

SEVERITY

TIMESTAMP

VIOLATION_CONTEXT

Use the map below for mapping other environment variables.

Table 4–6 pre-12c/12c Corrective Action Environment Variable Mappings

Pre-12c Environment Variable	Corresponding 12c Environment Variables
NUM_TARGETS	1
TARGET_NAME1	TARGET_NAME
TARGET_TYPE1	TARGET_TYPE
JOB_NAME	CA_JOB_NAME
JOB_OWNER	CA_JOB_OWNER
JOB_STATUS	CA_JOB_STATUS
JOB_TYPE	CA_JOB_TYPE

4.3.2.5 Notification Type Mapping

Table 4–7 pre-12c/12c notif_type Mappings

notif_type (12c)	notif_type (Pre-12c)
NOTIF_NORMAL	1
NOTIF_REPEAT	4
NOTIF_DURATION	9
NOTIF_RETRY	2

4.4 Sending Notifications Using PL/SQL Procedures

A user-defined PL/SQL procedure can receive notifications for matching events, incidents and problems.

> **Note:** When upgrading from pre-12c to 12c versions of Enterprise Manager, existing pre-12c PL/SQL advanced notification methods will continue to work without modification. You should, however, update the procedures to use new signatures.
>
> New PL/SQL advanced notification methods created with Enterprise Manager 12c must use the new signatures documented in the following sections.

Complete the following four steps to define a notification method based on a PL/SQL procedure.

4.4.1 Defining a PL/SQL-based Notification Method

Creating a PL/SQL-based notification method consists of four steps:

1. Define the PL/SQL procedure.
2. Create the PL/SQL procedure on the Management Repository.
3. Register your PL/SQL procedure as a new notification method.
4. Assign the notification method to an incident rule.

Step 1: Define the PL/SQL Procedure

The procedure must have one of the following signatures depending on the type of notification that will be received.

For Events:

PROCEDURE event_proc(event_msg IN gc$notif_event_msg)

For Incidents:

PROCEDURE incident_proc(incident_msg IN gc$notif_incident_msg)

For Problems:

PROCEDURE problem_proc(problem_msg IN gc$notif_problem_msg)

Note: The notification method based on a PL/SQL procedure must be configured by an administrator with Super Administrator privileges before a user can select it while creating/editing a incident rule.

For more information on passing specific types of information to scripts or PL/SQL procedures, see the following sections:

"Passing Information to a PL/SQL Procedure" on page 4-69

"Passing Corrective Action Status Change Information" on page 4-50

"Passing Job Execution Status Information" on page 4-52

Step 2: Create the PL/SQL procedure on the Management Repository.

Create the PL/SQL procedure on the repository database using one of the following procedure specifications:

PROCEDURE event_proc(event_msg IN gc$notif_event_msg)

PROCEDURE incident_proc(incident_msg IN gc$notif_incident_msg)

PROCEDURE problem_proc(problem_msg IN gc$notif_problem_msg)

The PL/SQL procedure must be created on the repository database using the database account of the repository owner (such as SYSMAN)

If an error is encountered during the running of the procedure, the Notification System can be instructed to retry the sending of the notification to the procedure by raising a user-defined exception that uses the error code -20000. The procedure initially retried after one minute, then two minutes, then three minutes and so on, until the notification is a day old, at which point it will be purged.

Step 3: Register your PL/SQL procedure as a new notification method.

Log in as a Super Administrator. From the **Setup** menu, choose **Notifications** and then **Notification Methods** to access the Notification Methods page. From this page, you can define a new notification based on 'PL/SQL Procedure'. See Section 4.4, "Sending Notifications Using PL/SQL Procedures".

Make sure to use a fully qualified name that includes the schema owner, package name and procedure name. The procedure will be executed by the repository owner and so the repository owner must have execute permission on the procedure.

Create a notification method based on your PL/SQL procedure. The following information is required when defining the method:

- Name
- Description
- PL/SQL Procedure

You must enter a fully qualified procedure name (for example, OWNER.PKGNAME.PROCNAME) and ensure that the owner of the Management Repository has execute privilege on the procedure.

An example of the required information is shown in Example 4–9.

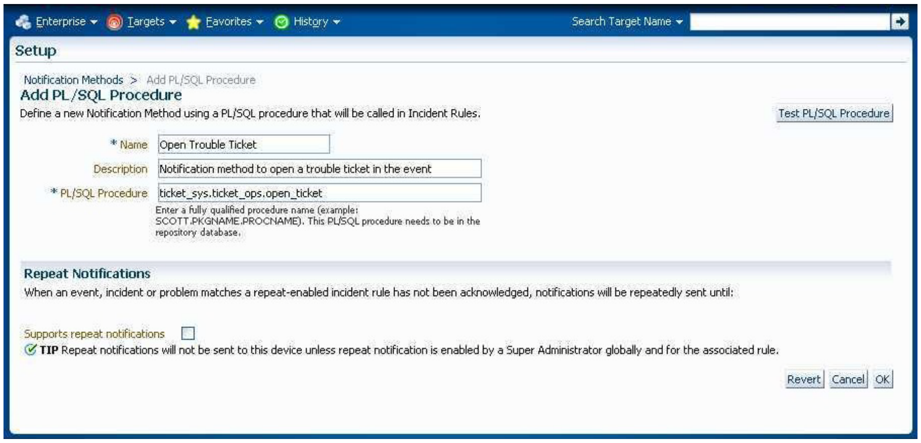
Example 4–9 PL/SQL Procedure Required Information

```
Name Open trouble ticket
```

```
Description Notification method to open a trouble ticket in the event
PLSQL Procedure ticket_sys.ticket_ops.open_ticket
```

Figure 4–6 illustrates how to add a PL/SQL-based notification method from the Enterprise Manager UI.

Figure 4–6 Adding a PL/SQL Procedure



Add PL/SQL Procedure

Define a new Notification Method using a PL/SQL procedure that will be called in Incident Rules.

* Name: Open Trouble Ticket

Description: Notification method to open a trouble ticket in the event

* PL/SQL Procedure: ticket_sys.ticket_ops.open_ticket

Enter a fully qualified procedure name (example: SCOTT.PKGNAME.PROCNAME). This PL/SQL procedure needs to be in the repository database.

Repeat Notifications

When an event, incident or problem matches a repeat-enabled incident rule has not been acknowledged, notifications will be repeatedly sent until:

Supports repeat notifications □

TIP Repeat notifications will not be sent to this device unless repeat notification is enabled by a Super Administrator globally and for the associated rule.

Step 4: Assign the notification method to an incident rule.

You can edit an existing rule (or create a new incident rule). From the **Setup** menu, select **Incidents** and then select **Incident Rules**. The Incident Rules page displays. From here, you can add an action to a rule specifying the new PL/SQL procedure found under **Advanced Notification Method.**

There can be more than one PL/SQL-based method configured for your Enterprise Manager environment.

See "Passing Information to a PL/SQL Procedure" on page 4-69 for more information about how incident, event, and problem information is passed to the PLSQL procedure.

Example 4–10 PL/SQL Script

```
-- Assume log_table is created by following DDL
-- CREATE TABLE log_table (message VARCHAR2(4000)) ;
-- Define PL/SQL notification method for Events
CREATE OR REPLACE PROCEDURE log_table_notif_proc(s IN GC$NOTIF_EVENT_MSG)
IS
  l_categories gc$category_string_array;
  l_category_codes gc$category_string_array;
  l_attrs gc$notif_event_attr_array;
  l_ca_obj gc$notif_corrective_action_job;
BEGIN
  INSERT INTO log_table VALUES ('notification_type: ' || s.msg_info.notification_
type);
  INSERT INTO log_table VALUES ('repeat_count: ' || s.msg_info.repeat_count);
  INSERT INTO log_table VALUES ('ruleset_name: ' || s.msg_info.ruleset_name);
  INSERT INTO log_table VALUES ('rule_name: ' || s.msg_info.rule_name);
  INSERT INTO log_table VALUES ('rule_owner: ' || s.msg_info.rule_owner);
  INSERT INTO log_table VALUES ('message: ' || s.msg_info.message);
  INSERT INTO log_table VALUES ('message_url: ' || s.msg_info.message_url);
  INSERT INTO log_table VALUES ('event_instance_guid: ' || s.event_payload.event_
instance_guid);
```

```
  INSERT INTO log_table VALUES ('event_type: ' || s.event_payload.event_type);
  INSERT INTO log_table VALUES ('event_name: ' || s.event_payload.event_name);
  INSERT INTO log_table VALUES ('event_msg: ' || s.event_payload.event_msg);
  INSERT INTO log_table VALUES ('source_obj_type: ' || s.event_
payload.source.source_type);
  INSERT INTO log_table VALUES ('source_obj_name: ' || s.event_
payload.source.source_name);
  INSERT INTO log_table VALUES ('source_obj_url: ' || s.event_
payload.source.source_url);
  INSERT INTO log_table VALUES ('target_name: ' || s.event_payload.target.target_
name);
  INSERT INTO log_table VALUES ('target_url: ' || s.event_payload.target.target_
url);
  INSERT INTO log_table VALUES ('severity: ' || s.event_payload.severity);
  INSERT INTO log_table VALUES ('severity_code: ' || s.event_payload.severity_
code);
  INSERT INTO log_table VALUES ('event_reported_date: ' || to_char(s.event_
payload.reported_date, 'D MON DD HH24:MI:SS'));

  l_categories := s.event_payload.categories;
  IF l_categories IS NOT NULL
  THEN
    FOR c IN 1..l_categories.COUNT
    LOOP
      INSERT INTO log_table VALUES ('category ' || c || ' - ' || l_categories(c));
    END LOOP;
  END IF;

  l_category_codes := s.event_payload.category_codes;
  IF l_categories IS NOT NULL
  THEN
    FOR c IN 1..l_category_codes.COUNT
    LOOP
      INSERT INTO log_table VALUES ('category_code ' || c || ' - ' || l_category_
codes(c));
    END LOOP;
  END IF;

  l_attrs := s.event_payload.event_attrs;
  IF l_attrs IS NOT NULL
  THEN
    FOR c IN 1..l_attrs.COUNT
    LOOP
        INSERT INTO log_table VALUES ('EV.ATTR name=' || l_attrs(c).name || '
value=' || l_attrs(c).value || ' nls_value=' || l_attrs(c).nls_value);
    END LOOP;
  END IF;

COMMIT ;
END ;
/
```

Example 4–11   PL/SQL Script to Log Events to a Table

```
CREATE TABLE event_log (
  notification_type      VARCHAR2(32),
  repeat_count           NUMBER,
  ruleset_name           VARCHAR2(256),
  rule_owner             VARCHAR2(256),
  rule_name              VARCHAR2(256),
  message                VARCHAR2(4000),
  message_url            VARCHAR2(4000),
  event_instance_guid    RAW(16),
  event_type             VARCHAR2(20),
  event_name             VARCHAR2(512),
  event_msg              VARCHAR2(4000),
  categories             VARCHAR2(4000),
  source_obj_type        VARCHAR2(120),
  source_obj_name        VARCHAR2(256),
  source_obj_url         VARCHAR2(4000),
  severity               VARCHAR2(128),
  severity_code          VARCHAR2(32),
  target_name            VARCHAR2(256),
  target_type            VARCHAR2(128),
  target_url             VARCHAR2(4000),
  host_name              VARCHAR2(256),
  timezone               VARCHAR2(64),
  occured                DATE,
  ca_guid                RAW(16),
  ca_name                VARCHAR2(128),
  ca_owner               VARCHAR2(256),
  ca_type                VARCHAR2(256),
  ca_status              VARCHAR2(64),
  ca_status_code         NUMBER,
  ca_job_step_output     VARCHAR2(4000),
  ca_execution_guid      RAW(16),
  ca_stage_change_guid   RAW(16)
)
;

CREATE OR REPLACE PROCEDURE log_event(s IN GC$NOTIF_EVENT_MSG)
IS
   l_categories gc$category_string_array;
   l_ca_obj gc$notif_corrective_action_job;
   l_categories_new VARCHAR2(1000);
BEGIN
    -- save event categories
   l_categories := s.event_payload.categories;
        IF l_categories IS NOT NULL
   THEN
     FOR c IN 1..l_categories.COUNT
     LOOP
       l_categories_new := (l_categories_new|| c || ' - ' || l_
categories(c)||',');
     END LOOP;
   END IF;

   -- save event message
   IF s.msg_info.notification_type = 'NOTIF_CA' AND s.event_payload.corrective_
action IS NOT NULL
   THEN
     l_ca_obj := s.event_payload.corrective_action;
      INSERT INTO event_log (notification_type, repeat_count, ruleset_name, rule_
name, rule_owner, message, message_url, event_instance_guid, event_type, event_
name, event_msg, categories, source_obj_type, source_obj_name, source_obj_url,
severity, severity_code, target_name, target_type, target_url, host_name,
timezone, occured, ca_guid, ca_name, ca_owner, ca_type, ca_status, ca_status_code,
ca_job_step_output, ca_execution_guid, ca_stage_change_guid)
      VALUES (s.msg_info.notification_type, s.msg_info.repeat_count, s.msg_
info.ruleset_name, s.msg_info.rule_name,s.msg_info.rule_owner, s.msg_info.message,
s.msg_info.message_url, s.event_payload.event_instance_guid, s.event_
payload.event_type, s.event_payload.event_name, s.event_payload.event_msg, l_
categories_new, s.event_payload.source.source_type, s.event_payload.source.source_
name, s.event_payload.source.source_url, s.event_payload.severity, s.event_
payload.severity_code, s.event_payload.target.target_name, s.event_
payload.target.target_type, s.event_payload.target.target_url, s.event_
payload.target.host_name, s.event_payload.target.target_timezone, s.event_
payload.occurrence_date, l_ca_obj.JOB_GUID, l_ca_obj.JOB_NAME, l_ca_obj.JOB_OWNER,
l_ca_obj.JOB_TYPE, l_ca_obj.JOB_STATUS, l_ca_obj.JOB_STATUS_CODE, l_ca_obj.JOB_
STEP_OUTPUT, l_ca_obj.JOB_EXECUTION_GUID, l_ca_obj.JOB_STATE_CHANGE_GUID);
   ELSE
      INSERT INTO event_log (notification_type, repeat_count, ruleset_name, rule_
name, rule_owner, message, message_url, event_instance_guid, event_type, event_
name, event_msg, categories, source_obj_type, source_obj_name, source_obj_url,
severity, severity_code, target_name, target_type, target_url, host_name,
timezone, occured, ca_guid, ca_name, ca_owner, ca_type, ca_status, ca_status_code,
ca_job_step_output, ca_execution_guid, ca_stage_change_guid)
      VALUES (s.msg_info.notification_type, s.msg_info.repeat_count, s.msg_
info.ruleset_name, s.msg_info.rule_name, s.msg_info.rule_owner, s.msg_
info.message, s.msg_info.message_url, s.event_payload.event_instance_guid,
s.event_payload.event_type, s.event_payload.event_name, s.event_payload.event_msg,
l_categories_new, s.event_payload.source.source_type, s.event_
payload.source.source_name, s.event_payload.source.source_url, s.event_
payload.severity, s.event_payload.severity_code, s.event_payload.target.target_
name, s.event_payload.target.target_type, s.event_payload.target.target_url,
s.event_payload.target.host_name, s.event_payload.target.target_timezone, s.event_
payload.occurrence_date, null,null,null,null,null,null,null,null,null);
   END IF;
   COMMIT;
END log_event;
/
```

Example 4–12 PL/SQL Script to Log Incidents to a Table

```
CREATE TABLE incident_log (
  notification_type      VARCHAR2(32),
  repeat_count           NUMBER,
  ruleset_name           VARCHAR2(256),
  rule_owner             VARCHAR2(256),
  rule_name              VARCHAR2(256),
  message                VARCHAR2(4000),
  message_url            VARCHAR2(4000),
  incident_id            VARCHAR2(128),
  ticket_url             VARCHAR2(4000),
  assoc_event_cnt        NUMBER,
  severity               VARCHAR2(128),
  severity_code          VARCHAR2(32),
  priority               VARCHAR2(128),
  priority_code          VARCHAR2(32),
  status                 VARCHAR2(32),
  categories             VARCHAR2(1000),
  target_name            VARCHAR2(256),
  target_type            VARCHAR2(128),
  host_name              VARCHAR2(256),
  timezone               VARCHAR2(64),
  occured                DATE
)
;
```

```
   CREATE OR REPLACE PROCEDURE log_incident(s IN GC$NOTIF_INCIDENT_MSG)
IS
   l_src_info_array GC$NOTIF_SOURCE_INFO_ARRAY;
   l_src_info  GC$NOTIF_SOURCE_INFO;
   l_categories gc$category_string_array;
   l_target_obj GC$NOTIF_TARGET;
   l_target_name VARCHAR2(256);
   l_target_type VARCHAR2(256);
   l_target_timezone VARCHAR2(256);
   l_hostname VARCHAR2(256);
   l_categories_new VARCHAR2(1000);
BEGIN
     -- Save Incident categories
  IF l_categories IS NOT NULL
   THEN
     FOR c IN 1..l_categories.COUNT
     LOOP
       l_categories_new := (l_categories_new|| c || ' - ' || l_
categories(c)||',');
     END LOOP;
   END IF;

   -- GET target info
   l_src_info_array := s.incident_payload.incident_attrs.source_info_arr;
   IF l_src_info_array IS NOT NULL
   THEN
     FOR I IN 1..l_src_info_array.COUNT
     LOOP
       IF l_src_info_array(I).TARGET IS NOT NULL
       THEN
         l_target_name := l_src_info_array(I).TARGET.TARGET_NAME;
         l_target_type := l_src_info_array(I).TARGET.TARGET_TYPE;
         l_target_timezone := l_src_info_array(I).TARGET.TARGET_TIMEZONE;
         l_hostname := l_src_info_array(I).TARGET.HOST_NAME;
      END IF;
     END LOOP;
   END IF;

   -- save Incident notification message
   INSERT INTO incident_log(notification_type, repeat_count, ruleset_name, rule_
owner, rule_name, message, message_url, incident_id, ticket_url, assoc_event_cnt,
severity, severity_code, priority, priority_code, status, categories, target_name,
target_type, host_name, timezone, occured)
   VALUES (s.msg_info.notification_type, s.msg_info.repeat_count, s.msg_
info.ruleset_name, s.msg_info.rule_owner, s.msg_info.rule_name, s.msg_
info.message, s.msg_info.message_url, s.incident_payload.incident_attrs.id,
s.incident_payload.ticket_url, s.incident_payload.assoc_event_count, s.incident_
payload.incident_attrs.severity, s.incident_payload.incident_attrs.severity_code,
s.incident_payload.incident_attrs.priority, s.incident_payload.incident_
attrs.priority_code, s.incident_payload.incident_attrs.STATUS, l_categories_new,
l_target_name, l_target_type, l_hostname,l_target_timezone, s.incident_
payload.incident_attrs.creation_date);
   COMMIT;
END log_incident;
/
```

Example 4–13 PL/SQL Script to Log Problems to a Table

```
CREATE TABLE problem_log (
  notification_type      VARCHAR2(32),
  repeat_count           NUMBER,
  ruleset_name           VARCHAR2(256),
  rule_owner             VARCHAR2(256),
  rule_name              VARCHAR2(256),
  message                VARCHAR2(4000),
  message_url            VARCHAR2(4000),
  problem_key            VARCHAR2(850),
  assoc_incident_cnt     NUMBER,
  problem_id             NUMBER,
  owner                  VARCHAR2(256),
  severity               VARCHAR2(128),
  severity_code          VARCHAR2(32),
  priority               VARCHAR2(128),
  priority_code          VARCHAR2(32),
  status                 VARCHAR2(32),
  categories             VARCHAR2(1000),
  target_name            VARCHAR2(256),
  target_type            VARCHAR2(128),
  host_name              VARCHAR2(256),
  timezone               VARCHAR2(64),
  occured                DATE
)
;
     CREATE OR REPLACE PROCEDURE log_problem(s IN GC$NOTIF_PROBLEM_MSG)
IS
   l_src_info_array GC$NOTIF_SOURCE_INFO_ARRAY;
   l_src_info  GC$NOTIF_SOURCE_INFO;
   l_categories gc$category_string_array;
   l_target_obj GC$NOTIF_TARGET;
   l_target_name VARCHAR2(256);
   l_target_type VARCHAR2(256);
   l_target_timezone VARCHAR2(256);
   l_hostname VARCHAR2(256);
   l_categories_new VARCHAR2(1000);
BEGIN
     -- Save Problem categories
  l_categories := s.problem_payload.problem_attrs.categories;
  IF l_categories IS NOT NULL
   THEN
     FOR c IN 1..l_categories.COUNT
     LOOP
       l_categories_new := (l_categories_new|| c || ' - ' || l_
categories(c)||',');
     END LOOP;
   END IF;

   -- GET target info
   l_src_info_array := s.problem_payload.problem_attrs.source_info_arr;
   IF l_src_info_array IS NOT NULL
   THEN
     FOR I IN 1..l_src_info_array.COUNT
     LOOP
       IF l_src_info_array(I).TARGET IS NOT NULL
       THEN
         l_target_name := l_src_info_array(I).TARGET.TARGET_NAME;
         l_target_type := l_src_info_array(I).TARGET.TARGET_TYPE;
         l_target_timezone := l_src_info_array(I).TARGET.TARGET_TIMEZONE;
         l_hostname := l_src_info_array(I).TARGET.HOST_NAME;
      END IF;
     END LOOP;
   END IF;

  -- save Problem notification message
   INSERT INTO problem_log(notification_type, repeat_count, ruleset_name, rule_
owner, rule_name, message, message_url, problem_key, assoc_incident_cnt, problem_
id, owner,  severity, severity_code, priority, priority_code, status, categories,
target_name, target_type, host_name, timezone, occured)
   VALUES (s.msg_info.notification_type, s.msg_info.repeat_count, s.msg_
info.ruleset_name, s.msg_info.rule_owner, s.msg_info.rule_name, s.msg_
info.message, s.msg_info.message_url, s.problem_payload.problem_key,
s.problem_payload.ASSOC_INCIDENT_COUNT, s.problem_payload.problem_attrs.id,
s.problem_payload.problem_attrs.owner,s.problem_payload.problem_attrs.severity,
s.problem_payload.problem_attrs.severity_code, s.problem_payload.problem_
attrs.PRIORITY, s.problem_payload.problem_attrs.PRIORITY_CODE, s.problem_
payload.problem_attrs.status, l_categories_new, l_target_name, l_target_type, l_
hostname,l_target_timezone, s.problem_payload.problem_attrs.CREATION_DATE);
   COMMIT;
END log_problem;
/
```

4.4.2 Migrating Pre-12c PL/SQL Advanced Notification Methods

Pre-12*c* notifications map to event notifications in Enterprise Manager 12*c*. The event types metric_alert, target_availability and job_status_alert correspond to the pre-12c notification functionality.

> **Note:** Policy Violations are no longer available beginning with Enterprise Manager 12*c*.

This section describes the mapping between Enterprise Manager 12c PL/SQL notification payload to the pre-12c PL/SQL notification payload. You can use this information for updating the existing pre-12c PL/SQL user callback procedures to use the 12c PL/SQL notification payload.

Please note that Policy Violations are no longer supported in the 12c release.

4.4.2.1 Mapping for MGMT_NOTIFY_SEVERITY

When event type is metric_alert

Use the following map when gc$notif_event_payload .event_type='metric_alert'.

Table 4–8 Metric Alert Mapping

MGMT_NOTIFY_SEVERITY	12c Notification Payload
TARGET_NAME	gc$notif_target.target_name
TARGET_TYPE	gc$notif_target.target_type
TIMEZONE	gc$notif_target.target_timezone
HOST_NAME	gc$notif_target.host_name

Table 4–8 (Cont.) Metric Alert Mapping

MGMT_NOTIFY_SEVERITY	12c Notification Payload
MERTIC_NAME	gc$notif_event_attr.value where its name=' metric_group' in gc$notif_event_attr_array.
METRIC_DESCRIPTION	gc$notif_event_attr.value where its name=' metric_description' in gc$notif_event_attr_array.
METRIC_COLUMN	gc$notif_event_attr.value where its name=' metric_column' in gc$notif_event_attr_array.
METRIC_VALUE	gc$notif_event_attr.value where its name=' value' in gc$notif_event_attr_array.
KEY_VALUE	It is applied for multiple keys based metric when value of gc$notif_event_attr.name='num_keys' is not null and is greater than 0 in gc$notif_event_attr_array. See detail descriptions below.
KEY_VALUE_NAME	It is applied for multiple keys based metric when value of gc$notif_event_attr.name='num_keys' is not null and is greater than 0 in gc$notif_event_attr_array. See detail descriptions below.
KEY_VALUE_GUID	gc$notif_event_attr.value where its name='key_ value' in gc$notif_event_attr_array.
CTXT_LIST	gc$notif_event_context_array
COLLECTION_TIMESTAMP	gc$notif_event_payload. reported_date
SEVERITY_CODE	Derive from gc$notif_event_payload.severity_code, see Table 4–9, " Severity Code Mapping".
MESSAGE	gc$notif_msg_info.message
SEVERITY_GUID	gc$notif_event_attr.value where its name=' severity_guid' in gc$notif_event_attr_array.
METRIC_GUID	gc$notif_event_attr.value where its name=' metric_guid’ in gc$notif_event_attr_array.
TARGET_GUID	gc$notif_target.target_guid
RULE_OWNER	gc$notif_msg_info.rule_owner
RULE_NAME	gc$notif_msg_info.ruleset_name

The following example illustrates how to obtain similar pre-12c KEY_VALUE and KEY_VALUE_NAME from an Enterprise Manager 12c notification payload.

Example 4–14 Extracting KEY_VALUE and KEY_VALUE_NAME

```
-- Get the pre-12c KEY_VALUE and KEY_VALUE_NAME from an Enterprise Manager 12c
-- notification payload
-- parameters
--   IN Parameters:
--      event_msg : The event notification payload
--   OUT Parameters
--      key_value_name_out : the KEY_VALUE_NAME backward compitable to pre-12c
--                           notification payload
--      key_value_out      : the KEY_VALUE backward compitable to pre-12c
--                           notification payload
--
CREATE OR REPLACE PROCEDURE get_pre_12c_key_value(
          event_msg IN GC$NOTIF_EVENT_MSG,
          key_value_name_out OUT VARCHAR2,
          key_value_out OUT VARCHAR2)
IS

  l_key_columns MGMT_SHORT_STRING_ARRAY := MGMT_SHORT_STRING_ARRAY();
  l_key_column_values MGMT_MEDIUM_STRING_ARRAY := MGMT_MEDIUM_STRING_ARRAY();
  l_key_value VARCHAR2(1790) := NULL;
  l_num_keys NUMBER := 0;
  l_attrs gc$notif_event_attr_array;
  l_key_value_name VARCHAR2(512);
BEGIN
  l_attrs := event_msg.event_payload.event_attrs;
  key_value_name_out := NULL;
  key_value_out := NULL;

  IF l_attrs IS NOT NULL AND
     l_attrs.COUNT > 0
  THEN
    l_key_columns.extend(7);
    l_key_column_values.extend(7);
    FOR c IN 1..l_attrs.COUNT
    LOOP
      CASE l_attrs(c).name
        WHEN 'num_keys' THEN
          BEGIN
            l_num_keys := to_number(l_attrs(c).value);
          EXCEPTION
          WHEN OTHERS THEN
            -- should never happen, but guard against it l_num_keys := 0;
          END;
        WHEN 'key_value' THEN
          l_key_value := substr(l_attrs(c).nls_value,1,1290);
        WHEN 'key_column_1' THEN
          l_key_columns(1) := substr(l_attrs(c).nls_value,1,64);
        WHEN 'key_column_2' THEN
          l_key_columns(2) := substr(l_attrs(c).nls_value,1,64);
        WHEN 'key_column_3' THEN
          l_key_columns(3) := substr(l_attrs(c).nls_value,1,64);
        WHEN 'key_column_4' THEN
          l_key_columns(4) := substr(l_attrs(c).nls_value,1,64);
        WHEN 'key_column_5' THEN
          l_key_columns(5) := substr(l_attrs(c).nls_value,1,64);
        WHEN 'key_column_6' THEN
          l_key_columns(6) := substr(l_attrs(c).nls_value,1,64);
        WHEN 'key_column_7' THEN
          l_key_columns(7) := substr(l_attrs(c).nls_value,1,64);
        WHEN 'key_column_1_value' THEN
          l_key_column_values(1) := substr(l_attrs(c).nls_value,1,256);
        WHEN 'key_column_2_value' THEN
          l_key_column_values(2) := substr(l_attrs(c).nls_value,1,256);
        WHEN 'key_column_3_value' THEN
          l_key_column_values(3) := substr(l_attrs(c).nls_value,1,256);
        WHEN 'key_column_4_value' THEN
          l_key_column_values(4) := substr(l_attrs(c).nls_value,1,256);
        WHEN 'key_column_5_value' THEN
          l_key_column_values(5) := substr(l_attrs(c).nls_value,1,256);
        WHEN 'key_column_6_value' THEN
          l_key_column_values(6) := substr(l_attrs(c).nls_value,1,256);
        WHEN 'key_column_7_value' THEN
          l_key_column_values(7) := substr(l_attrs(c).nls_value,1,256);
        ELSE
          NULL;
      END CASE;
    END LOOP;

    -- get key_value and key_value_name when l_num_keys > 0

    IF l_num_keys > 0
    THEN
      -- get key value name
      IF l_key_columns IS NULL OR l_key_columns.COUNT = 0
      THEN
        key_value_name_out := NULL;
      ELSE
        l_key_value_name := NULL;
        FOR i in l_key_columns.FIRST..l_num_keys
        LOOP
          IF i > 1
          THEN
            l_key_value_name := l_key_value_name || ';';
          END IF;
          l_key_value_name := l_key_value_name || l_key_columns(i);
        END LOOP;
        key_value_name_out := l_key_value_name;
      END IF;

      -- get key_value
      IF l_num_keys = 1
      THEN
        key_value_out := l_key_value;
      ELSE
        l_key_value := NULL;
        IF l_key_column_values IS NULL OR l_key_column_values.COUNT = 0
        THEN
          key_value_out := NULL;
        ELSE
          FOR i in l_key_column_values.FIRST..l_num_keys
          LOOP
            IF i > 1
            THEN
              l_key_value := l_key_value || ';';
            END IF;
            l_key_value := l_key_value || l_key_column_values(i);

          END LOOP;
          --  max length for key value in pre-12c = 1290
          key_value_out := substr(l_key_value,1,1290);
        END IF;
      END IF;
    END IF; -- l_num_keys > 0
  END IF;  -- l_attrs IS NOT NULL
END get_pre_12c_key_value;
/
```

When the event type is metric_alert:

Use the following severity code mapping from 12c to pre-12c when the event type is *metric_alert*.

Table 4–9 Severity Code Mapping

12c Severity Code	Pre-12c Severity Code
GC_EVENT_RECEIVER.FATAL 32	MGMT_GLOBAL.G_SEVERITY_CRITICAL 25
GC_EVENT_RECEIVER.CRITICAL 16	MGMT_GLOBAL.G_SEVERITY_CRITICAL 25
GC_EVENT_RECEIVER.WARNING 8	MGMT_GLOBAL.G_SEVERITY_WARNING 20
GC_EVENT_RECEIVER.CLEAR 0	MGMT_GLOBAL.G_SEVERITY_CLEAR 15

When event type is target_availability:

Use the following map when gc$notif_event_payload .event_type='target_availability'.

Table 4–10 Target Availability Mapping

MGMT_NOTIFY_SEVERITY	12c Notification Payload
TARGET_NAME	gc$notif_target.target_name
TARGET_TYPE	gc$notif_target.target_type
TIMEZONE	gc$notif_target.target_timezone
HOST_NAME	gc$notif_target.host_name
MERTIC_NAME	Use fixed value "Response".
METRIC_DESCRIPTION	NULL
METRIC_COLUMN	Use fixed value "Status".
METRIC_VALUE	gc$notif_event_attr.value where its name='target_status' in gc$notif_event_attr_array.
KEY_VALUE	NULL
KEY_VALUE_NAME	NULL
KEY_VALUE_GUID	NULL
CTXT_LIST	gc$notif_event_context_array
COLLECTION_TIMESTAMP	gc$notif_event_payload. reported_date
SEVERITY_CODE	gc$notif_event_attr.value where its name=' avail_severity' in gc$notif_event_attr_array.
MESSAGE	gc$notif_msg_info.message
SEVERITY_GUID	gc$notif_event_attr.value where its name=' severity_guid' in gc$notif_event_attr_array.
METRIC_GUID	gc$notif_event_attr.value where its name=' metric_guid_id' in gc$notif_event_attr_array.
TARGET_GUID	gc$notif_target.target_guid
RULE_OWNER	gc$notif_msg_info.rule_owner
RULE_NAME	gc$notif_msg_info.ruleset_name

4.4.2.2 Mapping for MGMT_NOTIFY_JOB

Use the following map when gc$notif_event_payload .event_type=job_status_change'.

Table 4–11 Job Status Change Mapping

MGMT_NOTIFY_JOB	12c Notification Payload
JOB_NAME	gc$notif_source.source_name
JOB_OWNER	gc$notif_source.source_owner
JOB_TYPE	gc$notif_source.source_sub_type
JOB_STATUS	gc$notif_event_attr.value where its name=' execution_status_code' in gc$notif_event_attr_array.
STATE_CHANGE_GUID	gc$notif_event_attr.value where its name=' state_change_guid' in gc$notif_event_attr_array.
JOB_GUID	gc$notif_source.source_guid
EXECUTION_ID	gc$notif_event_attr.value where its name=' execution_id' in gc$notif_event_attr_array.
TARGETS	gc$notif_target.target_name, gc$notif_target.target_type
RULE_OWNER	gc$notif_msg_info.rule_owner
RULE_NAME	gc$notif_msg_info.ruleset_name
OCCURRED_DATE	gc$notif_event_payload. reported_date

4.4.2.3 Mapping for MGMT_NOTIFY_CORRECTIVE_ACTION

Note that corrective action related payload is populated when gc$notif_msg_info.notification_type is set to NOTIF_CA.

For mapping the following attributes, use the mapping information provided for MGMT_NOTIFY_SEVERITY object Table 4–8, " Metric Alert Mapping"

MERTIC_NAME

METRIC_COLUMN

METRIC_VALUE

KEY_VALUE

KEY_VALUE_NAME

KEY_VALUE_GUID

CTXT_LIST

RULE_OWNER

RULE_NAME

OCCURRED_DATE

For mapping the job related attributes in MGMT_NOTIFY_CORRECTIVE_ACTION object, use the following map.

Table 4–12 Corrective Action Mapping

MGMT_NOTIFY_CORRECTIVE_ACTION	12c Notification Payload
JOB_NAME	gc$ notif_corrective_action_job.job_name
JOB_OWNER	gc$ notif_corrective_action_job.job_owner
JOB_TYPE	gc$ notif_corrective_action_job.job_type
JOB_STATUS	gc$ notif_corrective_action_job.status_code
STATE_CHANGE_GUID	gc$ notif_corrective_action_job. job_state_change_guid
JOB_GUID	gc$ notif_corrective_action_job. job _guid
EXECUTION_ID	gc$ notif_corrective_action_job. job_execution_guid
OCCURRED_DATE	gc$ notif_corrective_action_job.occurred_date
TARGETS	There can be at most one target. Use the values from gc$notif_target.target_name, gc$notif_target.target_type for the associated target.

4.5 Sending SNMP Traps to Third Party Systems

Enterprise Manager supports integration with third-party management tools through the Simple Network Management Protocol (SNMP). For example, you can use SNMP to notify a third-party application that a selected metric has exceeded its threshold.

Important: In order for a third-party system to interpret traps sent by the OMS, the omstrap.v1 file must first be loaded into the third-party SNMP console. For more information about this file and its location, see "MIB Definition" on page 4-48.

The Enterprise Manager 12c version of the MIB file incorporates the 10g and 11g MIB content, thus ensuring backward compatibility with earlier Enterprise Manager releases.

Enterprise Manager supports both SNMP Version 1 and Version 3 traps. The traps are described by the MIB definition shown in Appendix B, "Enterprise Manager MIB Definition." See "Management Information Base (MIB)" on page 4-48 for an explanation of how the MIB works. If you are using Enterprise Manager 12c, see Appendix A, "Interpreting Variables of the Enterprise Manager MIB" and Appendix B, "Enterprise Manager MIB Definition." If you are upgrading from a pre-12c version of Enterprise Manager, see Appendix C, "SNMP Trap Mappings" for specific version mappings.

For Enterprise Manager 12c, SNMP traps are delivered for event notifications only. SNMP trap notifications are not supported for incidents or problems.

Note: Notification methods based on SNMP traps must be configured by an administrator with Super Administrator privileges before any user can then choose to select one or more of these SNMP trap methods while creating/editing a incident rule.

4.5.1 SNMP Version 1 Versus SNMP Version 3

SNMP Version 3 shares the same basic architecture of Version 1, but adds numerous enhancements to SNMP administration and security. The primary enhancement relevant to Enterprise Manager involves additional security levels that provide both authentication and privacy as well as authorization and access control.

User-based Security Model (USM)

USM defines the security-related procedures followed by an SNMP engine when processing SNMP messages. Enterprise Manager SNMP V3 support takes advantage of this added SNMP message-level security enhancement to provide a secure messaging environment.

USM protects against two primary security threats:

- Modification of information: The modification threat is the danger that some unauthorized entity may alter in-transit SNMP messages generated on behalf of an authorized principal in such a way as to effect unauthorized management operations, including falsifying the value of an object.
- Masquerade: The masquerade threat is the danger that management operations not authorized for some user may be attempted by assuming the identity of another user that has the appropriate authorizations.

For both SNMP versions, the basic methodology for setting up Enterprise Manager advanced notifications using SNMP traps remains the same:

1. **Define the notification method based on an SNMP trap**.
2. **Assign the notification method to an incident rule**.

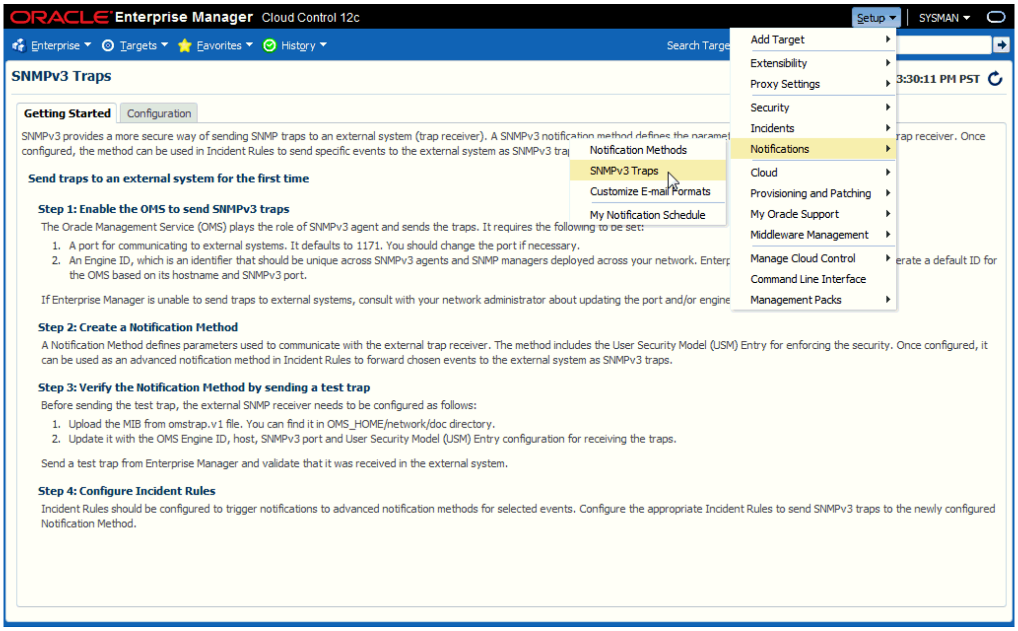
4.5.2 Working with SNMP V3 Trap Notification Methods

The procedure for defining an SNMP V3 trap notification method differs slightly from that of V1. Beginning with Enterprise Manager Release 12.1.0.4, a separate interface consolidates key information and configuration functionality pertaining to SNMP V3 trap notification methods. The SNMP V3 Trap interface helps guide you through the process of creating SNMP notification methods, enabling the OMS to send SNMP traps, and defining user security settings for SNMP trap notifications.

4.5.2.1 Configuring the OMS to Send SNMP Trap Notifications

Before creating an SNMP Trap notification method, you must enable at least one OMS is your environment to handle SNMP Trap notifications. For SNMP V3, the OMS serves as an SNMP Agent which sends traps to the SNMP Manager that is monitoring all SNMP Agents deployed in the network.

1. From the **Setup** menu, select **Notifications** and then **SNMP V3 Traps**. The Getting Started page displays. This page documents the high-level workflow for configuring Enterprise Manager to send traps to third-party SNMP Managers.



SNMPv3 Traps

SNMPv3 provides a more secure way of sending SNMP traps to an external system (trap receiver). A SNMPv3 notification method defines the paramet … rap receiver. Once configured, the method can be used in Incident Rules to send specific events to the external system as SNMPv3 tra

Send traps to an external system for the first time

Step 1: Enable the OMS to send SNMPv3 traps

The Oracle Management Service (OMS) plays the role of SNMPv3 agent and sends the traps. It requires the following to be set:

1. A port for communicating to external systems. It defaults to 1171. You should change the port if necessary.
2. An Engine ID, which is an identifier that should be unique across SNMPv3 agents and SNMP managers deployed across your network. Enterp … erate a default ID for the OMS based on its hostname and SNMPv3 port.

If Enterprise Manager is unable to send traps to external systems, consult with your network administrator about updating the port and/or engine

Step 2: Create a Notification Method

A Notification Method defines parameters used to communicate with the external trap receiver. The method includes the User Security Model (USM) Entry for enforcing the security. Once configured, it can be used as an advanced notification method in Incident Rules to forward chosen events to the external system as SNMPv3 traps.

Step 3: Verify the Notification Method by sending a test trap

Before sending the test trap, the external SNMP receiver needs to be configured as follows:

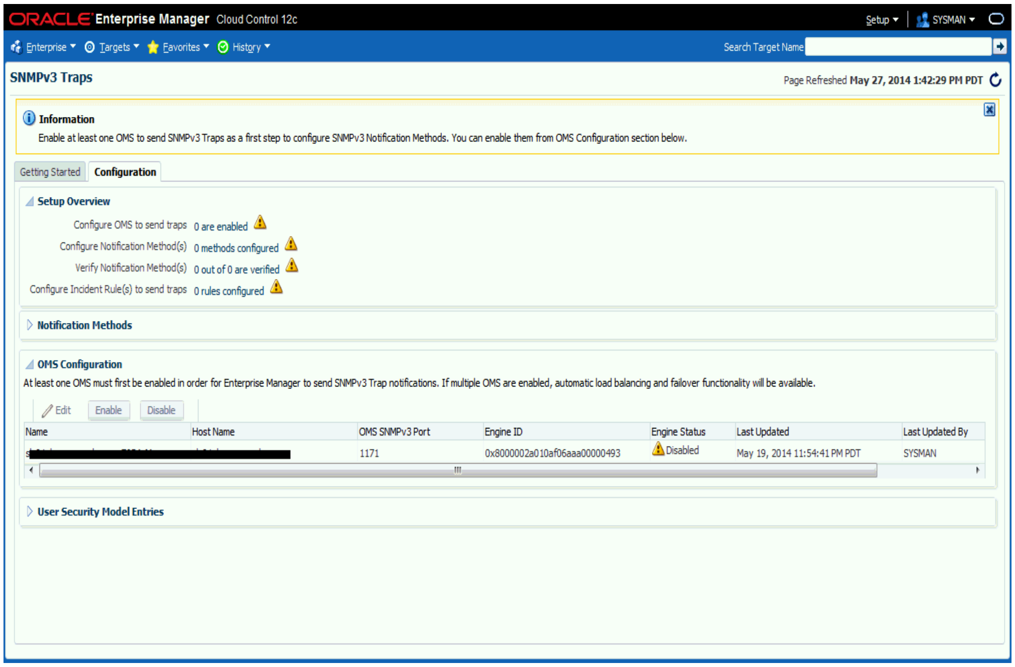
1. Upload the MIB from omstrap.v1 file. You can find it in OMS_HOME/network/doc directory.
2. Update it with the OMS Engine ID, host, SNMPv3 port and User Security Model (USM) Entry configuration for receiving the traps.

Send a test trap from Enterprise Manager and validate that it was received in the external system.

Step 4: Configure Incident Rules

Incident Rules should be configured to trigger notifications to advanced notification methods for selected events. Configure the appropriate Incident Rules to send SNMPv3 traps to the newly configured Notification Method.

2. Click the **Configuration** tab. The Configuration page displays.



SNMPv3 Traps

Page Refreshed May 27, 2014 1:42:29 PM PDT

Information

Enable at least one OMS to send SNMPv3 Traps as a first step to configure SNMPv3 Notification Methods. You can enable them from OMS Configuration section below.

Setup Overview

Configure OMS to send traps	0 are enabled ⚠
Configure Notification Method(s)	0 methods configured ⚠
Verify Notification Method(s)	0 out of 0 are verified ⚠
Configure Incident Rule(s) to send traps	0 rules configured ⚠

Notification Methods

OMS Configuration

At least one OMS must first be enabled in order for Enterprise Manager to send SNMPv3 Trap notifications. If multiple OMS are enabled, automatic load balancing and failover functionality will be available.

Name	Host Name	OMS SNMPv3 Port	Engine ID	Engine Status	Last Updated	Last Updated By
[redacted]	[redacted]	1171	0x8000002a010af06aaa00000493	⚠ Disabled	May 19, 2014 11:54:41 PM PDT	SYSMAN

User Security Model Entries

3. In the OMS Configuration region, select the OMS you wish to enable.

4. Check the following for each OMS and make changes, if necessary:

   - OMS requires a port for SNMPv3 traps. Check if the default port can be used by OMS.
   - OMS requires a unique Engine ID for sending traps. By default, it is being generated from the host name and port.

5. Click **Enable**.

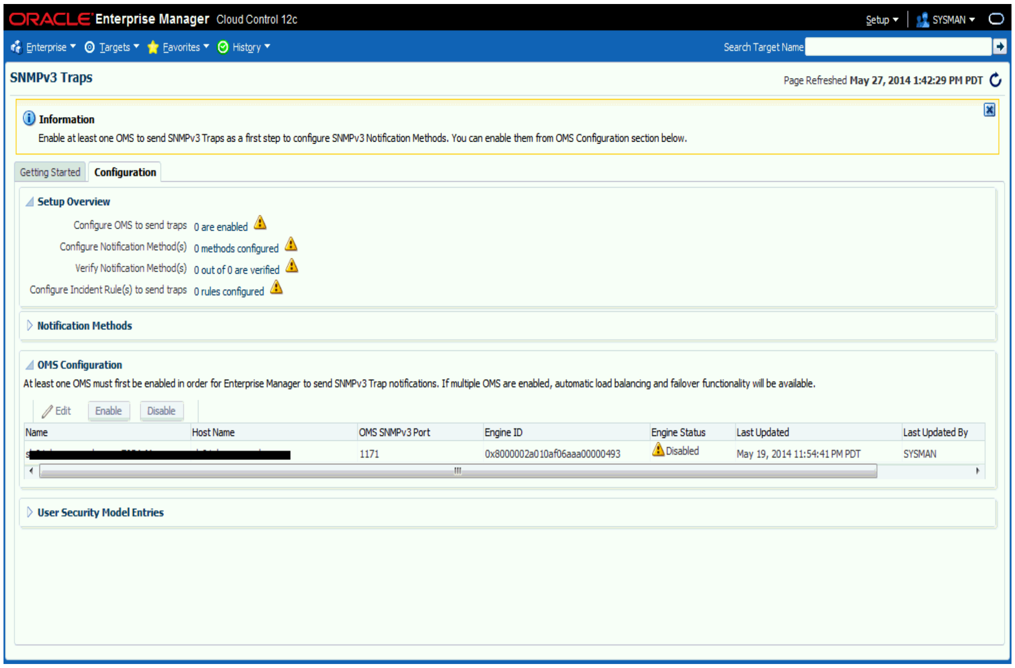
4.5.2.2 Creating/Editing an SNMP V3 Trap Notification Method

Once an OMS has been enabled to send SNMP traps notifications, the next step is to create a notification method than can be used by an incident rule.

1. From the **Setup** menu, select **Notifications** and then **SNMP V3 Traps**. The Getting Started page displays.

> **Note:** If want to edit an existing Notification Method, select the desired method from the Notification Methods region and click **Edit**.

2. Click the **Configuration** tab. The Configuration page displays.



SNMPv3 Traps

Page Refreshed May 27, 2014 1:42:29 PM PDT

Information

Enable at least one OMS to send SNMPv3 Traps as a first step to configure SNMPv3 Notification Methods. You can enable them from OMS Configuration section below.

Setup Overview

Configure OMS to send traps	0 are enabled ⚠
Configure Notification Method(s)	0 methods configured ⚠
Verify Notification Method(s)	0 out of 0 are verified ⚠
Configure Incident Rule(s) to send traps	0 rules configured ⚠

Notification Methods

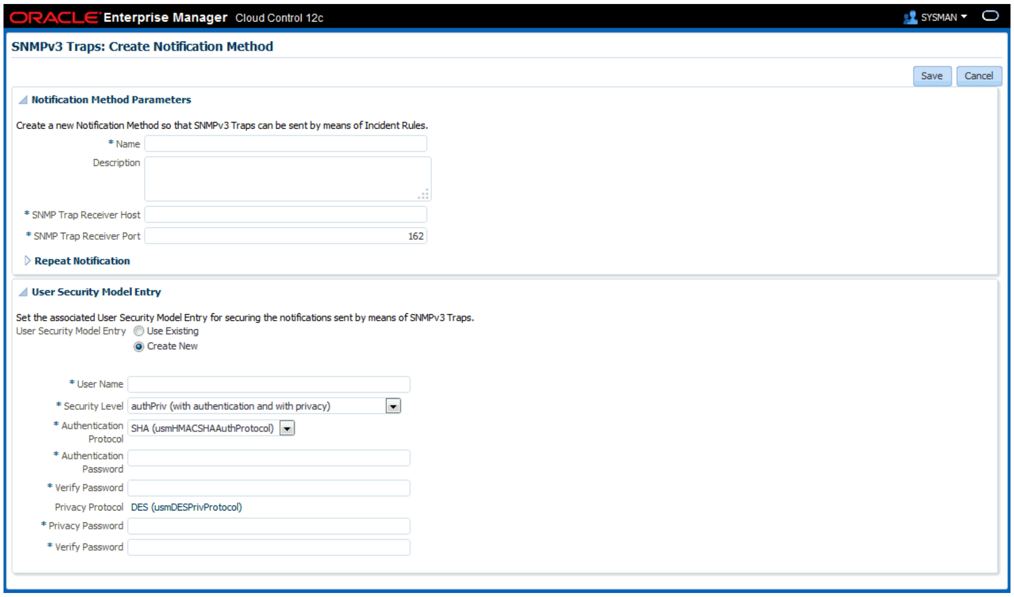
OMS Configuration

At least one OMS must first be enabled in order for Enterprise Manager to send SNMPv3 Trap notifications. If multiple OMS are enabled, automatic load balancing and failover functionality will be available.

Name	Host Name	OMS SNMPv3 Port	Engine ID	Engine Status	Last Updated	Last Updated By
[redacted]	[redacted]	1171	0x8000002a010af06aaa00000493	⚠ Disabled	May 19, 2014 11:54:41 PM PDT	SYSMAN

User Security Model Entries

3. From the Notification Methods region, click **Create**. The SNMPv3 Traps: Create Notification Method page displays.



SNMPv3 Traps: Create Notification Method

Notification Method Parameters

Create a new Notification Method so that SNMPv3 Traps can be sent by means of Incident Rules.

* Name	
Description	
* SNMP Trap Receiver Host	
* SNMP Trap Receiver Port	162

Repeat Notification

User Security Model Entry

Set the associated User Security Model Entry for securing the notifications sent by means of SNMPv3 Traps.

User Security Model Entry ○ Use Existing
● Create New

* User Name	
* Security Level	authPriv (with authentication and with privacy) ▾
* Authentication Protocol	SHA (usmHMACSHAAuthProtocol) ▾
* Authentication Password	
* Verify Password	
Privacy Protocol	DES (usmDESPrivProtocol)
* Privacy Password	
* Verify Password	

4. Enter the requisite Notification Method definition parameters. Note: You can enable Repeat Notifications at this point.

5. If you choose to create a new User Security Model entry, from the User Security Model region, ensure the **Create New** option is chosen.

    1. Specify a **Username** that uniquely identifies the credential. SNMP V3 allows multiple usernames to be set in an SNMP Agent as well as SNMP Manager applications.

    2. Select a **Security Level** from the drop-down menu. Available parameters become available depending on the security level. There are three levels from which to choose:

        AuthPriv (Authentication + Privacy:) The sender's identity must be confirmed by the receiver (authentication). SNMP V3 messages are encrypted by the sender and must be decrypted by the receiver (privacy).

        AuthNoPriv (Authentication only): The receiver must authenticate the sender's identity before accepting the message.

        NoAuthNoPriv (no security): Neither sender identity confirmation nor message encryption is used.

    3. For AuthPriv and AuthNoPriv security levels, choose a the desired **Authentication Protocol**. Two authentication protocols are available:

        Secure Hash Algorithm (SHA)

        Message Digest algorithm (MD5)

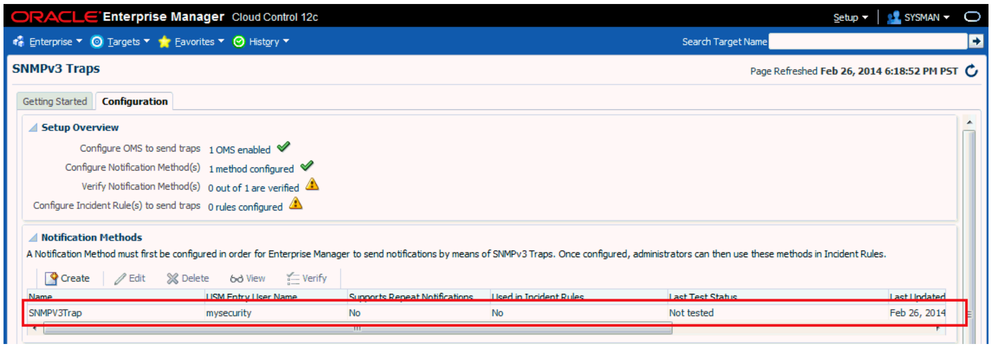
        The authentication protocols are used to build the message digest when the message is authenticated.

        Privacy Protocol (used for the AuthPriv security level) is used to encrypt/decrypt messages. USM uses the Data Encryption Standard (DES). The **Privacy Password** is used in conjunction with the Privacy Protocol. the privacy password on both the SNMP Agent and SNMP Manager must match in order for encryption/decryption to succeed.

    If you have already have predefined User Security Model entries, choose the **Use Existing** option and select one of the USM entries from the drop-down menu. USM entries are listed by username.

    > **Important:** Ensure that the USM credentials are identical in OMS and the external trap receiver. If they do not match, Enterprise Manager will still send the SNMP trap, but the trap will not be received. If the USM credentials are invalid, Enterprise Manager will still send the SNMP trap, however, the trap will not be received as the incorrect credentials will result in an authentication error at the SNMP receiver. This type of authentication error will not be apparent from the Enterprise Manager console.

6. Once you have entered the requisite Notification Method and USM parameters, click **Save**. The newly created notification method appears in the Notification Method region of the Configuration page.



SNMPv3 Traps

Page Refreshed **Feb 26, 2014 6:18:52 PM PST**

Setup Overview

Configure OMS to send traps	1 OMS enabled ✓
Configure Notification Method(s)	1 method configured ✓
Verify Notification Method(s)	0 out of 1 are verified ⚠
Configure Incident Rule(s) to send traps	0 rules configured ⚠

Notification Methods

A Notification Method must first be configured in order for Enterprise Manager to send notifications by means of SNMPv3 Traps. Once configured, administrators can then use these methods in Incident Rules.

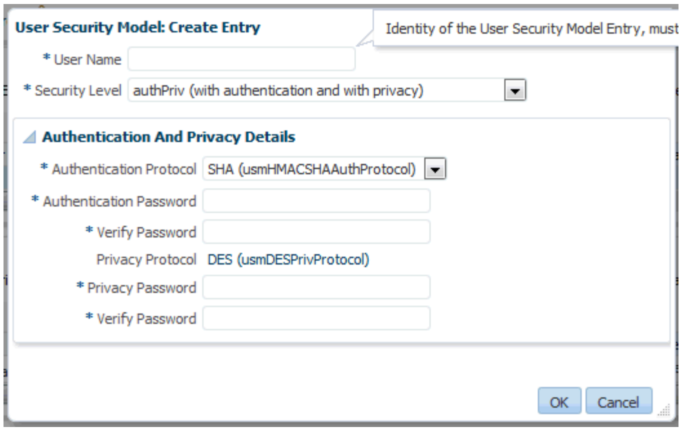
Name	USM Entry User Name	Supports Repeat Notifications	Used in Incident Rules	Last Test Status	Last Updated
SNMPV3Trap	mysecurity	No	No	Not tested	Feb 26, 2014

Note: Once you have defined the SNMP V3 Trap notification method, you must add it to a rule. See "Creating a Rule to Send SNMP Traps to Third Party Systems" on page 3-63 for instructions.

4.5.2.3 Editing a User Security Model Entry

You can add USM entries at any time.

1. From the **Setup** menu, select **Notifications**, and then **SNMP V3 Traps**.
2. Click on the **Configurations** tab.
3. From the User Security Model Entries region, click **Create**. The User Security Model Entries dialog displays.



User Security Model: Create Entry

Identity of the User Security Model Entry, must

* User Name	
* Security Level	authPriv (with authentication and with privacy)

Authentication And Privacy Details

* Authentication Protocol	SHA (usmHMACSHAAuthProtocol)
* Authentication Password	
* Verify Password	
Privacy Protocol	DES (usmDESPrivProtocol)
* Privacy Password	
* Verify Password	

4. Specify a **Username** that uniquely identifies the credential. SNMP V3 allows multiple usernames to be set in an SNMP Agent as well as SNMP Manager applications.
5. Select a **Security Level** from the drop-down menu. Available parameters become available depending on the security level. There are three levels from which to choose:

   AuthPriv (Authentication + Privacy:) The sender's identity must be confirmed by the receiver (authentication). SNMP V3 messages are encrypted by the sender and must be decrypted by the receiver (privacy).

   AuthNoPriv (Authentication only): The receiver must authenticate the sender's identity before accepting the message.

   NoAuthNoPriv (no security): Neither sender identity confirmation nor message encryption is used.

6. For AuthPriv and AuthNoPriv security levels, choose a the desired **Authentication Protocol**. Two authentication protocols are available:

   Secure Hash Algorithm (SHA)

   Message Digest algorithm (MD5)

   The authentication protocols are used to build the message digest when the message is authenticated.

   Privacy Protocol (used for the AuthPriv security level) is used to encrypt/decrypt messages. USM uses the Data Encryption Standard (DES). The **Privacy Password** is used in conjunction with the Privacy Protocol. the privacy password on both the SNMP Agent and SNMP Manager must match in order for encryption/decryption to succeed.

7. Click **OK**.

   The new USM username will appear in the User Security Model Entries table. When creating new SNMP V3 Trap notification methods, the USM username will appear as a selectable option from the **Existing Entries** drop-down menu.

   After editing the USM, you should verify the change via the notification methods that use it.

4.5.2.4 Viewing Available SNMP V3 Trap Notification Methods

To view available SNMP V3 Trap notification methods:

1. From the **Setup** menu, select **Notifications**, and then **SNMP V3 Traps**.
2. Click on the **Configurations** tab.
3. The Notification Methods region displays existing SNMP V3 Trap notification methods.

4.5.2.5 Deleting an SNMP V3 Trap Notification Method

To delete available SNMP V3 Trap notification methods:

1. From the **Setup** menu, select **Notifications**, and then **SNMP V3 Traps**.
2. Click on the **Configurations** tab.
3. From the Notification Methods region, select an existing SNMP V3 Trap notification method.
4. Click **Delete**.

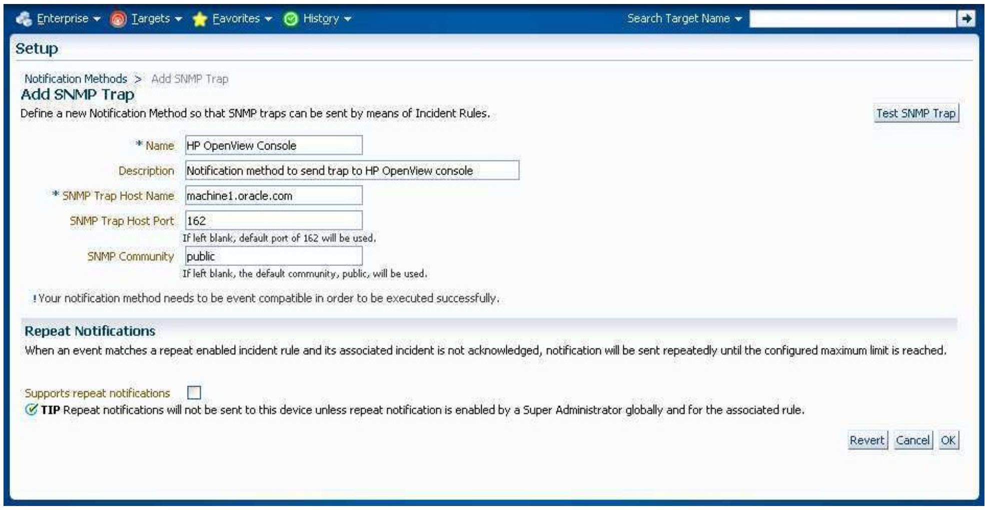
4.5.3 Creating an SNMP V1 Trap

Step 1: Define a new notification method based on an SNMP trap.

Log in to Enterprise Manager as a Super Administrator. From the **Setup** menu, select **Notifications** and then select **Notification Method** to access the Notification Methods page. From this page you can add a new method based on an SNMP trap.

You must provide the name of the host (machine) on which the SNMP master agent is running and other details as shown in the following example. As shown in, the SNMP host will receive your SNMP traps.

Figure 4–7 SNMP Trap Required Information



Setup

Notification Methods > Add SNMP Trap

Add SNMP Trap

Define a new Notification Method so that SNMP traps can be sent by means of Incident Rules.

* Name	HP OpenView Console
Description	Notification method to send trap to HP OpenView console
* SNMP Trap Host Name	machine1.oracle.com
SNMP Trap Host Port	162 If left blank, default port of 162 will be used.
SNMP Community	public If left blank, the default community, public, will be used.

! Your notification method needs to be event compatible in order to be executed successfully.

Repeat Notifications

When an event matches a repeat enabled incident rule and its associated incident is not acknowledged, notification will be sent repeatedly until the configured maximum limit is reached.

Supports repeat notifications ☐

✓ **TIP** Repeat notifications will not be sent to this device unless repeat notification is enabled by a Super Administrator globally and for the associated rule.

Note: A Test SNMP Trap button exists for you to test your setup.

Metric severity information will be passed as a series of variables in the SNMP trap.

Step 2: Assign the notification method to a rule.

You can edit an existing rule (or create a new incident rule), then add an action to the rule that subscribes to the advanced notification method. For instructions on setting up incident rules using SNMP traps, see "Creating a Rule to Send SNMP Traps to Third Party Systems" on page 3-63.

Example SNMP Trap Implementation

In this scenario, you want to identify the unique issues from the SNMP traps that are sent. Keep in mind that all events that are related to the same issue are part of the same event sequence. Each event sequence has a unique identification number.

An event sequence is a sequence of related events that represent the life of a specific issue from the time it is detected and an event is raised to the time it is fixed and a corresponding *clear* event is generated. For example, a warning metric alert event is raised when the CPU utilization of a host crosses 80%. This starts the event sequence representing the issue *CPU Utilization of the host is beyond normal level*. Another critical event is raised for the same issue when the CPU utilization goes above 90% and the event is added to the same event sequence. After a period of time, the CPU utilization returns to a normal level and a *clear* event is raised. At this point, the issue is resolved and the event sequence is closed.

The SNMP trap sent for this scenario is shown in Example 4–15. Each piece of information is sent as a variable embedded in the SNMP Trap.

Example 4–15 SNMP Trap

```
*************V1 TRAP***[1]****************
Community : public
Enterprise :1.3.6.1.4.1.111.15.2
Generic :6
Specific :3
TimeStamp :67809
Agent adress :10.240.36.109
```

```
1.3.6.1.4.1.111.15.3.1.1.2.1: NOTIF_NORMAL
1.3.6.1.4.1.111.15.3.1.1.3.1: CPU Utilization is 92.658%, crossed warning (80) or
critical (90) threshold.
1.3.6.1.4.1.111.15.3.1.1.4.1:
https://sampleserver.oracle.com:5416/em/redirect?pageType=sdk-core-event-console-d
etailEvent&issueID=C77AE9E578F00773E040F00A6D242F90
1.3.6.1.4.1.111.15.3.1.1.5.1: Critical
1.3.6.1.4.1.111.15.3.1.1.6.1: CRITICAL
1.3.6.1.4.1.111.15.3.1.1.7.1: 0
1.3.6.1.4.1.111.15.3.1.1.8.1:
1.3.6.1.4.1.111.15.3.1.1.9.1:
1.3.6.1.4.1.111.15.3.1.1.10.1: Aug 17, 2012 3:26:36 PM PDT
1.3.6.1.4.1.111.15.3.1.1.11.1: Capacity
1.3.6.1.4.1.111.15.3.1.1.12.1: Capacity
1.3.6.1.4.1.111.15.3.1.1.13.1: Metric Alert
1.3.6.1.4.1.111.15.3.1.1.14.1: Load:cpuUtil
1.3.6.1.4.1.111.15.3.1.1.15.1: 281
1.3.6.1.4.1.111.15.3.1.1.16.1:
1.3.6.1.4.1.111.15.3.1.1.17.1: No
1.3.6.1.4.1.111.15.3.1.1.18.1: New
1.3.6.1.4.1.111.15.3.1.1.19.1: None
1.3.6.1.4.1.111.15.3.1.1.20.1: 0
1.3.6.1.4.1.111.15.3.1.1.21.1: sampleserver.oracle.com
1.3.6.1.4.1.111.15.3.1.1.22.1:
https://sampleserver.oracle.com:5416/em/redirect?pageType=TARGET_
HOMEPAGE&targetName=sampleserver.oracle.com&targetType=host
1.3.6.1.4.1.111.15.3.1.1.23.1: Host
1.3.6.1.4.1.111.15.3.1.1.24.1: sampleserver.oracle.com
1.3.6.1.4.1.111.15.3.1.1.25.1: SYSMAN
1.3.6.1.4.1.111.15.3.1.1.26.1:
1.3.6.1.4.1.111.15.3.1.1.27.1: 5.8.0.0.0
1.3.6.1.4.1.111.15.3.1.1.28.1: Operating System=Linux, Platform=x86_64,
1.3.6.1.4.1.111.15.3.1.1.29.1:
1.3.6.1.4.1.111.15.3.1.1.30.1:
1.3.6.1.4.1.111.15.3.1.1.31.1:
1.3.6.1.4.1.111.15.3.1.1.32.1:
1.3.6.1.4.1.111.15.3.1.1.33.1:
1.3.6.1.4.1.111.15.3.1.1.34.1:
1.3.6.1.4.1.111.15.3.1.1.35.1:
1.3.6.1.4.1.111.15.3.1.1.36.1:
1.3.6.1.4.1.111.15.3.1.1.37.1:
1.3.6.1.4.1.111.15.3.1.1.38.1:
1.3.6.1.4.1.111.15.3.1.1.39.1: SnmpNotifRuleset
1.3.6.1.4.1.111.15.3.1.1.40.1: SnmpNotifRuleset,SnmpNotifEvent
1.3.6.1.4.1.111.15.3.1.1.41.1: SYSMAN
1.3.6.1.4.1.111.15.3.1.1.42.1: C77AE9E578F00773E040F00A6D242F90
1.3.6.1.4.1.111.15.3.1.1.43.1:
1.3.6.1.4.1.111.15.3.1.1.44.1:
1.3.6.1.4.1.111.15.3.1.1.45.1:
1.3.6.1.4.1.111.15.3.1.1.46.1: CPU Utilization is 92.658%, crossed warning (80) or
critical (90) threshold., Incident created by rule (Name = Incident management
Ruleset for all targets, Incident creation Rule for metric alerts.; Owner =
<SYSTEM>).
1.3.6.1.4.1.111.15.3.1.1.61.1: Metric GUID=0C71A1AFAC2D7199013837DA35522C08
1.3.6.1.4.1.111.15.3.1.1.62.1: Severity GUID=C77AE9E578EC0773E040F00A6D242F90
1.3.6.1.4.1.111.15.3.1.1.63.1: Cycle GUID=C77AE9E578EC0773E040F00A6D242F90
1.3.6.1.4.1.111.15.3.1.1.64.1: Collection Name=LoadLinux
1.3.6.1.4.1.111.15.3.1.1.65.1: Metric Group=Load
1.3.6.1.4.1.111.15.3.1.1.66.1: Metric=CPU Utilization (%)
1.3.6.1.4.1.111.15.3.1.1.67.1: Metric Description=
1.3.6.1.4.1.111.15.3.1.1.68.1: Metric value=92.658
1.3.6.1.4.1.111.15.3.1.1.69.1: Key Value=
1.3.6.1.4.1.111.15.3.1.1.70.1:
1.3.6.1.4.1.111.15.3.1.1.71.1:
1.3.6.1.4.1.111.15.3.1.1.72.1:
1.3.6.1.4.1.111.15.3.1.1.73.1:
1.3.6.1.4.1.111.15.3.1.1.74.1:
1.3.6.1.4.1.111.15.3.1.1.75.1:
1.3.6.1.4.1.111.15.3.1.1.76.1:
1.3.6.1.4.1.111.15.3.1.1.77.1:
1.3.6.1.4.1.111.15.3.1.1.78.1:
1.3.6.1.4.1.111.15.3.1.1.79.1:
1.3.6.1.4.1.111.15.3.1.1.80.1:
1.3.6.1.4.1.111.15.3.1.1.81.1:
1.3.6.1.4.1.111.15.3.1.1.82.1:
1.3.6.1.4.1.111.15.3.1.1.83.1:
1.3.6.1.4.1.111.15.3.1.1.84.1: Number of keys=0
1.3.6.1.4.1.111.15.3.1.1.85.1:
**************END V1 TRAP******************
```

This following example illustrates how OIDs are used during the lifecycle of an event. Here, for one event (while the event is open), the event sequence OID remains the same even though the event severity changes.

The OID for the event sequence is:

```
1.3.6.1.4.1.111.15.3.1.1.42.1: C77AE9E578F00773E040F00A6D242F90
```

The OID for the event severity code is:

```
1.3.6.1.4.1.111.15.3.1.1.6.1: CRITICAL
```

When the event clears, these OIDs show the same event sequence with a different severity code:

The OID for the event sequence is:

```
1.3.6.1.4.1.111.15.3.1.1.42.1: C77AE9E578F00773E040F00A6D242F90
```

The OID for the event severity code is:

```
1.3.6.1.4.1.111.15.3.1.1.6.1: CLEAR
```

The length of the SNMP OID value is limited to 2560 bytes by default. Configure the emoms property *oracle.sysman.core.notification.snmp.max_oid_length* to change the default limit.

4.5.4 SNMP Traps: Moving from Previous Enterprise Manager Releases to 12c

Note: When you upgrade from a pre-Enterprise Manager 12c release to 12c, SNMP advanced notification methods defined using previous versions of Enterprise Manager (pre-12c) will continue to function without modification.

For Enterprise Manager 11g and earlier, there were two types of SNMP traps:

- Alerts
- Job Status

For Enterprise Manager 12c there is now a single, comprehensive SNMP trap type that covers all available event types such as metric alerts, target availability, compliance standard violations, or job status changes. For more information about pre-12*c* to 12*c* SNMP trap mappings, see Appendix C, "SNMP Trap Mappings." Traps will conform to the older Enterprise Manager MIB definition. Hence, pre-Enterprise Manager 12c traps will continue to be sent. See Appendix C, "SNMP Trap Mappings" for more information.

Also, for Enterprise Manager 12c, size of SNMP trap has increased in order to accommodate all event types and provide more comprehensive information. By default, the maximum SNMP packet size is 5120 bytes. If the third party system has a limit in the size of SNMP trap it can receive, you can change the default size of SNMP trap that Enterprise Manager sends. To change the default packet size, set this *emoms* `oracle.sysman.core.notification.snmp_packet_length` parameter, and then bounce the OMS.

Note: When limiting the SNMP trap packet size, Oracle recommends not setting the oracle.sysman.core.notification.snmp_packet_length parameter any lower than 3072 bytes (3K).

The Enterprise Manager 12c MIB includes all pre-Enterprise Manager 12c MIB definitions. Hence, if you have an Enterprise Manager 12c MIB in your third party system, you can receive SNMP traps from both pre-Enterprise Manager 12c as well as Enterprise Manager 12c sites. For detailed information on version mapping, see Appendix C, "SNMP Trap Mappings."

4.6 Management Information Base (MIB)

Enterprise Manager Cloud Control can send SNMP Traps to third-party, SNMP-enabled applications. Details of the trap contents can be obtained from the management information base (MIB) variables. The following sections discuss Enterprise Manager MIB variables in detail.

4.6.1 About MIBs

A MIB is a text file, written in ASN.1 notation, which describes the variables containing the information that SNMP can access. The variables described in a MIB, which are also called MIB objects, are the items that can be monitored using SNMP. There is one MIB for each element being monitored. Each monolithic or subagent consults its respective MIB in order to learn the variables it can retrieve and their characteristics. The encapsulation of this information in the MIB is what enables master agents to register new subagents dynamically — everything the master agent needs to know about the subagent is contained in its MIB. The management framework and management applications also consult these MIBs for the same purpose. MIBs can be either standard (also called public) or proprietary (also called private or vendor).

The actual values of the variables are not part of the MIB, but are retrieved through a platform-dependent process called "instrumentation". The concept of the MIB is very important because all SNMP communications refer to one or more MIB objects. What is transmitted to the framework is, essentially, MIB variables and their current values.

4.6.2 MIB Definition

You can find the SNMP MIB file at the following location:

OMS_HOME/network/doc/omstrap.v1

> **Note:** The omstrap.v1 file is compatible with both SNMP V1 and SNMP V3.

The file *omstrap.v1* is the OMS MIB.

For more information, see Appendix A, "Interpreting Variables of the Enterprise Manager MIB."

A hardcopy version of omstrap.v1 can be found in Appendix B, "Enterprise Manager MIB Definition."

The length of the SNMP OID value is limited to 2560 bytes by default. Configure emoms property *oracle.sysman.core.notification.snmp.max_oid_length* to change the default limit.

For Enterprise Manager 12c, SNMP traps are delivered for event notifications only. SNMP trap notifications are not supported for incidents or problems.

> **Note:** SNMP advanced notification methods defined using previous versions of Enterprise Manager (pre-12c) will continue to function without modification. Traps will conform to the older Enterprise Manager MIB definition.

4.6.3 Reading the MIB Variable Descriptions

This section covers the format used to describe MIB variables. Note that the STATUS element of SNMP MIB definition, Version 1, is not included in these MIB variable descriptions. Since Oracle has implemented all MIB variables as CURRENT, this value does not vary.

4.6.3.1 Variable Name

Syntax
Maps to the SYNTAX element of SNMP MIB definition, Version 1.

Max-Access
Maps to the MAX-ACCESS element of SNMP MIB definition, Version 1.

Status
Maps to the STATUS element of SNMP MIB definition, Version 1.

Explanation
Describes the function, use and precise derivation of the variable. (For example, a variable might be derived from a particular configuration file parameter or performance table field.) When appropriate, incorporates the DESCRIPTION part of the MIB definition, Version 1.

Typical Range
Describes the typical, rather than theoretical, range of the variable. For example, while integer values for many MIB variables can theoretically range up to 4294967295, a typical range in an actual installation will vary to a lesser extent. On the other hand, some variable values for a large database can actually exceed this "theoretical" limit (a "wraparound"). Specifying that a variable value typically ranges from 0 to 1,000 or

1,000 to 3 billion will help the third-party developer to develop the most useful graphical display for the variable.

Significance
Describes the significance of the variable when monitoring a typical installation. Alternative ratings are Very Important, Important, Less Important, or Not Normally Used. Clearly, the DBA will want to monitor some variables more closely than others. However, which variables fall into this category can vary from installation to installation, depending on the application, the size of the database, and on the DBA's objectives. Nevertheless, assessing a variable's significance relative to the other variables in the MIB can help third-party developers focus their efforts on those variables of most interest to the most DBAs.

Related Variables
Lists other variables in this MIB, or other MIBs implemented by Oracle, that relate in some way to this variable. For example, the value of this variable might derive from that of another MIB variable. Or perhaps the value of this variable varies inversely to that of another variable. Knowing this information, third-party developers can develop useful graphic displays of related MIB variables.

Suggested Presentation
Suggests how this variable can be presented most usefully to the DBA using the management application: as a simple value, as a gauge, or as an alarm, for example.

4.7 Passing Corrective Action Status Change Information

Passing corrective action status change attributes (such as new status, job name, job type, or rule owner) to PL/SQL procedures or OS commands/scripts allows you to customize automated responses to status changes. For example, you many want to call an OS script to open a trouble ticket for an in-house support trouble ticket system if a critical corrective action fails to run. In this case, you will want to pass status (for example, Problems or Aborted) to the script to open a trouble ticket and escalate the problem.

4.7.1 Passing Corrective Action Execution Status to an OS Command or Script

The notification system passes information to an OS script or executable via system environment variables. Conventions used to access environmental variables vary depending on the operating system:

- UNIX: $ENV_VARIABLE
- MS Windows: %ENV_VARIABLE%

The notification system sets the following environment variables before calling the script. The notification system will set the environment variable $NOTIF_TYPE = NOTIF_CA for Corrective Action Execution. The script can then use any or all of these variables within the logic of the script.

Following table lists the environment variables for corrective action, they are populated when a corrective action is completed for an event.

Table 4–13 Corrective Action Environment Variables

Environment Variable	Description
CA_JOB_STATUS	Corrective action job execution status.
CA_JOB_NAME	Name of the Corrective Action.

Table 4–13 (Cont.) Corrective Action Environment Variables

Environment Variable	Description
CA_JOB_OWNER	Owner of Corrective Action.
CA_JOB_STEP_OUTPUT	The value will be the text output from the Corrective Action execution.
CA_JOB_TYPE	Corrective Action Job type

4.7.2 Passing Corrective Action Execution Status to a PLSQL Procedure

The notification system passes corrective action status change information to PL/SQL procedure - `PROCEDURE p(event_msg IN gc$notif_event_msg)`. The instance gc$notif_corrective_action_job object is defined in event_msg.event_payload. corrective_action if event_msg. msg_info. notification_type is equal to GC$NOTIFICATIONNOTIF_CA. When a corrective action executes, the notification system calls the PL/SQL procedure associated with the incident rule and passes the populated object to the procedure. The procedure is then able to access the fields of the object that has been passed to it. See Table 4–44, " Corrective Action Job-Specific Attributes" for details.

The following status codes are possible values for the job_status field of the MGMT_NOTIFY_CORRECTIVE_ACTION object.

Table 4–14 Corrective Action Status Codes

Name	Datatype	Value
SCHEDULED_STATUS	NUMBER(2)	1
EXECUTING_STATUS	NUMBER(2)	2
ABORTED_STATUS	NUMBER(2)	3
FAILED_STATUS	NUMBER(2)	4
COMPLETED_STATUS	NUMBER(2)	5
SUSPENDED_STATUS	NUMBER(2)	6
AGENTDOWN_STATUS	NUMBER(2)	7
STOPPED_STATUS	NUMBER(2)	8
SUSPENDED_LOCK_STATUS	NUMBER(2)	9
SUSPENDED_EVENT_STATUS	NUMBER(2)	10
SUSPENDED_BLACKOUT_STATUS	NUMBER(2)	11
STOP_PENDING_STATUS	NUMBER(2)	12
SUSPEND_PENDING_STATUS	NUMBER(2)	13
INACTIVE_STATUS	NUMBER(2)	14
QUEUED_STATUS	NUMBER(2)	15
FAILED_RETRIED_STATUS	NUMBER(2)	16
WAITING_STATUS	NUMBER(2)	17
SKIPPED_STATUS	NUMBER(2)	18
REASSIGNED_STATUS	NUMBER(2)	20

4.8 Passing Job Execution Status Information

Passing job status change attributes (such as new status, job name, job type, or rule owner) to PL/SQL procedures or OS commands/scripts allows you to customize automated responses to status changes. For example, you many want to call an OS script to open a trouble ticket for an in-house support trouble ticket system if a critical job fails to run. In this case you will want to pass status (for example, Problems or Aborted) to the script to open a trouble ticket and escalate the problem. The job execution status information is one of event type - job_status_change event, and its content is in OS command and PL/SQL payload as described in Section 4.3, "Sending Notifications Using OS Commands and Scripts" and Section 4.4, "Sending Notifications Using PL/SQL Procedures".

4.8.1 Passing Job Execution Status to a PL/SQL Procedure

The notification system passes job status change information to a PL/SQL procedure via the event_msg.event_payload object where event_type is equal to job_status_change. An instance of this object is created for every status change. When a job changes status, the notification system calls the PL/SQL `p(event_msg IN gc$notif_event_msg)` procedure associated with the incident rule and passes the populated object to the procedure. The procedure is then able to access the fields of the event_msg.event_payload object that has been passed to it.

Table 4–15 lists all corrective action status change attributes that can be passed:

Table 4–15 Job Status Attributes

Attribute	Datatype	Additional Information
event_msg.event_payload.source.source_name	VARCHAR2(128)	The job name.
event_msg.event_payload.source.source_owner	VARCHAR2(256)	The owner of the job.
event_msg.event_payload.source.source_sub_type	VARCHAR2(32)	The type of the job.
event_msg.event_payload. event_attrs(i).value where event_attrs(i).name='execution_status'	NUMBER	The new status of the job.
event_msg.event_payload. event_attrs(i).value where event_attrs(i).name='state_change_guid'	RAW(16)	The GUID of the state change record.
event_msg.event_payload.source.source_guid	RAW(16)	The unique id of the job.
event_msg target.event_payload. event_attrs(i).value where event_attrs(i).name='execution_id'	RAW(16)	The unique id of the execution.

Table 4–15 (Cont.) Job Status Attributes

Attribute	Datatype	Additional Information
event_msg.event_payload.target	gc$notif_target	Target Information object..
event_msg.msg_info.rule_owner	VARCHAR2(64)	The name of the notification rule that cause the notification to be sent.
event_msg.msg_info.rule_name	VARCHAR2(132)	The owner of the notification rule that cause the notification to be sent.
event_msg.event_payload. reported_date	DATE	The time and date when the status change happened.

When a job status change occurs for the job, the notification system creates an instance of the event_msg.event_payload. event_attrs(i).value where event_attrs(i).name=' execution_status' object and populates it with values from the status change. The following status codes have been defined as constants in the MGMT_JOBS package and can be used to determine the type of status in the job_status field of the event_msg.event_payload. event_attrs(i).value where event_attrs(i).name=' execution_status' object.

Table 4–16 Job Status Codes

Name	Datatype	Value
SCHEDULED_STATUS	NUMBER(2)	1
EXECUTING_STATUS	NUMBER(2)	2
ABORTED_STATUS	NUMBER(2)	3
FAILED_STATUS	NUMBER(2)	4
COMPLETED_STATUS	NUMBER(2)	5
SUSPENDED_STATUS	NUMBER(2)	6
AGENTDOWN_STATUS	NUMBER(2)	7
STOPPED_STATUS	NUMBER(2)	8
SUSPENDED_LOCK_STATUS	NUMBER(2)	9
SUSPENDED_EVENT_STATUS	NUMBER(2)	10
SUSPENDED_BLACKOUT_STATUS	NUMBER(2)	11
STOP_PENDING_STATUS	NUMBER(2)	12
SUSPEND_PENDING_STATUS	NUMBER(2)	13
INACTIVE_STATUS	NUMBER(2)	14
QUEUED_STATUS	NUMBER(2)	15
FAILED_RETRIED_STATUS	NUMBER(2)	16
WAITING_STATUS	NUMBER(2)	17
SKIPPED_STATUS	NUMBER(2)	18
REASSIGNED_STATUS	NUMBER(2)	20

Example 4–16 PL/SQL Procedure Using a Status Code (Job)

```
CREATE  TABLE job_log (jobid RAW(16), status_code NUMBER(2), occured DATE);

CREATE OR REPLACE PROCEDURE LOG_JOB_STATUS_CHANGE(event_msg IN GC$NOTIF_EVENT_MSG)
```

```
IS
  l_attrs gc$notif_event_attr_array;
  exec_status_code NUMBER(2) := NULL;
  occured_date DATE := NULL;
  job_guid RAW(16) := NULL;

BEGIN
  IF event_msg.event_payload.event_type = 'job_status_change'
  THEN
    l_attrs := event_msg.event_payload.event_attrs;
    IF l_attrs IS NOT NULL
    THEN
      FOR i IN 1..l_attrs.COUNT
      LOOP
        IF l_attrs(i).name = 'exec_status_code'
        THEN
          exec_status_code := TO_NUMBER(l_attrs(i).value);
        END IF;
      END LOOP;
    END IF;

    occured_date := event_msg.event_payload.reported_date;
    job_guid := event_msg.event_payload.source.source_guid;
    -- Log all jobs' status
    BEGIN
      INSERT INTO job_log (jobid, status_code, occured)
      VALUES (job_guid, exec_status_code, occured_date);
    EXCEPTION
    WHEN OTHERS
    THEN
      -- If there are any problems then get the notification retried
      RAISE_APPLICATION_ERROR(-20000, 'Please retry');
    END;
    COMMIT;

  ELSE
    null; -- it is not a job_status_change event, ignore
  END IF;
END LOG_JOB_STATUS_CHANGE;
/
```

4.8.2 Passing Job Execution Status to an OS Command or Script

The notification system passes job execution status information to an OS script or executable via system environment variables. Conventions used to access environmental variables vary depending on the operating system:

- UNIX: $ENV_VARIABLE
- MS Windows: %ENV_VARIABLE%

The notification system sets the following environment variables before calling the script. The script can then use any or all of these variables within the logic of the script.

Table 4–17 Environment Variables

Environment Variable	Description
SOURCE_OBJ_NAME	The name of the job.
SOURCE_OBJ_OWNE	The owner of the job.

Table 4–17 (Cont.) Environment Variables

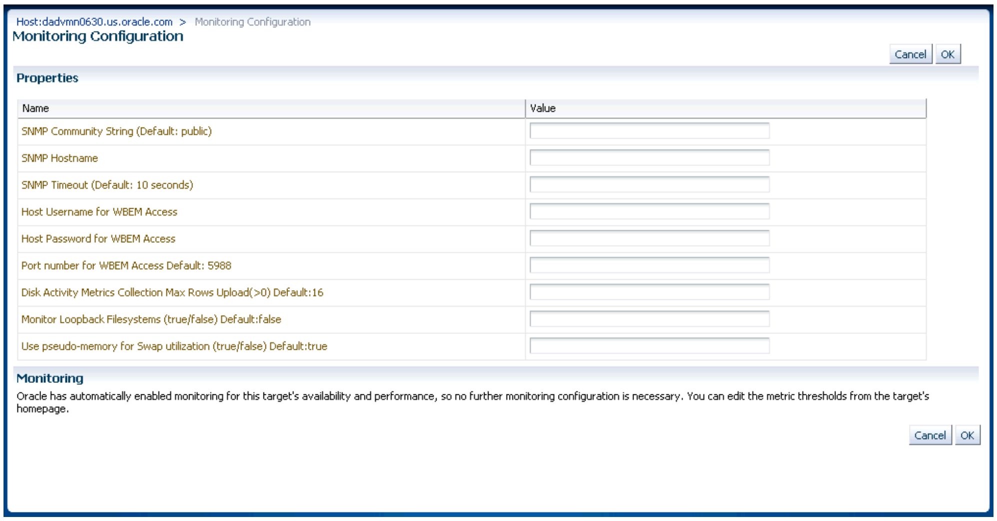
Environment Variable	Description
SOURCE_OBJ_SUB_TYPE	The type of job.
EXEC_STATUS_CODE	The job status.
EVENT_REPORTED_ TIME	Time when the severity occurred.
TARGET_NAME	The name of the target.
TARGET_TYPE	The type of the target.
RULE_NAME	Name of the notification rule that resulted in the severity.
RULE_OWNER	Name of the Enterprise Manager administrator who owns the notification rule.

4.9 Passing User-Defined Target Properties to Notification Methods

Enterprise Manager allows you to define target properties (accessed from the target home page) that can be used to store environmental or usage context information specific to that target. Target property values are passed to custom notification methods where they can be processed using conditional logic or simply passed as additional alert information to third-party devices, such as ticketing systems. By default, Enterprise Manager passes all defined target properties to notification methods.

> **Note:** Target properties are not passed to notification methods when short e-mail format is used.

Figure 4–8 Host Target Properties



Host:dadvmn0630.us.oracle.com > Monitoring Configuration

Monitoring Configuration

Properties

Name	Value
SNMP Community String (Default: public)	
SNMP Hostname	
SNMP Timeout (Default: 10 seconds)	
Host Username for WBEM Access	
Host Password for WBEM Access	
Port number for WBEM Access Default: 5988	
Disk Activity Metrics Collection Max Rows Upload(>0) Default:16	
Monitor Loopback Filesystems (true/false) Default:false	
Use pseudo-memory for Swap utilization (true/false) Default:true	

Monitoring

Oracle has automatically enabled monitoring for this target's availability and performance, so no further monitoring configuration is necessary. You can edit the metric thresholds from the target's homepage.

4.10 Notification Reference

This section contains the following reference material:

- EMOMS Properties
- Passing Event, Incident, Problem Information to an OS Command or Script

- Passing Information to a PL/SQL Procedure
-
- Troubleshooting Notifications

4.10.1 EMOMS Properties

EMOMS properties can be used for controlling the size and format of the short e-mail. The following table lists emoms properties for Notification System.

Table 4–18 emoms Properties for Notifications

Property Name	Default Value	Description
oracle.sysman.core.notification.emails_per_minute	250	Email delivery limits per minute. The Notification system uses this value to throttle number of Email delivery per minutes. Customer should set the value lower if doesn't want to over flow the Email server, or set the value higher if the Email server can handle high volume of Emails.
oracle.sysman.core.notification.cmds_per_minute	100	OS Command delivery limits per minute. The Notification system uses this value to throttle number of OS Command delivery per minutes.
oracle.sysman.core.notification.os_cmd_timeout	30	OS Command delivery timeout in seconds. This value indicates how long to allow OS process to execute the OS Command delivery. Set this value higher if the OS command script requires longer time to complete execution.
oracle.sysman.core.notification.plsql_per_minute	250	PL/SQL delivery limits per minute. The Notification system uses this value to throttle number of PL/SQL delivery per minutes.
em.notification.java_per_minute	500	JAVA delivery limits per minute. The Notification system uses this value to throttle number of Java delivery per minutes.
em.notification.ticket_per_minute	250	Ticket delivery limits per minute. The Notification system uses this value to throttle number of Ticket delivery per minutes.
oracle.sysman.core.notification.traps_per_minute	250	SNMP delivery limits per minute. The Notification system uses this value to control the number of SNMP trap per minutes.

Table 4–18 (Cont.) emoms Properties for Notifications

Property Name	Default Value	Description
oracle.sysman.core.notification.locale .plsql	OMS Locale	This property specifies the Locale delivered by advanced PL/SQL notification. The customer can define this property to overwrite the default Locale where the OMS is installed. Valid Locales: ■ en (English) ■ de (German) ■ es (Spanish) ■ fr (French) ■ it (Italian) ■ ja (Japanese) ■ ko (Korean) ■ pt_br (Portuguese, Brazilian) ■ zh_cn (Chinese, simplified) ■ zh_tw (Chinese, traditional)
oracle.sysman.core.notification.locale .email	OMS Locale	This property specifies the Locale delivered by Email. Customer can define this property to overwrite the default Locale where the OMS is installed. Valid Locales: ■ en (English) ■ de (German) ■ es (Spanish) ■ fr (French) ■ it (Italian) ■ ja (Japanese) ■ ko (Korean) ■ pt_br (Portuguese, Brazilian) ■ zh_cn (Chinese, simplified) ■ zh_tw (Chinese, traditional)

Table 4–18 (Cont.) emoms Properties for Notifications

Property Name	Default Value	Description
oracle.sysman.core.notification.locale.oscmd	OMS Locale	This property specifies the Locale delivered by OS Command. Customer can define this property to overwrite the default Locale where the OMS is installed. Valid Locales: ■ en (English) ■ de (German) ■ es (Spanish) ■ fr (French) ■ it (Italian) ■ ja (Japanese) ■ ko (Korean) ■ pt_br (Portuguese, Brazilian) ■ zh_cn (Chinese, simplified) ■ zh_tw (Chinese, traditional)
oracle.sysman.core.notification.locale.snmp	OMS Locale	This property specifies the Locale delivered by SNMP trap. Customer can define this property to overwrite the default Locale where the OMS is installed. Valid Locales: ■ en (English) ■ de (German) ■ es (Spanish) ■ fr (French) ■ it (Italian) ■ ja (Japanese) ■ ko (Korean) ■ pt_br (Portuguese, Brazilian) ■ zh_cn (Chinese, simplified) ■ zh_tw (Chinese, traditional)
oracle.sysman.core.notification.oscmd.max_env_var_length	512	The maximum length of OS Common environment variable value.
oracle.sysman.core.notification.snmp.max_oid_length	2560	The maximum length of SNMP OID value.
oracle.sysman.core.notification.min_delivery_threads	6	The minimum number of active threads in the thread pool initially and number of active threads are running when system is in low activities. Setting the value higher will use more system resources, but will deliver more notifications.
oracle.sysman.core.notification.max_delivery_threads	24	The maximum number of active threads in the thread pool when the system is in the high activities. This value should greater than em.notification.min_delivery_threads. Setting the value higher will use more system resources and deliver more notifications.

Table 4–18 (Cont.) emoms Properties for Notifications

Property Name	Default Value	Description
oracle.sysman.core.notification.short_format_length	>=1 (155)	The size limit of the total number of characters in short email format. The customer should modify this property value to fit their email or pager limit content size. The email subject is restricted to a maximum of 80 characters for short email format notifications.
oracle.sysman.core.notification.snmp_packet_length	<=1 (5120)	The maximum size of SNMP Protocol Data unit.
oracle.sysman.core.notification.email_content_transfer_encoding	8-bit, 7-bit(QP), 7-bit(BASE64) (8-bit)	The character set that can encode the Email. Oracle supports three character sets : 8-bit, 7-bit(QP), and7-bit(BASE64).
oracle.sysman.core.notification.emails_per_connection	>=1 (20)	The maximum number of emails delivered to same email gateway before switching to the next available email gateway (assumes customers have configured multiple email gateways). This property is used for email gateway load balance.
oracle.sysman.core.notification.short_format	both, subject, body (both)	Use short format on both subject and body, subject only, or body only..
oracle.sysman.core.notification.send_prior_status_after_agent_unreachable_clears	True	By default , a notification is sent indicating a target's status whenever the monitoring Agent comes out of *unreachable* status, even if the target's status has not changed. Use this emoms property to enable (True)/disable (False) the duplicate target status notification. To disable duplicate target status notifications, set this property to *False*: **1.**emctl set property oracle.sysman.core.notification.send_prior_status_after_agent_unreachable_clears -value false **2.** Restart the OMS. To enable duplicate target status notifications, set the property to *True*. **1.** emctl set property oracle.sysman.core.notification.send_prior_status_after_agent_unreachable_clears -value true **2.** Restart the OMS.

You must establish the maximum size your device can support and whether the message is sent in subject, body or both.

You can modify the emoms properties by using the Enterprise Manager command line control `emctl get/set/delete/list` property command.

Note: The following commands require an OMS restart in order for the changes to take place.

Get Property Command

```
emctl get [-sysman_pwd "sysman password"]-name
oracle.sysman.core.notification.short_format_length
```

Set Property Command

```
emctl set  property -name oracle.sysman.core.notification.short_format_length
-value 155
```

Emoms Properties Entries for a Short E-mail Format

```
emctl set  property -name oracle.sysman.core.notification.short_format_length
-value 155
emctl set property -name oracle.sysman.core.notification.short_format -value both
```

4.10.2 Passing Event, Incident, Problem Information to an OS Command or Script

The notification system passes information to an OS script or executable using system environment variables.

Conventions used to access environmental variables vary depending on the operating system:

- UNIX: $ENV_VARIABLE
- Windows:%ENV_VARIABLE%

The notification system sets the following environment variables before calling the script. The script can then use any or all of these variables within the logic of the script.

4.10.2.1 Environment Variables Common to Event, Incident and Problem

Table 4–19 Generic Environment Variables

Environment Variable	Description
NOTIF_TYPE	Type of notification and possible values NOTIF_NORMAL, NOTIF_RETRY, NOTIF_DURATION, NOTIF_REPEAT, NOTIF_CA, NOTIF_RCA
REPEAT_COUNT	How many times the notification has been sent out before this notification.
RULESET_NAME	The name of the ruleset that triggered this notification.
RULE_NAME	The name of the rule that triggered this notification.
RULE_OWNER	The owner of the ruleset that triggered this notification.
MESSAGE	The message of the event, incident, or problem.
MESSAGE_URL	EM console URL for this message.

Table 4–20 Category-Related Environment Variables

Environment Variable	Description
CATEGORIES_COUNT	Number of categories in this notification. This value is equal to1 if one category is associated with event, incident or problem. It is equal to 0 if no category associated with event, incident or problem.
CATEGORY_CODES_ COUNT	Number of category codes in this notification.
CATEGORY_n	Category is translated based on locale defined in OMS server. Valid values for the suffix "_n" are between 1.. $CATEGORIES_ COUNT
CATEGORY_CODE_n	Codes for the categories. Valid values for the suffix "_n" are between 1..$CATEGORY_CODES_COUNT

Table 4–21 lists the common environment variables for User Defined Target Properties. They will be populated under the following cases: (a) When an event has a related target, (b) When an incident or a problem have single event source and have a related target.

Table 4–21 User-Defined Target Property Environment Variables

Environment Variable	Description
ORCL_GTP_COMMENT	Comment
ORCL_GTP_CONTACT	Contact
ORCL_GTP_COST_ CENTER	Cost Center
ORCL_GTP_ DEPARTMENT	Department
ORCL_GTP_ DEPLOYMENT_TYPE	Deployment type
ORCL_GTP_LINE_OF_ BUS	Line of Business
ORCL_GTP_LOCATION	Location

4.10.2.2 Event Notification-Specific Environment Variables

Table 4–22 Event Notification-Specific Environment Variables

Environment Variable	Description
EVENT_NAME	Event Name.
EVENT_REPORTED_ TIME	Event reported date.
EVENT_SOURCE_ COUNT	Number of Sources associated with this event.
EVENT_TYPE	Event type.
EVENT_OCCURRENCE_ TIME	Event occurrence time.
EVENT_TYPE_ATTRS	The list of event type specific attributes.
EVENT_CONTEXT_ ATTRS	Event context data.

Table 4–22 (Cont.) Event Notification-Specific Environment Variables

Environment Variable	Description
LAST_UPDATED_TIME	Last updated time
SEQUENCE_ID	The unique event sequence identifier. An event sequence may consist of one or more events. All events in this sequence have the same event sequence ID.
SEVERITY	Severity of event, it is translated.
SEVERITY_CODE	Code for event severity. Possible values are the following. FATAL, CRITICAL, WARNING, MINOR_WARNING, INFORMATIONAL, and CLEAR
ACTION_MSG	Message describing the action to take for resolving the event.
TOTAL_OCCURRENCE_COUNT	Total number of duplicate occurrences
RCA_DETAILS	If RCA is associated with this events.
CURRENT_OCCURRENCE_COUNT	Total number of occurrences of the event in the current collection period. This attribute only applies to de-duplicated events.
CURRENT_FIRST_OCCUR_DATE	Time stamp when the event first occurred in the current collection period. This attribute only applies to de-duplicated events.
CURRENT_LAST_OCCUR_DATE_DESC	Time stamp when the e vent last occurred in the current collection period. This attribute only applies to de-duplicated events.

Table 4–23 lists the environment variables for the incident associated with an event. They are populated when the event is associated with an incident.

Table 4–23 Associated Incident Environment Variables

Environment Variable	Description
ASSOC_INCIDENT_ACKNOWLEDGED_BY_OWNER	Set to yes, if associated incident was acknowledged by owner
ASSOC_INCIDENT_ACKNOWLEDGED_DETAILS	The details of associated incident acknowledgement. For example: No - if not acknowledged Yes By userName - if acknowledged
ASSOC_INCIDENT_STATUS	Associated Incident Status
ASSOC_INCIDENT_ID	Associated Incident ID
ASSOC_INCIDENT_PRIORITY	Associated Incident priority. Supported value are Urgent, Very High, High, Medium,Low, None.
ASSOC_INCIDENT_OWNER	Associated Incident Owner if it is existed.
ASSOC_INCIDENT_ESCALATION_LEVEL	Escalation level of the associated incident has a value between 0 to 5.

Table 4–24 lists the common environment variables related to the Source Object. They are populated when $SOURCE_OBJ_TYPE is not TARGET.

Table 4–24 Source Object-Related Environment Variables

Environment Variable	Description
SOURCE_OBJ_TYPE	Type of the Source object. For example, JOB, TEMPLATE.
SOURCE_OBJ_NAME	Source Object Name.
SOURCE_OBJ_NAME_URL	Source's event console URL.
SOURCE_OBJ_SUB_TYPE	Sub-type of the Source object. For example, it provides the underlying job type for job status change events.
SOURCE_OBJ_OWNER	Owner of the Source object.

Table 4–25 lists the common environment variables for the target, associated with the given issue. They are populated when the issue is related to a target.

Table 4–25 Target-Related Environment Variables

Environment Variable	Description
TARGET_NAME	Name of Target
TARGET_TYPE	Type of Target
TARGET_OWNER	Owner of Target
HOST_NAME	The name of the host on which the target is deployed upon.
TARGET_URL	Target's Enterprise Manager Console URL.
TARGET_LIFECYCLE_STATUS	Life Cycle Status of the target. Possible values: Production, Mission Critical, Stage, Test, and Development. It is null if not defined.
TARGET_VERSION	Target Version of the target

4.10.2.3 Environment Variables Specific to Event Types

Events are classified into multiple types. For example, the mertc_alert event type is used for modeling metric alerts. You can use SQL queries to list the event types in your deployment as well as their event-specific payload. The following SQL example can be used to list all internal event type names that are registered in Enterprise Manager.

```
Select event_class as event_type, upper(name) as env_var_name
from em_event_class_attrs
where notif_order != 0
and event_class is not null
union
select event_class as event_type, upper(name) || '_NLS' as env_var_name
from em_event_class_attrs
where notif_order != 0
and event_class is not null
and is_translated = 1
order by event_type, env_var_name;
```

The environment variable payload specific to each event type can be accessed via the OS scripts. The following tables list notification attributes for the most critical event types.

Table 4–26 Environment Variables Specific to Metric Alert Event Type

Environment Variable	Description
COLL_NAME	The name of the collection collecting the metric.
COLL_NAME_NLS	The translated name of the collection collecting the metric
KEY_COLUMN_X	Internal name of Key Column X where X is a number between 1 and 7.
KEY_COLUMN_X_NLS	Translated name of Key Column X where X is a number between 1 and 7.
KEY_COLUMN_X_VALUE	Value of Key Column X where X is a number between 1 and 7.
KEY_VALUE	Monitored object for the metric corresponding to the Metric Alert event.
METRIC_COLUMN	The name of the metric column
METRIC_COLUMN_NLS	The translated name of the metric column.
METRIC_DESCRIPTION	Brief description of the metric.
METRIC_DESCRIPTION_NLS	Translated brief description of the metric.
METRIC_GROUP	The name of the metric.
METRIC_GROUP_NLS	The translated name of the metric
NUM_KEYS	The number of key metric columns in the metric.
SEVERITY_GUID	The GUID of the severity record associated with this metric alert.
CYCLE_GUID	A unique identifier for a metric alert cycle, which starts from the time the metric alert is initially generated until the time it is clear.
VALUE	Value of the metric when the event triggered.

Table 4–27 Environment variables specific to Target Availability Event Type

Environment Variable	Description
AVAIL_SEVERITY	The transition severity that resulted in the status of the target to change to the current availability status. Possible Values for AVAIL_SEVERITY ■ 15 (Target Up) ■ 25 (Target Down) ■ 115 (Agent Unreachable, Cleared) ■ 125 (Agent Unreachable) ■ 215 (Blackout Ended) ■ 225 (Blackout Started) ■ 315 (Collection Error Cleared) ■ 325 (Collection Error) ■ 425 (No Beacons Available) ■ 515 (Status Unknown)
AVAIL_SUB_STATE	The substatus of a target for the current status.

Table 4–27 (Cont.) Environment variables specific to Target Availability Event Type

Environment Variable	Description
CYCLE_GUID	A unique identifier for a metric alert cycle, which starts from the time the metric alert is initially generated until the time it is clear.
METRIC_GUID	Metric GUID of response metric.
SEVERITY_GUID	The GUID of the severity record associated with this availability status.
TARGET_STATUS	The current availability status of the target.
TARGET_STATUS_NLS	The translated current availability status of the target.

Table 4–28 Environment variables specific to Job Status Change event type

Environment Variable	Description
EXECUTION_ID	Unique ID of the job execution..
EXECUTION_LOG	The job output of the last step executed.
EXECUTION_STATUS	The internal status of the job execution.
EXECUTION_STATUS_NLS	The translated status of the job execution.
EXEC_STATUS_CODE	Execution status code of job execution. For possible values, see Table 4–16, " Job Status Codes".
STATE_CHANGE_GUID	Unique ID of last status change

You can use SQL queries to list the deployed event types in your deployment and the payload specific to each one of them. The following SQL can be used to list all internal event type names which are registered in the Enterprise Manager.

```
select class_name as event_type_name from em_event_class;
```

Following SQL lists environment variables specific to metric_alert event type.

```
select env_var_name
  from
    ( Select event_class as event_type, upper(name) as env_var_name
     from em_event_class_attrs
    where notif_order != 0
    and event_class is not null
    union
    select event_class as event_type, upper(name) || '_NLS' as env_var_name
    from em_event_class_attrs
    where notif_order != 0
    and event_class is not null
    and is_translated = 1)
    where event_type = 'metric_alert';
```

You can also obtain the description of notification attributes specific to an event type directly from the Enterprise Manager console:

1. From the **Setup** menu, select **Notifications**, then select **Customize Email Formats**.
2. Select the event type.
3. Click **Customize**.

4. Click **Show Predefined Attributes**.

Environment variables, ending with the suffix _NLS, provide the translated value for given attribute. For example, METRIC_COLUMN_NLS environment variable will provide the translated value for the metric column attribute. Translated values will be in the locale of the OMS.

4.10.2.4 Environment Variables Specific to Incident Notifications

Table 4–29 Incident-Specific Environment Variables

Environment Variable	Description
SEVERITY	Incident Severity, it is translated. Possible Values: Fatal, Critical, Warning, Informational, Clear
SEVERITY_CODE	Code for Severity. Possible values are the FATAL, CRITICAL, WARNING, MINOR_WARNING, INFORMATIONAL, and CLEAR
INCIDENT_REPORTED_TIME	Incident reported time
INCIDENT_ACKNOWLEDGED_BY_OWNER	Set yes, if incident is acknowledged by owner.
INCIDENT_ID	Incident ID
INCIDENT_OWNER	Incident Owner
ASSOC_EVENT_COUNT	The number events associated with this incident.
INCIDENT_STATUS	Incident status. There are two internal fixed resolution status. NEW CLOSED Users can define additional statuses.
ESCALATED	Is Incident escalated
ESCALATED_LEVEL	The escalated level of incident.
PRIORITY	Incident priority. It is the translated priority name. Possible Values: Urgent, Very High, High, Medium, Low, None
PRIOTITY_CODE	Incident priority code It is the internal value defined in EM. PRIORITY_URGENT PRIORITY_VERY_HIGH PRIORITY_HIGH PRIORITY_MEDIUM PRIORITY_LOW PRIORITY_NONE
TICKET_STATUS	Status of external ticket, if it exists.
TICKET_ID	ID of external ticket, if it exists.
LAST_UPDATED_TIME	Incident last update time.

Table 4–29 (Cont.) Incident-Specific Environment Variables

Environment Variable	Description
ADR_INCIDENT_ID	Automatic Diagnostic Reposito ry (ADR) Incident ID: A unique numeric identifier for the ADR Incident. An ADR I ncident is an occurrence of a Problem.
ADR_IMPACT	Impact of the Automatic Diagnostic Repository (ADR) Incident.
ADR_ECID	Execution Context ID (ECID) associated with the associated Automatic Diagnostic Repository (ADR) incident. An ECID i s a globally unique identifier used to tag and track a single call through the Oracle software stack. It is used to correlate problems that could occur across multiple tiers of the stack.
ASSOC_PROBLEM_KEY	Problem key associated with the Automatic Diagnostic Repository (ADR) incident. Problems are critical error s in an Oracle product. The Problem key is a text string that describes the prob lem. It includes an error code and in some cases, other error-specific values.

Table 4–30 lists the associated problem's environment variables, when the incident is associated with a problem.

Table 4–30 Associated Problem Environment Variables for Incidents

Environment Variable	Description
ASSOC_PROBLEM_ACKNOWLEDGED_BY_OWNER	Set to yes, if this problem was acknowledged by owner
ASSOC_PROBLEM_STATUS	Associated Problem Status
ASSOC_PROBLEM_ID	Associated Problem ID
ASSOC_PROBLEM_PRIORITY	Associated Problem priority
ASSOC_PROBLEM_OWNER	Associated Problem Owner if it is existed.
ASSOC_PROBLEM_ESCALATION_LEVEL	Escalation level of the associated Problem has a value between 0 to 5.

4.10.2.5 Environment Variables Specific to Problem Notifications

Table 4–31 Problem-Specific Environment Variables

Environment Variable	Description
SEVERITY	Problem Severity, it is translated.
SEVERITY_CODE	Code for Severity. Possible values are : FATAL, CRITICAL, WARNING, MINOR_WARNING, INFORMATIONAL, and CLEAR
PROBLEM_REPORTED_TIME	Problem reported time.

Table 4–31 (Cont.) Problem-Specific Environment Variables

Environment Variable	Description
PROBLEM_ ACKNOWLEDGED_BY_ OWNER	Set yes, if problem is acknowledged by owner.
PROBLEM_ID	Problem ID
PROBLEM_KEY	Problem Key
PROBLEM_OWNER	Problem Owner
ASSOC_INCIDENT_ COUNT	The number incident associated with this problem..
PROBLEM_STATUS	Incident status. They are STATUS_NEW STATUS_CLOSED Any other user defined status.
ESCALATED	Is Incident escalated. Yes if it is escalated, otherwise No.
ESCALATED_LEVEL	The escalated level of incident.
PRIORITY	Incident priority. It is the translated priority name..
PRIOTITY_CODE	Incident priority code It is the internal value defined in Enterprise Manager. PRIORITY_URGENT PRIORITY_VERY_HIGH PRIORITY_HIGH PRIORITY_MEDIUM PRIORITY_LOW PRIORITY_NONE
LAST_UPDATED_TIME	Last updated time
SR_ID	Oracle Service Request Id, if it exists.
BUD_ID	Oracle Bug ID, if an associated bug exists.

4.10.2.6 Environment Variables Common to Incident and Problem Notifications

An incident or problem may be associated with multiple event sources. An event source can be a Target, a Source Object, or both.

4.10.2.6.1 Environment Variables Related to Event Sources The number of event sources is set by the EVENT_SOURCE_COUNT environment variable. Using the EVENT_ SOURCE_COUNT information, a script can be written to loop through the relevant environment variables to fetch the information about multiple event sources. Environment variables for all event sources are prefixed with EVENT_SOURCE_. Environment variables for source objects are suffixed with SOURCE_<attribute_ name> . For example, EVENT_SOURCE_1_SOURCE_TYPE provides the source object type of first event source. Environment variables for a target are suffixed with TARGET_<attribute_name>. For example, EVENT_SOURCE_1_TARGET_NAME provides the target name of first event source.

The following table lists the environment variables for source object of x-th Event Source.

Table 4–32 Source Object of the x-th Event Source

Environment Variable	Description
EVENT_SOURCE_x_SOURCE_GUID	Source Object GUID.
EVENT_SOURCE_x_SOURCE_TYPE	Source Object Type
EVENT_SOURCE_x_SOURCE_NAME	Source Object Name.
EVENT_SOURCE_x_SOURCE_OWNER	Source Object Owner.
EVENT_SOURCE_x_SOURCE_SUB_TYPE	Source Object Sub-Type.
EVENT_SOURCE_x_SOURCE_URL	Source Object URL to EM console.

Table 4–33 lists the environment variables for a target of *x*th Event Source.

Table 4–33 Target of x-th Event Source

Environment Variable	Description
EVENT_SOURCE_x_TARGET_GUID	Target GUID
EVENT_SOURCE_x_TARGET_NAME	Target name
EVENT_SOURCE_x_TARGET_OWNER	Target Owner
EVENT_SOURCE_x_TARGET_VERSION	Target version
EVENT_SOURCE_x_TARGET_LIFE_CYCLE_STATUS	Target life cycle status
EVENT_SOURCE_x_TARGET_TYPE	Target Type
EVENT_SOURCE_x_HOST_NAME	Target Host Name
EVENT_SOURCE_x_TARGET_URL	Target URL to EM Console.

4.10.3 Passing Information to a PL/SQL Procedure

Passing event, incident, and problem information (payload) to PL/SQL procedures allows you to customize automated responses to these conditions. All three types of notification payloads have a common element: `gc$notif_msg_info`. It provides generic information that applies to all types of notifications. In addition, each of the three payloads have one specific element that provides the payload specific to the given issue type.

gc$notif_event_msg (*payload for event notifications*)

gc$notif_event_msg contains two objects - event payload object and message information object.

Table 4–34 Event Notification Payload

Attribute	Datatype	Additional Information
EVENT_PAYLOAD	gc$notif_event_payload	Event notification payload. See gc$notif_event_payload type definition for detail.
MSG_INFO	gc$notif_msg_info	Notification message. See gc$notif_msg_info definition for detail.

gc$notif_incident_msg (*payload for incident notifications*)

gc$notif_incident_msg type contains two objects - incident payload and message information. This object represents the delivery payload for Incident notification message, contains all data associated with Incident notification, and can be accessed by user's custom PL/SQL procedures.

Table 4–35 Incident Notification Payload

Attribute	Datatype	Additional Information
INCIDENT_PAYLOAD	gc$notif_incident_payload	Incident notification payload. See gc$notif_incident_payload type definition for detail.
MSG_INFO	gc$notif_msg_info	Envelope level notification information. See gc$notif_msg_info type definition for detail.

gc$notif_problem_msg (*payload for problem notifications*)

This object represents the delivery payload for Problem notification message, contains all data associated with problem notification, and can be accessed by a user's custom PL/SQL procedures.

Table 4–36 Problem Notification Payload

Attribute	Datatype	Additional Information
PROBLEM_PAYLOAD	gc$notif_problem_payload	Problem notification payload. See gc$notif_problem_payload type definition for detail.
MSG_INFO	gc$notif_msg_info	Notification message. See gc$notif_msg_info type definition for detail.

gc$notif_msg_info (*common for event/incident/problem payloads*)

This object contains the generic notification information including notification_type, rule set and rule name, etc. for Event, Incident or Problem delivery payload.

Table 4–37 Event, Incident, Problem Common Payload

Attribute	Datatype	Description
NOTIFICATION_TYPE	VARCHAR2(32)	Type of notification, can be one of the following values. GC$NOTIFICATION.NOTIF_NORMAL GC$NOTIFICATION.NOTIF_RETRY GC$NOTIFICATION.NOTIF_REPEAT GC$NOTIFICATION.NOTIF_DURATION GC$NOTIFICATION.NOTIF_CA GC$NOTIFICATION.NOTIF_RCA
REPEAT_COUNT	NUMBER	Repeat notification count
RULESET_NAME	VARCHAR2(256)	Name of the rule set that triggered the notification
RULE_NAME	VARCHAR2(256)	Name of the rule that triggered the notification
RULE_OWNER	VARCAH2(256)	EM User who owns the rule set
MESSAGE	VARCHAR2(4000)	Message about event/incident/problem.
MESSAGE_URL	VARCHAR2(4000)	Link to the Enterprise Manager console page that provides the details of the event/incident/problem.

gc$notif_event_payload (*payload specific to event notifications*)

This object represents the payload specific to event notifications.

Table 4–38 Common Payloads for Events, Incidents, and Problems

Attribute	Datatype	Additional Information
EVENT_INSTANCE_GUID	RAW(16)	Event instance global unique identifier.
EVENT_SEQUENCE_GUID	RAW(16)	Event sequence global unique identifier.
TARGET	gc$notif_target	Related Target Information object. See gc$notif_target type definition for detail.
SOURCE	gc$notif_source	Related Source Information object, that is not a target. See gc$notif_source type definition for detail.
EVENT_ATTRS	gc$notif_event_attr_array	The list of event specified attributes. See gc$notif_event_attr type definition for detail.
CORRECTIVE_ACTION	gc$notif_corrective_action_job	Corrective action information, optionally populated when corrective action job execution has completed.
EVENT_TYPE	VARCHAR2(20)	Event type - example: Metric Alert.
EVENT_NAME	VARCHAR2(512)	Event name.
EVENT_MSG	VARCHAR2(4000)	Event message.
REPORTED_DATE	DATE	Event reported date.
OCCURRENCE_DATE	DATE	Event occurrence date.
SEVERITY	VARCHAR2(128)	Event Severity. It is the translated severity name.

Table 4–38 (Cont.) Common Payloads for Events, Incidents, and Problems

Attribute	Datatype	Additional Information
SEVERITY_CODE	VARCHAR2(32)	Event Severity code. It is the internal severity name used in Enterprise Manager.
ASSOC_INCIDENT	gc$notif_issue_summary	Summary of associated incident. It is populated if the event is associated with an incident. See gc$notif_issue_summary type definition for detail
ACTION_MSG	VARCHAR2(4000)	Message describing the action to take for resolving the event.
RCA_DETAIL	VARCHAR2(4000)	Root cause analysis detail. The size of RCA details output is limited to 4000 characters long.
EVENT_CONTEXT_DATA	gc$notif_event_context_array	Event context data. See gc$notif_event_context type definition for detail.
CATEGORIES	gc$category_string_array	List of categories that the event belongs to. Category is translated based on locale defined in OMS server. Notification system sends up to 10 categories.
CATEGORY_CODES	gc$category_string_array	Codes for the categories. The size of array is up to 10.

gc$notif_incident_payload (*payload specific to incident notifications*)

Contains the incident specific attributes, associated problem and ticket information.

Table 4–39 Incident Notification Payloads

Attribute	Datatype	Additional Information
INCIDENT_ATTRS	gc$notif_issue_attrs	Incident specific attributes. See gc$notif_issue_attrs type definition for detail.
ASSOC_EVENT_COUNT	NUMBER	The total number of events associated with this incident.
TICKET_STATUS	VARCHAR2(64)	The status of external Ticket, if it exists.
TICKET_ID	VARCHAR2(128)	The ID of external Ticket, if it exists.
TICKET_URL	VARCHAR2(4000)	The URL for external Ticket, if it exists.
ASSOC_PROBLEM	gc$notif_issue_summary	Summary of the problem, if it has an associated problem. See gc$notif_issue_summary type definition for detail.

gc$notif_problem_payload (*payload specific to problems*)

Contains problem specific attributes, key, Service Request(SR) and Bug information.

Table 4–40 Problem Payload

Attribute	Datatype	Additional Information
PROBLEM_ATTRS	gc$notif_issue_attrs	Problem specific attributes. See gc$notif_issue_attrs type definition for detail.
PROBLEM_KEY	VARCHAR2(850)	Problem key if it is generated.
ASSOC_INCIDENT_COUNT	NUMBER	Number of incidents associated with this problem.

Table 4–40 (Cont.) Problem Payload

Attribute	Datatype	Additional Information
SR_ID	VARCHAR2(64)	Oracle Service Request Id, if it exists.
SR_URL	VARCHAR2(4000)	URL for Oracle Service Request, if it exists.
BUG_ID	VARCHAR2(64)	Oracle Bug ID, if an associated bug exists.

gc$notif_issue_attrs (*payload common to incidents and problems*)

Provides common details for incident and problem. It contains details such as id, severity, priority, status, categories, acknowledged by owner, and source information with which it is associated.

Table 4–41 Payload Common to Incidents and Problems

Attribute	Datatype	Additional Information
ID	NUMBER(16)	ID of the incident or problem.
SEVERITY	VARCHAR2(128)	Issue Severity. It is the translated.
SEVERITY_CODE	VARCHAR2(32)	Issue Severity Code.The possible values are defined in descending order of severity: GC$EVENT.FATAL GC$EVENT.CRITICAL GC$EVENT.WARNING GC$EVENT.MINOR_WARNING GC$EVENT.INFORMATIONAL GC$EVENT.CLEAR
PRIORITY	VARCHAR2(128)	Issue Priority. It is the translated priority name.
PRIORITY_CODE	VARCHAR2(32)	Issue Priority. It is the internal value defined in EM. The possible values are defined in descending order of priority: GC$EVENT.PRIORITY_URGENT GC$EVENT.PRIORITY_VERY_HIGH GC$EVENT.PRIORITY_HIGH GC$EVENT.PRIORITY_MEDIUM GC$EVENT.PRIORITY_LOW GC$EVENT.PRIORITY_NONE
STATUS	VARCHAR2(32)	Status of Issue. The possible values are GC$EVENT.STATUS_NEW GC$EVENT.STATUS_CLOSED Any other user defined status.
ESCALATION_LEVEL	NUMBER(1)	Escalation level of the issue, has a value between 0 to 5.
OWNER	VARCHAR(256)	Issue Owner. Set to NULL if no owner exists.
ACKNOWLEDGED_BY_OWNER	NUMBER(1)	Set to 1, if this issue was acknowledged by owner.
CREATION_DATE	DATE	Issue creation date.
CLOSED_DATE	DATE	Issue closed date, null if not closed.

Table 4–41 (Cont.) Payload Common to Incidents and Problems

Attribute	Datatype	Additional Information
CATEGORIES	gc$category_string_array	List of categories that the event belongs to. Category is translated based on locale defined in OMS server. Notification system sends up to 10 categories.
CATEGORY_CODES	gc$category_string_array	Codes for the categories. Notification system sends up to 10 category codes.
SOURCE_INFO_ARR	gc$notif_source_info_array	Array of source information associated with this issue. See $gcnotif_source_info type definition for detail.
LAST_MODIFIED_BY	VARCHAR2(256)	Last modified by user.
LAST_UPDATED_DATE	DATE	Last updated date.

gc$notif_issue_summary (*common to incident and problem payloads*)

Represents the associated incident summary in the event payload, or associated problem summary in the incident payload, respectively.

Table 4–42 Payload

Attribute	Datatype	Additional Information
ID	NUMBER	Issue Id, either Incident Id or Problem Id.
SEVERITY	VARCHAR(128)	The severity level of an issue. It is translated severity name.
SEVERITY_CODE	VARCHAR2(32)	Issue Severity Code, has one of the following values. GC$EVENT.FATAL GC$EVENT.CRITICAL GC$EVENT.WARNING GC$EVENT.MINOR_WARNING GC$EVENT.INFORMATIONAL GC$EVENT.CLEAR
PRIORITY	VARCHAR2(128)	Current priority. It is the translated priority name.
PRIORITY_CODE	VARCHAR2(32)	Issue priority code, has one of the following values. GC$EVENT.PRIORITY_URGENT GC$EVENT.PRIORITY_VERY_HIGH GC$EVENT.PRIORITY_HIGH GC$EVENT.PRIORITY_MEDIUM GC$EVENT.PRIORITY_LOW GC$EVENT.PRIORITY_NONE

Table 4–42 (Cont.) Payload

Attribute	Datatype	Additional Information
STATUS	VARCHAR2(64)	Status of issue. The possible values are GC$EVENT.STATUS_NEW GC$EVENT.STATUS_CLOSED GC$EVENT.WIP (work in progress) GC$EVENT.RESOLVED any other user defined status
ESCALATION_LEVEL	VARCHAR2(2)	Issue escalation level range from 0 to 5, default 0.
OWNER	VARCHAR2(256)	Issue Owner. Set to NULL if no owner exists.
ACKNOWLEDGED_BY_OWNER	NUMBER(1)	Set to 1, if this issue was acknowledged by owner.

gc$category_string_array

gc$category_string_array is an array of string containing the categories which event, incident or problem is associated with. The notification system delivers up to 10 categories.

gc$notif_event_context_array

gc$notif_event_context_array provides information about the additional diagnostic data that was captured at event detection time. Note that notification system delivers up to 200 elements from the captured event context. Each element of this array is of the type *gc$notif_event_context*.

gc$notif_event_context: This object represents the detail of event context data which is additional contextual information captured by the source system at the time of event generation that may have diagnostic value. The context for an event should consist of a set of keys and values along with data type (Number or String only).

Table 4–43 Event Context Type

Attribute	Datatype	Additional Information
NAME	VARCHAR2(256)	The event context name.
TYPE	NUMBER(1)	The data type of the value, which is stored (0) - for numeric data (1) - for string data.
VALUE	NUMBER	The numerical value.
STRING_VALUE	VARCHAR2(4000)	The string value.

gc$notif_corrective_action_job

Provides information about the execution of a corrective action job. Note that the corrective actions are supported for metric alert and target availability events only.

Table 4–44 Corrective Action Job-Specific Attributes

Attribute	Datatype	Additional Information
JOB_GUID	RAW(16)	Corrective Action Job global unique identifier.

Table 4–44 (Cont.) Corrective Action Job-Specific Attributes

Attribute	Datatype	Additional Information
JOB_NAME	VARCHAR2(128)	The value will be the name of the Corrective Action. It applies to Metric Alert and Target Availability Events.
JOB_OWNER	VARCHAR2(256)	Corrective action job owner.
JOB_TYPE	VARCHAR2(256)	Corrective action job type.
JOB_STATUS	VARCHAR2(64)	Corrective action job execution status.
JOB_STATUS_CODE	NUMBER	Corrective action job execution status code. It is the internal value defined in Enterprise Manager. For more information on status codes, see Table 4–14, " Corrective Action Status Codes".
JOB_STEP_OUTPUT	VARCHAR2(4000)	The value will be the text output from the Corrective Action execution. This will be truncated to last 4000 characters.
JOB_EXECUTION_GUID	RAW(16)	Corrective Action Job execution global unique identifier.
JOB_STATE_CHANGE_GUID	RAW(16)	Corrective Action Job change global unique identifier.
OCCURRED_DATE	DATE	Corrective action job occurred date.

gc$notif_source_info_array

Provides access to the multiple sources to which an incident or a problem could be related. NOTE: The notification system delivers up to 200 sources associated with an incident or a problem.

```
CREATE OR REPLACE TYPE gc$notif_source_info_array AS VARRAY(200)
OF gc$notif_source_info;
```

gc$notif_source_info

Notification source information which is used for referencing source information containing either target or source, or both.

Table 4–45 Source Information Type

Attribute	Datatype	Additional Information
TARGET	gc$notif_target	It is populated when the event is related to a target. See gc$notif_target type definition for detail.
SOURCE	gc$notif_source	It is populated when the event is related to a (non-target) source. See gc$notif_source type definition for detail.

gc$notif_source

Used for referencing source objects other than a job target.

Table 4–46 Payload

Attribute	Datatype	Additional Information
SOURCE_GUID	RAW(16)	Source's global unique identifier.

Table 4–46 (Cont.) Payload

Attribute	Datatype	Additional Information
SOURCE_TYPE	VARCHAR2(120)	Type of the Source object, e.g., TARGET, JOB, TEMPLATE, etc.
SOURCE_NAME	VARCHAR2(256)	Source Object Name.
SOURCE_OWNER	VARCHAR2(256)	Owner of the Source object.
SOURCE_SUB_TYPE	VARCHAR2(256)	Sub-type of the Source object, for example, within the TARGET these would be the target types like Host, Database etc.
SOURCE_URL	VARCHAR2(4000)	Source's event console URL.

gc$notif_target

Target information object is used for providing target information.

Table 4–47 Target Information

Attribute	Datatype	Additional Information
TARGET_GUID	RAW(16)	Target's global unique identifier.
TARGET_NAME	VARCHAR2(256)	Name of target.
TARGET_OWNER	VARCHAR2(256)	Owner of target.
TARGET_LIFECYCLE_STATUS	VARCHAR2(1024)	Life Cycle Status of the target.
TARGET_VERSION	VARCHAR2(64)	Target Version of the target.
TARGET_TYPE	VARCHAR2(128)	Type of a target.
TARGET_TIMEZONE	VARCHAR2(64)	Target's regional time zone.
HOST_NAME	VARCHAR2(256)	The name of the host on which the target is deployed upon.
TARGET_URL	VARCHAR2(4000)	Target's EM Console URL.
UDTP_ARRAY	gc$notif_udtp_array	The list of user defined target properties. It is populated for events that are associated with a target. It is populated for incidents and problems, when they are associated with a single source (gc$notif_source_info).

gc$notif_udtp_array

Array of *gc$notif_udtp* type with a maximum size of 20.

```
CREATE OR REPLACE TYPE gc$notif_udtp_array AS VARRAY(20) OF
gc$notif_udtp;
```

gc$notif_udtp

Used for referencing User-defined target properties. UDTP should consist of a set of property key names and property values.

Table 4–48 Payload

Attribute	Datatype	Additional Information
NAME	VARCHAR2(64),	The name of property.
VALUE	VARCHAR2(1024)	Property value.

Table 4–48 (Cont.) Payload

Attribute	Datatype	Additional Information
LABEL	VARCHAR(256)	Property label.
NLS_ID	VARCHAR(64)	Property nls id

4.10.3.1 Notification Payload Elements Specific to Event Types

gc$notif_event_attr_array

Array of *gc$notif_event_attr* is used for referencing event-specific attributes. The array has a maximum size of 25. Each element of the array is of type *gc$notif_event_attr* (used for referencing event type-specific attributes).

Table 4–49 Event Attribute Type

Attribute	Datatype	Additional Information
NAME	VARCHAR2(64)	The internal name of event type specific attribute.
VALUE	VARCHAR2(4000)	value.
NLS_VALUE	VARCHAR2(4000)	Translated value for the attribute.

You can use SQL queries to list the deployed event types in your deployment and the payload specific to each. The following SQL can be used to list all internal event type names which are registered in the Enterprise Manager.

```
Select event_class as event_type, upper(name) as env_var_name
from em_event_class_attrs
where notif_order != 0
and event_class is not null
order by event_type, env_var_name;
```

You should convert the attribute name to upper case before using the name for comparison.

There is an attribute variable payload specific to each event type that can be accessed from a *gc$notif_event_attr_array* database type. The following tables list notification attributes for the most critical event types. You should convert the attribute name to uppercase before using the name for comparison.

Table 4–50 Environment variables specific to Metric Alert Event Type

Environment Variable	Description
COLL_NAME	The name of the collection collecting the metric.
KEY_COLUMN_X	Internal name of Key Column X where X is a number between 1 and 7.
KEY_COLUMN_X_VALUE	Value of Key Column X where X is a number between 1 and 7.
KEY_VALUE	Monitored object for the metric corresponding to the Metric Alert event.
METRIC_COLUMN	The name of the metric column
METRIC_DESCRIPTION	Brief description of the metric.
METRIC_GROUP	The name of the metric.
NUM_KEYS	The number of key metric columns in the metric.

Table 4–50 (Cont.) Environment variables specific to Metric Alert Event Type

Environment Variable	Description
SEVERITY_GUID	The GUID of the severity record associated with this metric alert.
VALUE	Value of the metric when the event triggered.

Table 4–51 Environment variables specific to Target Availability Event Type

Environment Variable	Description
AVAIL_SEVERITY	The transition severity (0-6) that resulted in the status of the target to change to the current availability status. Possible Values for AVAIL_SEVERITY ■ 0 (Target Down) ■ 1 (Target Up) ■ 2 (Target Status Error) ■ 3 (Agent Down) ■ 4 (Target Unreachable) ■ 5 (Target Blackout) ■ 6 (Target Status Unknown)
AVAIL_SUB_STATE	The substatus of a target for the current status.
CYCLE_GUID	A unique identifier for a metric alert cycle, which starts from the time the metric alert is initially generated until the time it is clear.
METRIC_GUID	Metric GUID of response metric.
SEVERITY_GUID	The GUID of the severity record associated with this availability status.
TARGET_STATUS	The current availability status of the target.

Table 4–52 Environment variables specific to Job Status Change event type

Environment Variable	Description
EXECUTION_ID	Unique ID of the job execution..
EXECUTION_LOG	The job output of the last step executed.
EXECUTION_STATUS	The internal status of the job execution.
EXEC_STATUS_CODE	Execution status code of job execution. For possible values, see Table 4–16, " Job Status Codes".
STATE_CHANGE_GUID	Unique ID of last status change

Example 4–17 PL/SQL Script: Event Type Payload Elements

```
-- log_table table is created by following DDL to demostrate how to access
-- event notification payload GC$NOTIF_EVENT_MSG.

CREATE TABLE log_table (message VARCHAR2(4000)) ;

-- Define PL/SQL notification method for Events
CREATE OR REPLACE PROCEDURE log_table_notif_proc(s IN GC$NOTIF_EVENT_MSG)
IS
  l_categories gc$category_string_array;
  l_category_codes gc$category_string_array;
  l_attrs gc$notif_event_attr_array;
  l_ca_obj gc$notif_corrective_action_job;
BEGIN
  INSERT INTO log_table VALUES ('notification_type: ' || s.msg_info.notification_
type);
  INSERT INTO log_table VALUES ('repeat_count: ' || s.msg_info.repeat_count);
  INSERT INTO log_table VALUES ('ruleset_name: ' || s.msg_info.ruleset_name);
  INSERT INTO log_table VALUES ('rule_name: ' || s.msg_info.rule_name);
  INSERT INTO log_table VALUES ('rule_owner: ' || s.msg_info.rule_owner);
  INSERT INTO log_table VALUES ('message: ' || s.msg_info.message);
  INSERT INTO log_table VALUES ('message_url: ' || s.msg_info.message_url);
  INSERT INTO log_table VALUES ('event_instance_guid: ' || s.event_payload.event_
instance_guid);
  INSERT INTO log_table VALUES ('event_type: ' || s.event_payload.event_type);
  INSERT INTO log_table VALUES ('event_name: ' || s.event_payload.event_name);
  INSERT INTO log_table VALUES ('event_msg: ' || s.event_payload.event_msg);
  INSERT INTO log_table VALUES ('source_obj_type: ' || s.event_
payload.source.source_type);
  INSERT INTO log_table VALUES ('source_obj_name: ' || s.event_
payload.source.source_name);
  INSERT INTO log_table VALUES ('source_obj_url: ' || s.event_
payload.source.source_url);
  INSERT INTO log_table VALUES ('target_name: ' || s.event_payload.target.target_
name);
  INSERT INTO log_table VALUES ('target_url: ' || s.event_payload.target.target_
url);
  INSERT INTO log_table VALUES ('severity: ' || s.event_payload.severity);
  INSERT INTO log_table VALUES ('severity_code: ' || s.event_payload.severity_
code);
  INSERT INTO log_table VALUES ('event_reported_date: ' || to_char(s.event_
payload.reported_date, 'D MON DD HH24:MI:SS'));

  IF s.event_payload.target.TARGET_LIFECYCLE_STATUS IS NOT NULL
  THEN
    INSERT INTO log_table VALUES ('target lifecycle_status: ' || s.event_
payload.target.TARGET_LIFECYCLE_STATUS);
  END IF;

  -- Following block illustrates the list of category codes to which the event
  -- belongs.

  l_category_codes := s.event_payload.category_codes;
  IF l_categories IS NOT NULL
  THEN
    FOR c IN 1..l_category_codes.COUNT
    LOOP
      INSERT INTO log_table VALUES ('category_code ' || c || ' - ' || l_category_
codes(c));
    END LOOP;
  END IF;

  --
  -- Each event type has a specific set of attributes modeled. Examples of
  -- event types include metric_alert, target_availability, job_status_change.
  -- Following block illustrates how to access the attributes for job_status
change
  -- event type
  --
  IF s.event_payload.event_type = 'job_staus_chage'
  THEN
    l_attrs := s.event_payload.event_attrs;
    IF l_attrs IS NOT NULL
    THEN
      FOR c IN 1..l_attrs.COUNT
      LOOP
        INSERT INTO log_table VALUES ('EV.ATTR name=' || l_attrs(c).name || '
value=' || l_attrs(c).value || ' nls_value=' || l_attrs(c).nls_value);
      END LOOP;
    END IF;
  END IF;

  -- Following block illustrates how to access corrective action job's attributes
  IF s.msg_info.notification_type = GC$NOTIFICATION.NOTIF_CA AND s.event_
payload.corrective_action IS NOT NULL
  THEN
    l_ca_obj := s.event_payload.corrective_action;
    INSERT INTO log_table VALUES ('CA JOB_GUID: ' || l_ca_obj.JOB_GUID);
    INSERT INTO log_table VALUES ('CA JOB_NAME: ' || l_ca_obj.JOB_NAME);
    INSERT INTO log_table VALUES ('CA JOB_OWNER: ' || l_ca_obj.JOB_OWNER);
    INSERT INTO log_table VALUES ('CA JOB_TYPE: ' || l_ca_obj.JOB_TYPE);
    INSERT INTO log_table VALUES ('CA JOB_STATUS: ' || l_ca_obj.JOB_STATUS);
    INSERT INTO log_table VALUES ('CA JOB_STATUS_CODE: ' || l_ca_obj.JOB_STATUS_
CODE);
    INSERT INTO log_table VALUES ('CA JOB_STEP_OUTPUT: ' || l_ca_obj.JOB_STEP_
OUTPUT);
    INSERT INTO log_table VALUES ('CA JOB_EXECUTION_GUID: ' || l_ca_obj.JOB_
EXECUTION_GUID);
    INSERT INTO log_table VALUES ('CA JOB_STATE_CHANGE_GUID: ' || l_ca_obj.JOB_
STATE_CHANGE_GUID);
    INSERT INTO log_table VALUES ('CA OCCURRED_DATE: ' || l_ca_obj.OCCURRED_DATE);
  END IF;

COMMIT ;
END ;
/
```

4.10.4 Troubleshooting Notifications

To function properly, the notification system relies on various components of Enterprise Manager and your IT infrastructure. For this reason, there can be many causes of notification failure. The following guidelines and suggestions can help you isolate potential problems with the notification system.

4.10.4.1 General Setup

The first step in diagnosing notification issues is to ensure that you have properly configured and defined your notification environment.

OS Command, PL/SQL and SNMP Trap Notifications

Make sure all OS Command, PLSQL and SNMP Trap Notification Methods are valid by clicking the Test button. This will send a test notification and show any problems the OMS has in contacting the method. Make sure that your method was called, for example, if the OS Command notification is supposed to write information to a log file, check that it has written information to its log file.

E-mail Notifications

- Make sure an e-mail gateway is set up under the Notification Methods page of Setup. The Sender's e-mail address should be valid. Clicking the Test button will send an e-mail to the Sender's e-mail address. Make sure this e-mail is received. Note that the Test button ignores any Notification Schedule.

- Make sure an e-mail address is set up. Clicking the Test button will send an e-mail to specified address and you should make sure this e-mail is received. Note that the Test button ignores any Notification Schedule.
- Make sure an e-mail schedule is defined. No e-mails will be sent unless a Notification Schedule has been defined.
- Make sure a incident rule is defined that matches the states you are interested and make sure e-mail and notification methods are assigned to the rule.

4.10.4.2 Notification System Errors

For any alerts involving problems with notifications, check the following for notification errors.

- Any serious errors in the Notification System are logged as system errors in the MGMT_SYSTEM_ERROR_LOG table. From the **Setup** menu, select **Management Services and Repository** to view these errors.
- Check for any delivery errors. You can view them from Incident Manager. From the **Enterprise** menu, select **Monitoring**, then select **Incident Manager**. The details will give the reason why the notification was not delivered.

4.10.4.3 Notification System Trace Messages

The Notification System can produce trace messages in sysman/log/emoms.trc file.

Tracing is configured by setting the *log4j.category.oracle.sysman.em.notification* property flag using the `emctl set property` command. You can set the trace level to INFO, WARN, DEBUG. For example,

```
emctl set property -name log4j.category.oracle.sysman.em.notification -value
DEBUG -module logging
```

Note: The system will prompt you for the SYSMAN password.

Trace messages contain the string "em.notification". If you are working in a UNIX environment, you can search for messages in the emoms.trc and emoms_pbs.trc files using the `grep` command. For example,

```
grep em.notification emoms.trc emoms_pbs.trc
```

What to look for in the trace file.

The following entries in the emoms.trc file are relevant to notifications.

Normal Startup Messages

When the OMS starts, you should see these types of messages.

```
2011-08-17 13:50:29,458 [EventInitializer] INFO  em.notification init.167 - Short
format maximum length is 155
2011-08-17 13:50:29,460 [EventInitializer] INFO  em.notification init.185 - Short
format is set to both subject and body
2011-08-17 13:50:29,460 [EventInitializer] INFO  em.notification init.194 -
Content-Transfer-Encoding is 8-bit
2011-08-17 13:50:29,460 [EventInitializer] DEBUG em.notification
registerAdminMsgCallBack.272 - Registering notification system message call back
2011-08-17 13:50:29,461 [EventInitializer] DEBUG em.notification
registerAdminMsgCallBack.276 - Notification system message callback is registered
```

```
successfully
2011-08-17 13:50:29,713 [EventInitializer] DEBUG em.notification
upgradeEmailTemplates.2629 - Enter upgradeEmailTemplates
2011-08-17 13:50:29,735 [EventInitializer] INFO  em.notification
upgradeEmailTemplates.2687 - Email template upgrade is not required since no
customized templates exist.
2011-08-17 13:49:28,739 [EventCoordinator] INFO  events.EventCoordinator logp.251
- Creating event worker thread pool: min = 4 max = 15
2011-08-17 13:49:28,791 [[STANDBY] ExecuteThread: '2' for queue:
'weblogic.kernel.Default (self-tuning)'] INFO emdrep.pingHBRecorder
initReversePingThreadPool.937 - Creating thread pool for reverse ping : min = 10
max = 50
2011-08-17 13:49:28,797 [[STANDBY] ExecuteThread: '2' for queue:
'weblogic.kernel.Default (self-tuning)'] DEBUG emdrep.HostPingCoordinator logp.251
- Creating thread pool of worker thread  for host ping: min = 1 max = 10
2011-08-17 13:49:28,799 [[STANDBY] ExecuteThread: '2' for queue:
'weblogic.kernel.Default (self-tuning)'] DEBUG emdrep.HostPingCoordinator logp.251
- Creating thread pool for output of worker's  output for host ping: min = 2 max =
20
2011-08-17 13:49:30,327 [ConnectorCoordinator] INFO
connector.ConnectorPoolManager logp.251 - Creating Event thread pool: min = 3 max
= 10
2011-08-17 13:51:48,152 [NotificationMgrThread] INFO  notification.pbs logp.251 -
Creating thread pool: min = 6 max = 24
2011-08-17 13:51:48,152 [NotificationMgrThread] INFO  em.rca logp.251 - Creating
RCA thread pool: min = 3 max = 20
```

Notification Delivery Messages

```
2006-11-08 03:18:45,387 [NotificationMgrThread] INFO  em.notification run.682 -
Notification ready on EMAIL1

2006-11-08 03:18:46,006 [DeliveryThread-EMAIL1] INFO  em.notification run.114 -
Deliver to SYSMAN/admin@myco.com

2006-11-08 03:18:47,006 [DeliveryThread-EMAIL1] INFO  em.notification run.227 -
Notification handled for SYSMAN/admin@myco.com
```

Notification System Error Messages

```
2011-08-17 14:02:23,905 [NotificationMgrThread] DEBUG notification.pbs logp.251 -
Notification ready on EMAIL1
2011-08-17 14:02:23,911 [NotificationMgrThread] DEBUG notification.pbs logp.251 -
Notification ready on PLSQL4
2011-08-17 14:02:23,915 [NotificationMgrThread] DEBUG notification.pbs logp.251 -
Notification ready on OSCMD14
2011-08-17 14:02:19,057 [DeliveryThread-EMAIL1] INFO  notification.pbs logp.251 -
Deliver to To: my.admin@myco.com; issue type: 1; notification type: 1
2011-08-17 14:02:19,120 [DeliveryThread-OSCMD14] INFO  notification.pbs logp.251 -
Deliver to SYSMAN, OSCMD, 8; issue type: 1; notification type: 1
2011-08-17 14:02:19,346 [DeliveryThread-PLSQL4] INFO  notification.pbs logp.251 -
Deliver to SYSMAN, LOG_JOB_STATUS_CHANGE, 9; issue type: 1; notification type: 1
2011-08-17 14:02:19,977 [DeliveryThread-PLSQL4] DEBUG notification.pbs logp.251 -
Notification handled for SYSMAN, LOG_JOB_STATUS_CHANGE, 9
2011-08-17 14:02:20,464 [DeliveryThread-EMAIL1] DEBUG notification.pbs logp.251 -
Notification handled for To: my.admin@myco.com
2011-08-17 14:02:20,921 [DeliveryThread-OSCMD14] DEBUG notification.pbs logp.251 -
Notification handled for SYSMAN, OSCMD, 8
```

4.10.4.4 E-mail Errors

The SMTP gateway is not set up correctly:

```
Failed to send e-mail to my.admin@myco.com: For e-mail notifications to be sent,
your Super Administrator must configure an Outgoing Mail (SMTP) Server within
Enterprise Manager. (SYSMAN, myrule)
```

Invalid host name:

```
Failed to connect to gateway: badhost.oracle.com: Sending failed;
nested exception is:
javax.mail.MessagingException: Unknown SMTP host: badhost.example.com;
```

Invalid e-mail address:

```
Failed to connect to gateway: rgmemeasmtp.mycorp.com: Sending failed;
nested exception is:
javax.mail.MessagingException: 550 5.7.1 <smpemailtest_ie@example.com>... Access
denied
```

Always use the Test button to make sure the e-mail gateway configuration is valid. Check that an e-mail is received at the sender's e-mail address

4.10.4.5 OS Command Errors

When attempting to execute an OS command or script, the following errors may occur. Use the Test button to make sure OS Command configuration is valid. If there are any errors, they will appear in the console.

Invalid path or no read permissions on file:

```
Could not find /bin/myscript (machineb10.oracle.com_Management_Service) (SYSMAN,
myrule )
```

No execute permission on executable:

```
Error calling /bin/myscript: java.io.IOException: /bin/myscript: cannot execute
(machineb10.oracle.com_Management_Service) (SYSMAN, myrule )
```

Timeout because OS Command ran too long:

```
Timeout occurred running /bin/myscript (machineb10.oracle.com_Management_Service)
(SYSMAN, myrule )
```

Any errors such as out of memory or too many processes running on OMS machine will be logged as appropriate.

Always use the Test button to make sure OS Command configuration is valid.

4.10.4.6 SNMP Trap Errors

Use the Test button to make sure SNMP Trap configuration is valid.

The OMS will not report an error if the SNMP trap cannot reach the third party SNMP console as this is sent via UDP. If the SNMP trap encounters problems when trying to reach the third party SNMP console, possible SNMP trap problems include: invalid host name, port, community for a machine running an SNMP Console or a network issue such as a firewall problem.

Other possible SNMP trap problems include: invalid host name, port, or community for a machine running an SNMP Console.

4.10.4.7 PL/SQL Errors

When attempting to execute an PL/SQL procedure, the following errors may occur. Use the Test button to make sure the procedure is valid. If there are any errors, they will appear in the console.

Procedure name is invalid or is not fully qualified. Example: SCOTT.PKG.PROC

```
Error calling PL/SQL procedure plsql_proc: ORA-06576: not a valid function or
procedure name (SYSMAN, myrule)
```

Procedure is not the correct signature. Example: `PROCEDURE event_proc(s IN GC$NOTIF_EVENT_MSG)`

```
Error calling PL/SQL procedure plsql_proc: ORA-06553: PLS-306: wrong number or
types of arguments in call to 'PLSQL_PROC' (SYSMAN, myrule)
```

Procedure has bug and is raising an exception.

```
Error calling PL/SQL procedure plsql_proc: ORA-06531: Reference to uninitialized
collection (SYSMAN, myrule)
```

Care should be taken to avoid leaking cursors in your PL/SQL. Any exception due to this condition will result in delivery failure with the message being displayed in the Details section of the alert in the Cloud Control console.

Always use the Test button to make sure the PL/SQL configuration is valid.

5 Using Blackouts

Blackouts allow Enterprise Manager administrators to suspend all data collection activity on one or more monitored targets. The primary reason for blacking out targets is to allow Enterprise Manager administrators to perform scheduled maintenance on those targets.

A blackout can be defined for individual target(s), a group of multiple targets that reside on different hosts, or for all targets on a host. The blackout can be scheduled to run immediately or in the future, and to run indefinitely or stop after a specific duration. Blackouts can be created on an as-needed basis, or scheduled to run at regular intervals. If, during the maintenance period, the administrator discovers that he needs more (or less) time to complete his maintenance tasks, he can easily extend (or stop) the blackout that is currently in effect.

Blackout functionality is available from both the Enterprise Manager console as well as via the Enterprise Manager command-line interface (EMCLI). EMCLI is often useful for administrators who would like to incorporate the blacking out of a target within their maintenance scripts.

5.1 Working with Blackouts

Blackouts allow you to collect accurate monitoring data. For example, you can stop data collections during periods where a managed target is undergoing routine maintenance, such as a database backup or hardware upgrade. 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.

Blackout Access

Enterprise Manager administrators who have at least Blackout Target privileges on all Selected Targets in a blackout will be able to create, edit, stop, or delete the blackout.

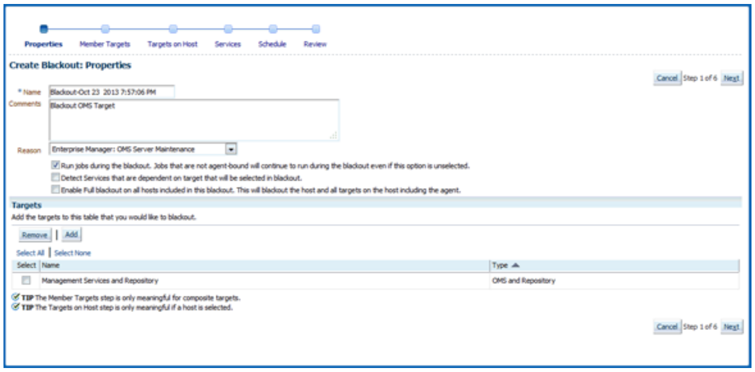
In case an administrator has at least Blackout Target privileges on all Selected Targets (targets directly added to the blackout), but does not have Blackout Target privileges on some or all of the Dependent Targets, then that administrator will be able to edit, stop, or delete the blackout. For more information on Blackout access, see About Blackouts Best Effort.

5.1.1 Creating a Blackout

To create a blackout:

1. From the **Enterprise** menu, select **Monitoring**, then select **Blackouts**.

2. From the table, click **Create**. Enterprise Manager displays a wizard page to guide you through the steps required to create a blackout. Click Help from any wizard page for more information on specific steps.



Create Blackout: Properties

* Name: Blackout-Oct 23 2013 7:57:06 PM

Comments: Blackout OMS Target

Reason: Enterprise Manager: OMS Server Maintenance

☑ Run jobs during the blackout. Jobs that are not agent-bound will continue to run during the blackout even if this option is unselected.

□ Detect Services that are dependent on target that will be selected in blackout.

□ Enable Full blackout on all hosts included in this blackout. This will blackout the host and all targets on the host including the agent.

Targets

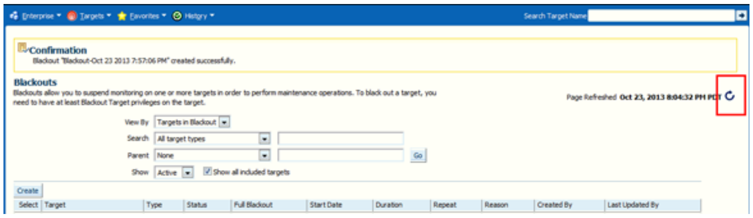
Add the targets to this table that you would like to blackout.

Select	Name	Type
□	Management Services and Repository	OMS and Repository

TIP The Member Targets step is only meaningful for composite targets.

TIP The Targets on Host step is only meaningful if a host is selected.

3. To display the latest blackout information, click the refresh icon.



Confirmation

Blackout "Blackout-Oct 23 2013 7:57:06 PM" created successfully.

Blackouts

Blackouts allow you to suspend monitoring on one or more targets in order to perform maintenance operations. To black out a target, you need to have at least Blackout Target privileges on the target.

Page Refreshed **Oct 23, 2013 8:04:32 PM PDT**

View By: Targets in Blackout

Search: All target types

Parent: None

Show: Active ☑ Show all included targets

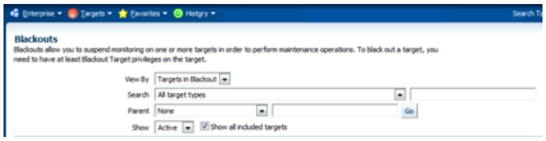
Select	Target	Type	Status	Full Blackout	Start Date	Duration	Repeat	Reason	Created By	Last Updated By

5.1.2 Editing a Blackout

To edit a blackout:

1. From the **Enterprise** menu, select **Monitoring**, then select **Blackouts**.

2. If necessary, use the Search and display options to show the blackouts you want to change in the blackouts table.



Blackouts

Blackouts allow you to suspend monitoring on one or more targets in order to perform maintenance operations. To black out a target, you need to have at least Blackout Target privileges on the target.

View By: Targets in Blackout

Search: All target types

Parent: None

Show: Active ☑ Show all included targets

3. Select the desired blackout and click **Edit**.

> **Note:** Enterprise Manager also allows you to edit blackouts after they have already started.

5.1.3 Viewing Blackouts

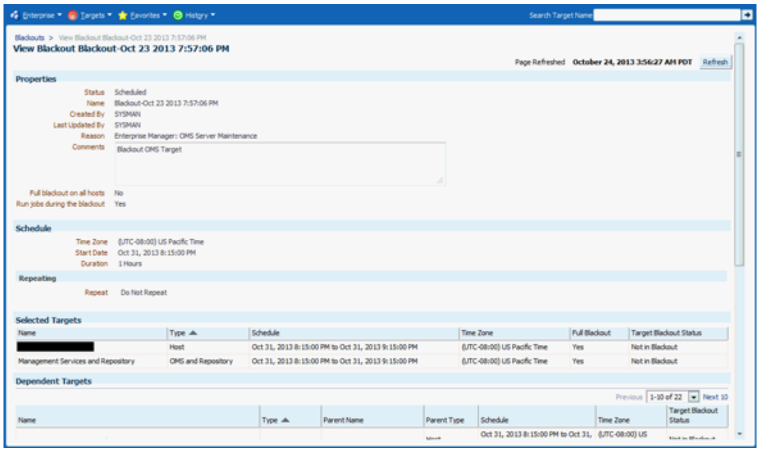
To view information and current status of a blackout:

1. From the **Enterprise** menu, select **Monitoring**, then select **Blackouts**.

2. If necessary, you can use the Search and display options to show the blackouts you want to view in the blackouts table.

3. Select the desired blackout and click View. Alternatively, if you are in View By - 'Targets in Blackout', then you can click on blackout status in the table to access the

View Blackout page. If you are in View By - 'Blackout Name', then you can click on a blackout name in the table to access the View Blackout page.



View Blackout Blackout-Oct 23 2013 7:57:06 PM

Page Refreshed **October 24, 2013 3:56:27 AM PDT**

Properties

Status	Scheduled
Name	Blackout-Oct 23 2013 7:57:06 PM
Created By	SYSMAN
Last Updated By	SYSMAN
Reason	Enterprise Manager: OMS Server Maintenance
Comments	Blackout OMS Target
Full blackout on all hosts	No
Run jobs during the blackout	Yes

Schedule

Time Zone	(UTC-08:00) US Pacific Time
Start Date	Oct 31, 2013 8:15:00 PM
Duration	1 Hours

Repeating

Repeat	Do Not Repeat

Selected Targets

Name	Type ▲	Schedule	Time Zone	Full Blackout	Target Blackout Status
[redacted]	Host	Oct 31, 2013 8:15:00 PM to Oct 31, 2013 9:15:00 PM	(UTC-08:00) US Pacific Time	Yes	Not in Blackout
Management Services and Repository	OMS and Repository	Oct 31, 2013 8:15:00 PM to Oct 31, 2013 9:15:00 PM	(UTC-08:00) US Pacific Time	Yes	Not in Blackout

Dependent Targets

Previous 1-10 of 22 ▾ Next 10

Name	Type ▲	Parent Name	Parent Type	Schedule	Time Zone	Target Blackout Status
			Host	Oct 31, 2013 8:15:00 PM to Oct 31,	(UTC-08:00) US	Not in Blackout

You can bookmark the View Blackout page as a quick way to monitor the status of a particular blackout. Click **Refresh** to display the most recent blackout information.

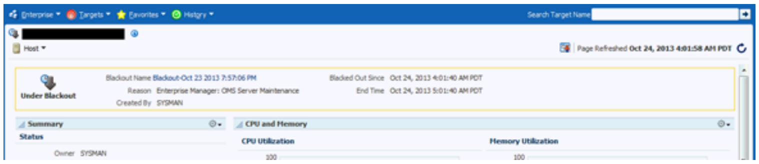
5.1.3.1 Viewing Blackouts on Targets Monitored by a Specific Management Agent

To view the blackouts configured for the targets monitored by the Management Agent:

1. From the Cloud Control home page, click **Targets** and then **All Targets**. In the All Targets page, locate the Management Agent in the list of targets. Click on the Management Agent's name. This brings you to the Management Agent's home page.
2. The list of targets monitored by the Management Agent are listed in the Monitored Targets section.
3. For each of target in the list:
   a. Click the target name. This brings you to the target's home page.
   b. From the <Target> menu, select **Monitoring** and then click **Blackouts**. This allows you to check any currently running blackouts or blackouts that are scheduled in the future for this target.

5.1.3.2 Viewing Blackouts from Target Home Pages

For most target types, you can view a blackout information from the target home page for any target currently under blackout. A blackout message provides pertinent blackout status information for that target.



[redacted]

Page Refreshed **Oct 24, 2013 4:01:58 AM PDT**

Under Blackout

Blackout Name	Blackout-Oct 23 2013 7:57:06 PM	Blacked Out Since	Oct 24, 2013 4:01:40 AM PDT
Reason	Enterprise Manager: OMS Server Maintenance	End Time	Oct 24, 2013 5:01:40 AM PDT
Created By	SYSMAN		

Status

Owner SYSMAN

5.1.3.3 Viewing Blackouts from Groups and Systems Target Administration Pages

For Groups and Systems, you can view blackout information about the number of active/scheduled blackouts on a group/system and its member targets.

5.1.4 Purging Blackouts that have Ended

When managing a large number of targets, the number of completed blackouts, or those blackouts that have been ended by an administrator can become quite large. Removing these ended blackouts facilitates better search an display for current blackouts.

To purge ended blackouts from Enterprise Manager:

1. From the **Enterprise** menu, select **Monitoring**, then select **Blackouts**.
2. Use the search criteria to filter for the desired targets.
3. From the **Show** drop-down menu, select **History**.
4. In the table, select the ended blackouts you want to remove and click **Delete**. The purge confirmation page appears.
5. Click **Yes** to complete the purge process.

5.2 Controlling Blackouts Using the Command Line Utility

You can control blackouts from the Oracle Enterprise Manager 12c Cloud Control Console or from the Enterprise Manager command line utility (`emctl`). However, if you are controlling target blackouts from the command line, you should not attempt to control the same blackouts from the Cloud Control Console. Similarly, if you are controlling target blackouts from the Cloud Control Console, do not attempt to control those blackouts from the command line.

From the command line, you can perform the following blackout functions:

- Starting Immediate Blackouts
- Stopping Immediate Blackouts
- Checking the Status of Immediate Blackouts

Note: When you start a blackout from the command line, any Enterprise Manager jobs scheduled to run against the blacked out targets will still run. If you use the Cloud Control Console to control blackouts, you can optionally prevent jobs from running against blacked out targets.

To use the Enterprise Manager command-line utility to control blackouts:

1. Change directory to the `AGENT_HOME/bin` directory (UNIX) or the `AGENT_INSTANCE_HOME\bin` directory (Windows).
2. Enter the appropriate command as described in Table 5–1, " Summary of Blackout Commands".

Note: When you start a blackout, you must identify the target or targets affected by the blackout. To obtain the correct target name and target type for a target, see "Listing the Targets on a Managed Host" on page 20-13.

Table 5–1 Summary of Blackout Commands

Blackout Action	Command
Set an immediate blackout on a particular target or list of targets	`emctl start blackout <Blackoutname> [<Target_name>[:<Target_Type>]].... [-d <Duration>]` Be sure to use a unique name for the blackout so you can refer to it later when you want to stop or check the status of the blackout. The `-d` option is used to specify the duration of the blackout. Duration is specified in `[days] hh:mm where:` ■ days indicates number of days, which is optional ■ hh indicates number of hours ■ mm indicates number of minutes If you do not specify a target or list of targets, Enterprise Manager will blackout the local host target. All monitored targets on the host are not blacked out unless a list is specified or you use the `-nodelevel` argument. If two targets of different target types share the same name, you must identify the target with its target type.
Stop an immediate blackout	`emctl stop blackout <Blackoutname>`
Set an immediate blackout for all targets on a host	`emctl start blackout <Blackoutname> [-nodeLevel] [-d <Duration>]` The `-nodeLevel` option is used to specify a blackout for all the targets on the host; in other words, all the targets that the Management Agent is monitoring, including the Management Agent host itself. The `-nodeLevel` option must follow the blackout name. If you specify any targets after the `-nodeLevel` option, the list is ignored.
Check the status of a blackout	emctl status blackout `[<Target_name>[:<Target_Type>]]....`

Use the following examples to learn more about controlling blackouts from the Enterprise Manager command line:

- To start a blackout called "bk1" for databases "db1" and "db2," and for Oracle Listener "ldb2," enter the following command:

  ```
  $PROMPT> emctl start blackout bk1 db1 db2 ldb2:oracle_listener -d 5 02:30
  ```

  The blackout starts immediately and will last for 5 days 2 hours and 30 minutes.

- To check the status of all the blackouts on a managed host:

  ```
  $PROMPT> emctl status blackout
  ```

- To stop blackout "bk2" immediately:

  ```
  $PROMPT> emctl stop blackout bk2
  ```

- To start an immediate blackout called "bk3" for all targets on the host:

  ```
  $PROMPT> emctl start blackout bk3 -nodeLevel
  ```

- To start an immediate blackout called "bk3" for database "db1" for 30 minutes:

  ```
  $PROMPT> emctl start blackout bk3 db1 -d 30
  ```

- To start an immediate blackout called "bk3" for database "db2" for five hours:

```
$PROMPT> emctl start blackout bk db2 -d 5:00
```

5.3 About Blackouts Best Effort

The Blackouts Best Effort feature allows you to create blackouts on aggregate targets, such as groups or systems, for which you do not have Blackout Target (or Higher) privileges on all members of the aggregate target.

Here, an Enterprise Manager administrator has Blackout Target privilege on an aggregate target but do not have OPERATOR privilege on its member/associated targets. You should ideally create a Full Blackout on this aggregate target. When defining the blackout, you are allowed to select any member target, even those member targets for which you have no Blackout Target privileges.

When the blackout actually starts, Enterprise Manager checks privileges on each member target and only blackout those on which you have Blackout Target(or Higher) privileges. This automated privilege check and target blackout selection is Enterprise Manager's "best effort" at blacking out the aggregate target.

5.3.1 When to Use Blackout Best Effort

The Blackout Best Effort functionality is targeted towards the creation of blackouts on targets of any aggregate type, such as Group, Hosts, Application Servers, Web Applications, Redundancy Groups, or Systems.

All targets the blackout creator has Blackout Target (or higher) privilege on will be displayed in the first step of Create/Edit Blackout Wizard. Once the blackout creator selects an aggregate type of target to be included in the Blackout Definition, this Blackout is "Full Blackout" by default.

The creator has the option of choosing the Blackout to run on “All Current” or “Selected” Targets, by selecting the appropriate values from the List box. Only when the "Full Blackout" option is chosen, will Blackout Best Effort affect targets for which the creator does not have Blackout Target (or higher) privileges.

Example Use Case

Consider 3 targets T1,T2 and T3 (all databases). A Group G1 contains all these 3 targets.

User U1 has OPERATOR privilege on T1,T2 and G1. User U1 has VIEW privilege on T3.

User U1 creates a scheduled full blackout on target G1. Scheduled implies that the blackout will start at a later point in time.

At the time of blackout creation, the tip text *Needs Blackout Target privilege, see Tip below the table* would be shown beside target T3.

When this blackout starts, if by that time User U1 has been granted OPERATOR privileges on target T3, then target T3 would also be under blackout. Otherwise only targets T1, T2 and G1 will be under blackout.

6 Managing Groups

This chapter introduces the concept of group management and contains the following sections:

- Introduction to Groups
- Managing Groups
- Using Out-of-Box Reports

6.1 Introduction to Groups

Groups are an efficient way to logically organize, manage, and monitor the targets in your global environments. Each group has its own group home page. The group home page shows the most important information for the group and enables you to drill down for more information. The home page shows the overall status of the group and other information such as current availability, incidents, and patch recommendations for members of the group.

Group Management Tasks

You can use Enterprise Manager to perform the following group management functions:

- Edit the configuration of a selected group, remove groups, and, in the case of an Administration Group, associate or disassociate a Template Collection.
- View the status and health of the group from the System Dashboard
- Drill down from a specific group to collectively monitor and manage its member targets.
- View a roll-up of member statuses and open incidents for members of the group.
- Apply blackouts to all targets in a group.
- Run jobs against a group
- Run a report
- Apply monitoring templates
- Associate compliance standards

In addition to creating groups, you can also create specific types of groups, such as redundancy groups, privilege propagating groups, and dynamic groups. The following sections explain the different types of groups.

6.1.1 Overview of Groups

Groups enable you to collectively monitor and administer many targets as a single logical unit. For example, you can define a group to contain all the databases serving an enterprise application, and define another group to contain all the hosts in a host farm. You can then use these groups to perform administrative operations. To create a group, you can manually select and add the members of the group. If you add an aggregate target, such as a Cluster Database, all of its member targets are automatically added to the group.

A group can include targets of the same type, such as all your production databases, or it could include all the targets on a host which would be comprised of different target types. You can nest static groups inside each other. In the target selector when you are selecting group members, choose Group as the target type, or choose a parent group as part of the process of creating a group.

If a system target is added to a group, it automatically pulls in its member targets. This could be the case of a regular group where a system such as WebLogic Server is added and also pulls in its members, or in a dynamic group where you specify a Target type to be an Oracle WebLogic Server and it also pulls in members of the WebLogic Server even though it does not match the dynamic group criteria. In this scenario, the group operations (for example, runnning jobs, blackouts, and so on) apply to all members of the group.

After you configure a group, you can perform various administrative operations, such as:

- View a summary status of the targets within the group.
- View a roll-up of member statuses and open incidents for members of the group.
- View a summary of critical patch advisories.
- View configuration changes during the past 7 days.
- Create jobs and view the status of job executions.
- Create blackouts and view the status of current blackouts.

6.1.2 Overview of Privilege Propagating Groups

Privilege propagating groups enable administrators to propagate privileges to members of a group. You can grant a privilege on a group once to an administrator or a role and have that same privilege automatically propagate to any new member of the group. For example, granting *operator* privilege on a privilege propagating group to an Administrator grants him the *operator* privilege on its member targets and also to any members that will be added in the future. Privilege propagating groups can contain individual targets or other privilege propagating groups. Any aggregate that you add to a privilege propagating group must also be privilege propagating as well. For example, any group that you add to a privilege propagating group must also be privilege propagating.

Privileges on the group can be granted to an Enterprise Manager administrator or a role. Use a role if the privileges you want to grant are to be granted to a group of Enterprise Manager administrators.

For example, suppose you create a privilege propagating group and grant a privilege to a role which is then granted to administrators. If new targets are later added to the privilege propagating group, then the administrators receive the privileges on the target automatically. Additionally, when a new administrator is hired, you only need to grant the role to the administrator for the administrator to receive all the privileges on the targets automatically.

6.1.3 Overview of Dynamic Groups

The membership management for groups is typically manual or static in nature. Manually managing memberships works well for small deployments but not necessarily in large, dynamic environments where new targets come into the system frequently. Groups whose members are added frequently would be easier to maintain if they were to be defined by membership criteria instead of adding targets directly into the group. When the membership criteria is defined once, Enterprise Manager will automatically add targets.

A dynamic group is a group whose membership is determined by membership criteria. The owner of a dynamic group specifies the membership criteria during dynamic group creation (or modification) and membership in the group is determined solely by the criteria specified. Membership in a dynamic group cannot be modified directly because targets cannot be directly added to a dynamic group. Enterprise Manager automatically adds targets that match membership criteria when a dynamic group is created. It also updates group membership as new targets are added or target properties are changed and the target matches the group’s membership criteria.

It is important to note that static groups can contain dynamic groups as members but not the other way around. You cannot include a static group as a member of a dynamic group.

Use the Define Membership Criteria function of Dynamic Groups to define the criteria for group membership. Once you have defined criteria, the targets selected by the criteria will be displayed in a read-only table in the Members region of the Groups page. Since dynamic groups are defined by criteria, you can intentionally or unintentionally define criteria that could result in very large groups.

The following requirements apply to dynamic groups:

- Dynamic groups cannot contain static groups, other dynamic groups, or administration groups.
- Administration groups cannot contain dynamic groups, however, a static group can contain dynamic groups as a member.
- OR-based criteria is not supported. All criteria selected on the criteria page are AND-based.
- Supported properties are limited to global properties plus other attributes specifically supported for administration groups such as Version, Platform, Target Name and Type, and so on. Specifically user-defined properties and other instance properties, plus config data elements are not supported as criteria.
- The View Any Target and Add Any Target privileges are required to create a dynamic group.
- The Full Any Target, Add Any Target, and Create Privilege Propagating Group privileges are required to create a privilege-propagating dynamic group.

6.1.4 Overview of Administration Groups

Administration Groups greatly simplify the process of setting up targets for management in Enterprise Manager by automating the application of management settings such as monitoring settings or compliance standards. Typically, these settings are manually applied to individual target, or perhaps semi-automatically using custom scripts. However, by defining Administration Groups, Enterprise Manager uses specific target properties to direct the target to the appropriate Administration Group and then automatically apply the requisite monitoring and management settings. This level of automation simplifies the target setup process and also enables a datacenter to easily scale as new targets are added to Enterprise Manager for management.

Administration groups are a special type of group used to fully automate application of monitoring and other management settings upon joining the group. When a target is added to the group, Enterprise Manager applies these settings using a Template Collection consisting of Monitoring Templates, compliance standards, and cloud policies. This completely eliminates the need for administrator intervention.

To watch Part 1 of a video about using administrative groups and template collections, click here.

To watch Part 2 of the video about using administrative groups and template collections, click here.

6.1.5 Choosing Which Type of Group To Use

There are two major types of groups you can choose to manage targets: Static Groups/ Dynamic groups, which can be one or more groups that you define, and Administration Groups for automating monitoring setup using templates.

You should carefully consider the purpose of your group and the function it serves before determining which type of group to use.

The following table diagrams when you should use Administration Groups or Dynamic Groups.

Table 6–1 When To Use Administration Groups vs. Dynamic Groups

Type of Group	Main Purpose	Membership Based on Criteria	Additional Membership Requirements	Privilege Propagating
Administration Group	Auto-apply monitoring templates	Yes, based on target properties	Target can belong to at most one administration group	Yes (always)
Dynamic Group	Perform any group operation.	Yes, based on target properties	Target can belong to one or more groups	User-specified option

The main purpose of an Administration Group is to automate the application of management settings, such as monitoring settings or compliance standards. When a target is added to the group, Enterprise Manager automatically applies these settings using templates to eliminate the need for administrator action.

Dynamic groups, on the other hand, can be used to manage many targets as a single unit where you can define the group membership by defining the properties that constitute the group. For example, you could use dynamic groups to manage privileges or groups that you create containing the targets that are managed for different support teams.

6.2 Managing Groups

By combining targets in a group, Enterprise Manager provides management features that enable you to efficiently manage these targets as one group. Using the Group functionality, you can:

- View a summary status of the targets within the group.

- Monitor incidents for the group collectively, rather than individually.
- Monitor the overall performance of the group.
- Perform administrative tasks, such as scheduling jobs for the entire group, or blacking out the group for maintenance periods.

You can also customize the console to provide direct access to group management pages.

When you choose Groups from the Targets menu in the Enterprise Manager, the Groups page appears. You can view the currently available groups and perform the following tasks:

- View a list of all the defined groups.
- Search for existing groups and save search criteria for future searches.
- View a member status summary and rollup of incidents for members in a group.
- Create Groups, Dynamic Groups or the Administration Group hierarchy, edit the configuration of a selected group, remove groups, and, in the case of an Administration Group, associate or disassociate a Template Collection.
- Add groups or privilege propagating groups, remove groups, and change the configuration of currently defined groups.
- Drill down from a specific group to collectively monitor and manage its member targets.
- Customize the homepage of a specific group

Redundancy systems and special high availability groups are not accessed from this Groups page. You can access them from the All Targets page or you can access Redundancy Systems and other systems from the Systems page.

6.2.1 Creating and Editing Groups

Enterprise Manager Groups enable administrators to logically organize distributed targets for efficient and effective management and monitoring.

To create a group, follow these steps:

1. From the Enterprise Manager Console, choose **Targets** then choose **Groups**. Alternately, you can choose **Add Target** from the **Setup** menu and choose the menu option to add the specific type of group.
2. Click **Create** and choose the type of group you want to create. The Enterprise Manager Console displays a set of Create Group pages that function similarly to a wizard.
3. On the General tab of the Create Group page, enter the **Name** of the Group you want to create. If you want to make this a privilege propagating group, then enable the Privilege Propagation option by clicking **Enabled**. If you enable Privilege Propagation for the group, the target privileges granted on the group to an administrator or a role are propagated to the member targets. As with regular groups with privilege propagation, the Create Privilege Propagating Group privilege is required for creation of privilege propagating dynamic groups. In addition, the Full any Target privilege is required to enable privilege propagation because only targets on which the owner has Full Target privileges can be members, and any target can potentially match the criteria and a system wide Full privilege is required. To create a regular dynamic group, the View any Target

system wide privilege is required as the group owner must be able to view any target that can potentially match the membership criteria.

4. Configure each page, then click **OK**. You should configure all the pages before clicking **OK**. For more information about these steps, see the online help.

After you create the group, you always have immediate access to it from the Groups page.

You can edit a group to change the targets that comprise the group, or change the metrics that you want to use to summarize a given target type. To edit a group, follow these steps:

1. From the Enterprise Manager Console, choose **Targets** then choose **Groups**.
2. Click the group **Name** for the group you want to edit.
3. Click **Edit** from the top of the groups table.
4. Change the configuration for a page or pages, then click **OK**.

6.2.2 Creating Dynamic Groups

The owner of a dynamic group specifies the membership criteria during dynamic group creation (or modification) and membership in the group is determined solely by the criteria specified. Membership in a dynamic group cannot be modified directly. Enterprise Manager automatically adds targets that match membership criteria when a dynamic group is created. It also updates group membership as new targets are added or target properties are changed and the targets match the group's membership criteria.

To create a dynamic group, follow these steps:

1. From the Groups page, click **Create** and then select **Dynamic Group** from the drop-down list. Alternately, you can choose **Add Target** from the **Setup** menu and then select **Group**.
2. On the General tab of the Create Dynamic Group page, enter the **Name** of the Dynamic Group you want to create. If you want to make this a privilege propagating dynamic group, then enable the Privilege Propagation option by clicking **Enabled**. If you enable Privilege Propagation for the group, the target privileges granted on the group to an administrator or a role are propagated to the member targets. As with regular groups with privilege propagation, the Create Privilege Propagating Group privilege is required for creation of privilege propagating dynamic groups. In addition, the Full any Target privilege is required to enable privilege propagation because only targets on which the owner has Full Target privileges can be members, and any target can potentially match the criteria and a system wide Full privilege is required. To create a regular dynamic group, the View any Target system wide privilege is required as the group owner must be able to view any target that can potentially match the membership criteria.

   The privilege propagating group feature contains two privileges:

   - Create Privilege Propagating Group

     This privileged activity allows the administrators to create the privilege propagating groups. Administrators with this privilege can create propagating groups and delegate the group administration activity to other users.

   - Group Administration

Grant this privilege to an administrator or role that enables him to become group administrator for the group. This means he can perform operations on the group, share privileges on the group with other administrators, etc.

The Group Administration Privilege is available for both Privilege Propagating Groups and conventional groups. If you are granted this privilege, you can grant full privilege access to the group to other Enterprise Manager users without having to be the SuperAdministrator to grant the privilege.

3. In the Define Membership Criteria section, define the criteria for the dynamic group membership by clicking **Define Membership Criteria**.

   The Define Membership Criteria page appears where you can Add or Remove properties of targets to be included in the group. Group members must match one value in each of the populated target properties. Use the Member Preview section to review a list of targets that match the criteria. Click **OK** to return to the General page.

   At least one of the criteria on the Define Membership Criteria page must be specified. You cannot create a Dynamic group without at least one of the target types, on hosts or target properties specified. Use the following criteria for dynamic groups:

   - Target type(s)
   - Department
   - On Host
   - Target Version
   - Lifecycle Status
   - Operating System
   - Line of Business
   - Platform
   - Location
   - CSI
   - Cost Center
   - Contact
   - Comment

   You can add or remove properties using the **Add** or **Remove** Target Properties button on the Define Membership Criteria page.

4. Enter the **Time Zone**. The time zone you select is used for scheduling operations such as jobs and blackouts on this group. The groups statistics charts will also use this time zone.

5. Click the **Charts** tab. Specify the charts that will be shown in the Dynamic Group Charts page. By default, the commonly used charts for the target types contained in the Dynamic Group are added.

6. Click the **Columns** tab to add columns and abbreviations that will be seen in the Members page and also in the Dashboard.

7. Click the **Dashboard** tab to specify the parameters for the System Dashboard. The System Dashboard displays the current status and incidents and compliance

violations associated with the members of the Dynamic Group in graphical format.

8. Click the **Access** tab. Use the Access page to administer access privileges for the group. On the Access page you can grant target access to Enterprise Manager roles and grant target access to Enterprise Manager administrators.
9. Click **OK** to create the Dynamic Group.

6.2.3 Adding Members to Privilege Propagating Groups

The target privileges granted on a propagating group are propagated to member targets. The administrator grants target objects scoped to another administrator, and the grantee maintains the same privileges on member targets. The propagating groups maintain the following features:

- The administrator with a Create Privilege Propagating Group privilege will be able to create a propagating group
- To add a target as a member of a propagating group, the administrator must have *Full* target privileges on the target

You can add any non-aggregate target as the member of a privilege propagating group. For aggregate targets in Cloud Control version 12*c*, cluster and RAC databases and other propagating groups can be added as members. Cloud Control version 12*c* supports more aggregate target types, such as redundancy systems, systems and services.

If you are not the group creator, you must have at least the *Full* target privilege on the group to add a target to the group.

6.2.4 Converting Conventional Groups to Privilege Propagating Groups

In Enterprise Manager release 12*c* you can convert conventional groups to privilege propagating groups (and vice-versa) through the use of the specified EM CLI verb. Two new parameters have been added in the *modify_group* EM CLI verb:

- *privilege_propagation*

  This parameter is used to modify the privilege propagation behavior of the group. The possible value of this parameter is either true or false.

- *drop_existing_grants*

  This parameter indicates whether existing privilege grants on that group are to be revoked at the time of converting a group from privilege propagation to normal (or vice versa). The possible values of this parameter are yes or no. The default value of this parameter is yes.

These same enhancements have been implemented on the following EM CLI verbs: *modify_system*, *modify_redundancy_group*, and *modify_aggregrate_service*.

The EM CLI verb is listed below:

```
emcli modify_group
   -name="name"
   [-type=<group>]
   [-add_targets="name1:type1;name2:type2;..."]...
   [-delete_targets="name1:type1;name2:type2;..."]...
   [-privilege_propagation = true/false]
   [-drop_existing_grants = Yes/No]
```

For more information about this verb and other EM CLI verbs, see the *EM CLI Reference Manual*.

6.2.5 Viewing and Managing Groups

Enterprise Manager enables you to quickly view key information about members of a group, eliminating the need to navigate to individual member targets to check on availability and performance. You can view the entire group on a single screen and drill down to obtain further details. The Group Home page provides the following sections:

- A General section that displays the general information about the group, such as the Owner, Group Type, and whether the group is privilege propagating. You can drill down to the Edit Group page to enable or disable privilege propagating by clicking on the Privilege Propagating field.
- A Status section that shows how many member targets are in Up, Down, and Unknown states. For nested groups, this segment shows how many targets are in up, down, and unknown states across all its sub-groups. The status roll up count is based on the unique member targets across all sub-groups. Consequently, even if a target appears more than once in sub-groups, it is counted only once in status roll ups.
- An Overview of Incidents and Problems section that displays the summary of incidents on members of the group that have been updated in the recent period of time. It also shows a count of open problems as well as problems updated in recent period of time.

  The rolled up information is shown for all the member targets regardless of their status. The status roll up count is based on the unique member targets across all sub-groups. Consequently, even if a target appears more than once in sub-groups, its alerts are counted only once in alert roll ups.

  Click the number in the Problems column to go to the Incident Manager page to search, view, and manage exceptions and issues in your environment. By using Incident Manager, you can track outstanding incidents and problems.
- A Compliance Summary section that shows the compliance of members of the group against the compliance standards defined for the group. This section also shows a rollup of violations by severity (critical, warning, minor warning) as well as the average compliance score(%).
- A Job Activity section that displays a summary of jobs for the targets in the group whose start date is within the last 7 days. You can click Show to see the latest run or all runs. Click View to select and reorder the columns that appear in the table or to adjust scrolling and expanding the table.
- A Blackouts section that displays information about current or pending blackouts. You can also create a blackout from this section.
- A Patch Recommendations section that displays the Oracle patch recommendations that are applicable to your enterprise. You can view patch recommendations by classification or target type.

  You can navigate to My Oracle Support to view all recommendations by clicking the All Recommendations link.
- An Inventory and Usage section where you can view inventory summaries for deployments such as hosts, database installations, and fusion middleware installations on an enterprise basis or for specific targets. You can also view

inventory summary information in the context of different dimensions. From here you can click See Details to display the Inventory and Usage page.

- A Configuration Changes section that displays the number of configuration changes to the group in the previous 7 days. You can click the number to display a page that displays detailed information about the changes. Enterprise Manager automatically collects configuration information for group targets and changes to configurations are recorded and may be viewed from that page.

Viewing a Group

To view a group, follow these steps:

1. From the Enterprise Manager Console, choose **Targets** then choose **Groups**. A summary table lists all defined groups.
2. Click the desired group to go to the Home page of that group.

You can use View By filters (located in the upper right corner of the home page) to change the view of the homepage to members of targets of a specific type. When you do this, the Group homepage refreshes to only show information for targets of that type. Additional regions of interest might display. For example, DBAs might switch to the Database filter to view information specifically on Database targets in the group.

You can also personalize the home page by clicking the Actions icon in the upper right corner of each region on the home page to move that region up or down on the page. You can also expand or contract a region by clicking the arrow icon in the upper left corner of each region.

You can also navigate to other management operations on the group using the Group menu. For example, you can view all the members in a group by choosing **Member** from the Group menu. Likewise you can view the **Membership History** of the group by choosing Membership History from the Group menu.

6.2.6 Overview of Group Charts

Group Charts enable you to monitor the collective performance of a group. Out-of-box performance charts are provided based on the type of members in the group. For example, when databases are part of the group, a Wait Time (%) chart is provided that shows the top databases with the highest wait time percentage values. You can view this performance information over the last 24 hours, last 7 days, or last 31 days. You can also add your own custom charts to the page.

6.2.7 Overview of Group Members

Enterprise Manager allows you to summarize information about the member targets in a group. It provides information on their current availability status, roll-up of open incidents and compliance violations, and key performance metrics based on the type of targets in the group.

You can visually assess availability and relative performance across all member targets. You can rank members by a certain criterion (for example, database targets in order of decreasing wait time percentage). You can display default key performance metrics based on the targets you select, but you can customize these to include additional metrics that are important for managing your group.

You can view the members of a group by choosing **Members** from the Group menu. Enterprise Manager displays the Members page where you can view the table of members filtered by All Members, Direct Members, or Indirect Members. Direct members are targets directly added to the group. Indirect members are targets that are members of a direct member target, and are automatically included into the group because their parent target was added to the group. The page provides the option to **Export** or **Edit** the group.

You can also access information about membership history by choosing **Membership History** from the Group menu. The Membership History page displays changes in the group membership over time.

6.2.8 Viewing Group Status History

You can view Status History for a group to see the historical availability of a member during a specified time period or view the current status of all group members. You can access the Status History page by choosing **Monitoring** from the Group menu and then selecting **Status History**.

Bar graphs provide a historical presentation of the availability of group members during a time period you select from the View Data drop-down list. The color-coded graphs can show statuses of Up, Down, Under Blackout, Agent Down, Metric Collection Error, and Status Pending. You can select time periods of 24 hours, 7 days, or 31 days.

To view the current status of a member, you can click a Status icon on the View Group Status History page to go to the Availability page, which shows the member's current and past availability status within the last 24 hours, 7 days, or 31 days. Click a member Name to go to the member's Home page. You can use this page as a starting point when evaluating the performance of the selected member.

6.2.9 About the System Dashboard

The System Dashboard enables you to proactively monitor the status, incidents and compliance violations in the group as they occur. The color-coded interface is designed to highlight problem areas — targets that are down are highlighted in red, metrics in critical severity are shown as red dots, metrics in warning severity are shown as yellow dots, and metrics operating within normal boundary conditions are shown as green dots.

Using these colors, you can easily determine the problem areas for any target and drill down for details as needed. An incident table is also included to provide a summary for all open incidents in the group. The incidents in the table are presented in reverse chronological order to show the most recent incidents first, but you can also click any column in the table to change the sort order. The colors in top bar of the Member Targets table change based on the incident's critical level. The priority progresses from warning to critical to fatal. If the group has at least one fatal incident (irrespective of critical or warning incidents), the top bar becomes dark red. If the group has at least one critical incident (irrespective of warning incidents), the top bar becomes faint red. If the group has only warning incidents, the top bar turns yellow. If the group has no incidents, the top bar remains colorless.

The Dashboard auto-refreshes based on the Refresh Frequency you set on the Customize Dashboard page.

The Dashboard allows you to drill down for more detailed information. You can click the following items in the Dashboard for more information:

- A target name to access the target home page
- A group or system name to access the System Dashboard
- Status icon corresponding to specific metric columns to access the metric detail page

- Status icon for a metric with key values to access the metric page with a list of all key values
- Dashboard header to access the group home page
- Incidents and Problems table to view summary information about all incidents or specific categories of incidents.

Click **Customize** to access the Customize Dashboard page. This page allows you to change the refresh frequency and display options for the Member Targets table at the top of the dashboard. You can either show all individual targets or show by target type. There is also the option to expand or contract the Incidents and Problems table at the bottom. To change the columns shown in the Member Targets table, go to the Columns tab of the Edit Group page which you can access by choosing Target Setup from the Group menu.

In the Group by Target Type mode, the Dashboard displays information of the targets based on the specific target types present in the group or system. The statuses and incidents displayed are rolled up for the targets in that specific target type.

If you minimize the dashboard window, pertinent alert information associated with the group or system is still displayed in the Microsoft Windows toolbar.

You can use Information Publisher reports to make the System Dashboard available to non-Enterprise Manager users. First, create a report and include the System Monitoring Dashboard reporting element. In the report definition, choose the option, Allow viewing without logging in to Enterprise Manager. Once this is done, you can view it from the Enterprise Manager Information Publisher Reports website.

6.3 Using Out-of-Box Reports

Enterprise Manager provides several out-of-box reports for groups as part of the reporting framework, called Information Publisher. These reports display important administrative information, such as hardware and operating system summaries across all hosts within a group, and monitoring information, such as outstanding alerts and incidents for a group.

You can access these reports from the **Information Publisher Reports** menu item on the Groups menu.

See Also: Chapter 26, "Using Information Publisher"

7 Using Administration Groups

Administration groups greatly simplify the process of setting up targets for management in Enterprise Manager by automating the application of management settings such as monitoring settings or compliance standards. Typically, these settings are manually applied to individual target, or perhaps semi-automatically using custom scripts. However, by defining administration groups, Enterprise Manager uses specific target properties to direct the target to the appropriate administration group and then automatically apply the requisite monitoring and management settings. Any change to the monitoring setting will be automatically applied to the appropriate targets in the administration group. This level of automation simplifies the target setup process and also enables a datacenter to easily scale as new targets are added to Enterprise Manager for management.

This chapter covers the following topics:

- What is an Administration Group?
- Planning
- Implementing Administration Groups and Template Collections
- Removing Administration Groups

Instructional Videos: For a video tutorials on using administration groups and template collections, see:

Use Administration Groups and Template Collections - Part 1

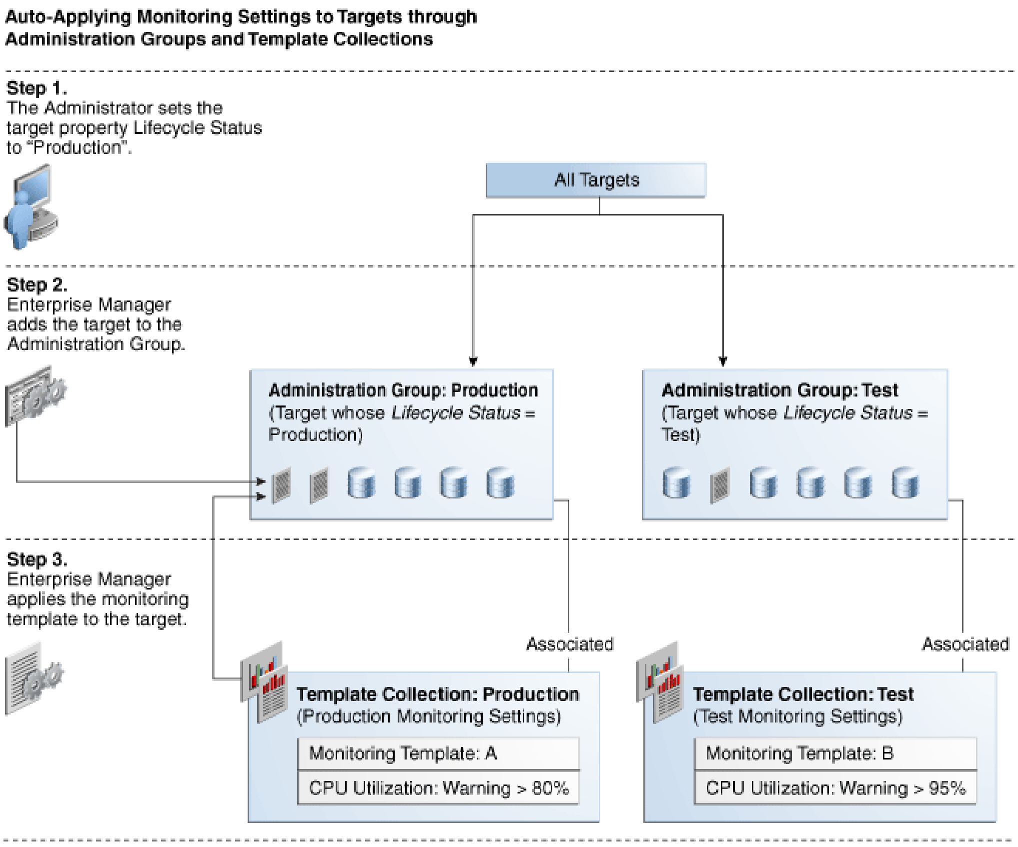
`https://apex.oracle.com/pls/apex/f?p=44785:24:6424795248965:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5732%2C24`

Use Administration Groups and Template Collections - Part 2

`https://apex.oracle.com/pls/apex/f?p=44785:24:15101831740469:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5733%2C24`

7.1 What is an Administration Group?

Administration groups are a special type of group used to fully automate application of monitoring and other management settings targets upon joining the group. When a target is added to the group, Enterprise Manager applies these settings using a template collection consisting of monitoring templates, compliance standards, and cloud policies. This completely eliminates the need for administrator intervention. The following illustration demonstrates the typical administration group workflow:


Auto-Applying Monitoring Settings to Targets through Administration Groups and Template Collections
Step 1.
The Administrator sets the target property Lifecycle Status to "Production".
All Targets
Step 2.
Enterprise Manager adds the target to the Administration Group.
Administration Group: Production
(Target whose *Lifecycle Status* = Production)
Administration Group: Test
(Target whose *Lifecycle Status* = Test)
Step 3.
Enterprise Manager applies the monitoring template to the target.
Associated
Associated
Template Collection: Production
(Production Monitoring Settings)
Monitoring Template: A
CPU Utilization: Warning > 80%
Template Collection: Test
(Test Monitoring Settings)
Monitoring Template: B
CPU Utilization: Warning > 95%

The first step involves setting a target's Lifecycle Status property when a target is first added to Enterprise Manager for monitoring. At that time, you determine where in the prioritization hierarchy that target belongs; the highest level being "mission critical" and the lowest being "development."

Target Lifecycle Status prioritization consists of the following levels:

- Mission Critical (highest priority)
- Production
- Stage
- Test
- Development (lowest priority)

As shown in step two of the illustration, once Lifecycle Status is set, Enterprise Manger uses it to determine which administration group the target belongs.

In order to prevent different monitoring settings to be applied to the same target, administration groups were designed to be mutually exclusive with other administration groups in terms of group membership. Administration groups can also be used for hierarchically classifying targets in an organization, meaning a target can belong to at most one administration group. This also means you can only have one administration group hierarchy in your Enterprise Manager deployment.

For example, in the previous illustration, you have an administration group hierarchy consisting of two subgroups: *Production* targets and *Test* targets, with each subgroup having its own template collections. In this example, the Production group inherits monitoring settings from monitoring template A while targets in the Test subgroup inherit monitoring settings from monitoring template B.

7.1.1 Developing an Administration Group

In order to create an administration group, you must have both *Full Any Target* and *Create Privilege Propagating Group* target privileges.

Developing an administration group is performed in two phases:

- **Planning**
  - Plan your administration group hierarchy by creating a group hierarchy in a way reflects how you monitor your targets.
  - Plan the management settings associated with the administration groups in the hierarchy.
    - Management settings: Monitoring settings, Compliance standard settings, Cloud policy settings
    - For Monitoring settings, you can have additional metric settings or override metric settings lower in your hierarchy
    - For Compliance standards or Cloud policies, additional rules/policies lower in the hierarchy are additive
- **Implementation**
  - Enter the group hierarchy definition and management settings in Enterprise Manager.
    - Create the administration group hierarchy.
    - Create the monitoring templates, compliance standards, cloud policies and add these to template collections.
    - Associate template collections with administration groups.
    - Add targets to the administration group by assigning the appropriate values to the target properties such that Enterprise Manager automatically adds them to the appropriate administration group.

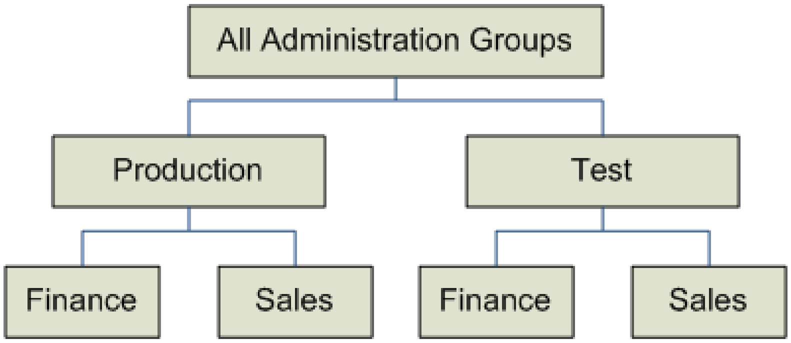
7.2 Planning

As with any management decision, the key to effective implementation is planning and preparation. The same holds true for administration groups.

Step 1: Plan Your Group Hierarchy

You can only have one administration group hierarchy in your Enterprise Manager deployment, thus ensuring that administration group member targets can only directly belong to one administration group. This prevents monitoring conflicts from occurring as a result of having a target join multiple administration groups with different associated monitoring settings.

To define the hierarchy, you want to think about the highest (root) level as consisting of all targets that have been added to Enterprise Manager. Next, think about how you want to divide your targets along the lines of how they are monitored, where targets that are monitored in one way are in one group, and targets that are monitored in another way are part of another group. For example, Production targets might be monitored one way and Test targets might be monitored in another way. You can further divide individual groups if there are further differences in monitoring. For example, your Production targets might be further divided based on the line of business they support because they might have additional metrics that need to be monitored for that line of business. Eventually, you will end up with a hierarchy of groups under a root node.



The attributes used to define each level of grouping and thus the administration group membership criteria are based on *global target properties*, which are attributes of every target that specify operational information within the organization. For example, *location*, *line of business* to which it belongs, and *lifecycle status*. Target properties that can be used in the definition of administration groups are:

- Lifecycle Status

> **Note:** Lifecycle Status target property is of particular importance because it denotes a target's operational status. Lifecycle Status can be any of the following: Mission Critical, Production, Staging, Test, or Development.

- Location
- Line of Business
- Department
- Cost Center
- Contact
- Platform
- Operating System
- Target Version
- Customer Support Identifier
- Target Type (Allowed but not a global target property.)

You cannot manually add targets to an administration group. Instead, you set the target properties of the target (prospective group member) to match the membership criteria defined for the administration group. Once the target properties are set, Enterprise Manager automatically adds the target to the appropriate administration group.

Enterprise Manager Administrators and Target Properties

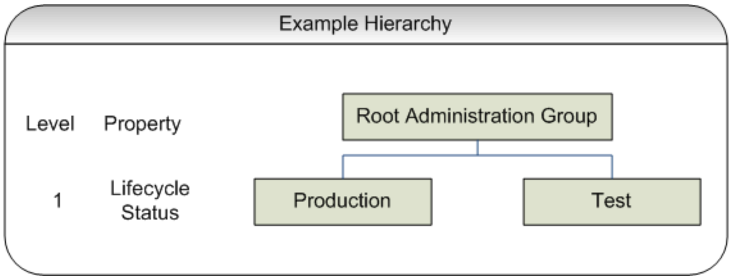
When creating an Enterprise Manager administrator, you can associate properties such as Contact, Location, and Description. However, there are additional resource allocation properties that can be associated with their profile. These properties are:

- Department
- Cost Center
- Line of Business

It is important to note that these properties are persistent--when associated with an administrator, the properties (which mirror, in part, the target properties listed above) are automatically passed to any targets that are discovered or created by the administrator.

Example

In the following administration group hierarchy, two administration groups are created under the node *Root Administration Group*, *Production* and *Test*, because monitoring settings for production targets will differ from the monitoring settings for test targets.



In this example, the group membership criteria are based on the *Lifecycle Status* target property. Targets whose *Lifecycle Status* is 'Production' join the Production group and targets whose *Lifecycle Status* is 'Test' join the Test group. For this reason, *Lifecycle Status* is the target property that determines the first level in the administration group hierarchy. The values of Lifecycle Status property determine the membership criteria of the administration groups in the first level: Production group has membership criteria of "Lifecycle Status = Production" and Test group has membership criteria of "Lifecycle Status = Test' membership criteria.

Additional levels in the administration group hierarchy can be added based on other target properties. Typically, additional levels are added if there are additional monitoring (or management) settings that need to be applied and these could be different for different subsets of targets in the administration group. For example, in the *Production* group, there could be additional monitoring settings for targets in *Finance* line of business that are different from targets in *Sales* line of business. In this case, an additional level based on *Line of Business* target property level would be added.

The end result of this hierarchy planning exercise is summarized in the following table.

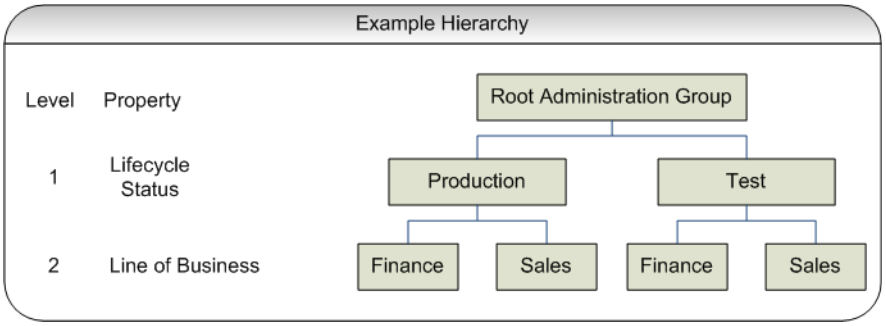
Root Level (First Row)	Level 1 target property (second row) Lifecycle Status	Level 2 target property (third row) Line of Business
Root Administration Group	Production or Mission Critical	Finance
		Sales
	Staging or Test or Development	Finance
		Sales

Each cell of the table represents a group. The values in each cell represent the values of the target property that define membership criteria for the group.

It is possible to have the group membership criteria be based on more than one target property value. In that case, any target whose target property matches any of the values will be added to the group. For example, in the case of the Production group, if the *Lifecycle Status* of a target is either *Production* or *Mission Critical*, then it will be added to the Production group.

It is also important to remember that group membership criteria is cumulative. For example, for the *Finance* group under *Production or Mission Critical* group, a target must have its *Lifecycle Status* set to *Production or Mission Critical* **AND** its *Line of Business* set to *Finance* before it can join the group. If the target has its *Lifecycle Status* set to *Production* but does not have its *Line of Business* set to *Finance* or *Sales*, then it does not join any administration group.

For this planning example, the resulting administration group hierarchy would appear as shown in the following graphic.



It is important to note that a target can become part of hierarchy if and only if its property values match criteria at both the levels. A target possessing matching values for *lifecycle status* cannot become member of the administration group at the first level. Also, all targets in the administration group hierarchy will belong to the lowest level groups.

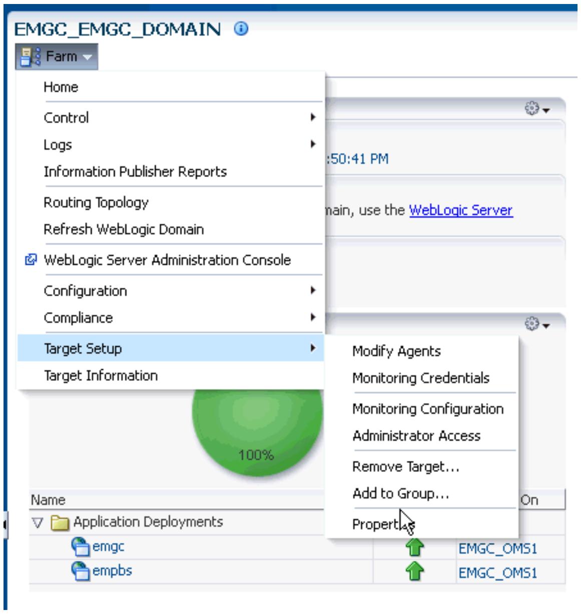
Step 2: Assign Target Properties

After establishing the desired administration group hierarchy, you must make sure properties are set correctly for each target to ensure they join the correct administration group. Using target properties, Enterprise Manager automatically places targets into the appropriate administration group without user intervention. For targets that have already been added to Enterprise Manager, you can also set the target properties via the console or using the EM CLI verb *set_target_property_value*, See the Enterprise

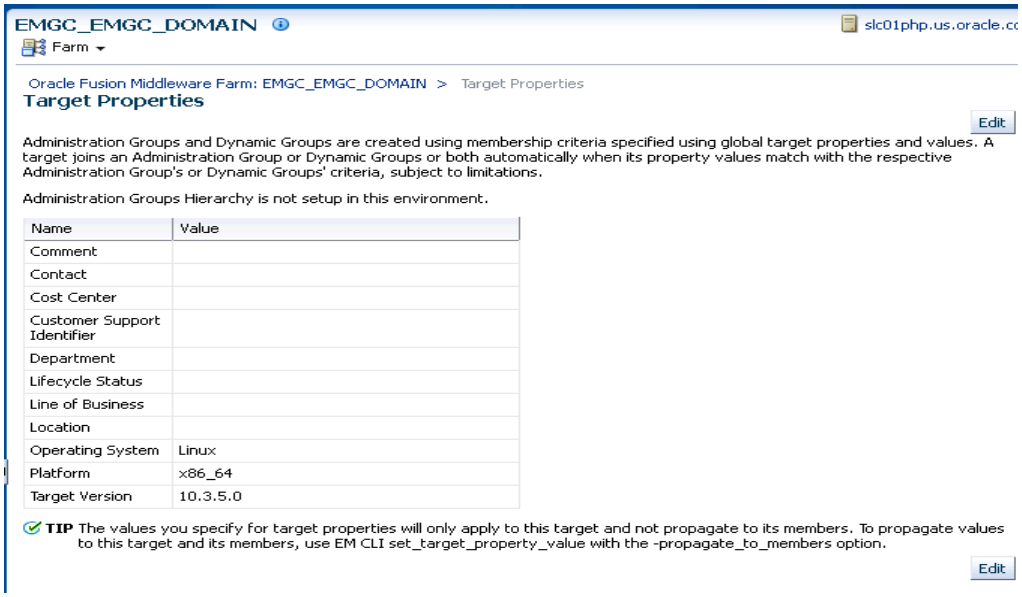
Manager Command Line Interface guide for more information. Note that when running *set_target_property_value*, any prior values of the target property are overwritten. If you set target properties before hierarchy creation, it will join the group after it is created. The targets whose properties are set using EM CLI will automatically join their appropriate administration groups. Target properties can, however, be set after the administration group hierarchy is created.

For small numbers of targets, you can change target properties directly from the Enterprise Manager console.

1. From an Enterprise Manager target's option menu, select **Target Setup**, then select **Properties**.



2. On the **Target Properties** page, click **Edit** to change the property values.



EMGC_EMGC_DOMAIN
Farm
slc01php.us.oracle.cc

Oracle Fusion Middleware Farm: EMGC_EMGC_DOMAIN > Target Properties

Target Properties

Edit

Administration Groups and Dynamic Groups are created using membership criteria specified using global target properties and values. A target joins an Administration Group or Dynamic Groups or both automatically when its property values match with the respective Administration Group's or Dynamic Groups' criteria, subject to limitations.

Administration Groups Hierarchy is not setup in this environment.

Name	Value
Comment	
Contact	
Cost Center	
Customer Support Identifier	
Department	
Lifecycle Status	
Line of Business	
Location	
Operating System	Linux
Platform	x86_64
Target Version	10.3.5.0

TIP The values you specify for target properties will only apply to this target and not propagate to its members. To propagate values to this target and its members, use EM CLI set_target_property_value with the -propagate_to_members option.

Edit

To help you specify the appropriate target property values used as administration group criteria, pay attention to the instructional verbiage at the top of the page.

3. Once you have set the target properties, click **OK**.

For large numbers of targets, it is best to use the Enterprise Manager Command Line Interface (EM CLI) `set_target_property_value` verb to perform a mass update. For more information about this EM CLI verb, see the Enterprise Manager Command Line Interface guide.

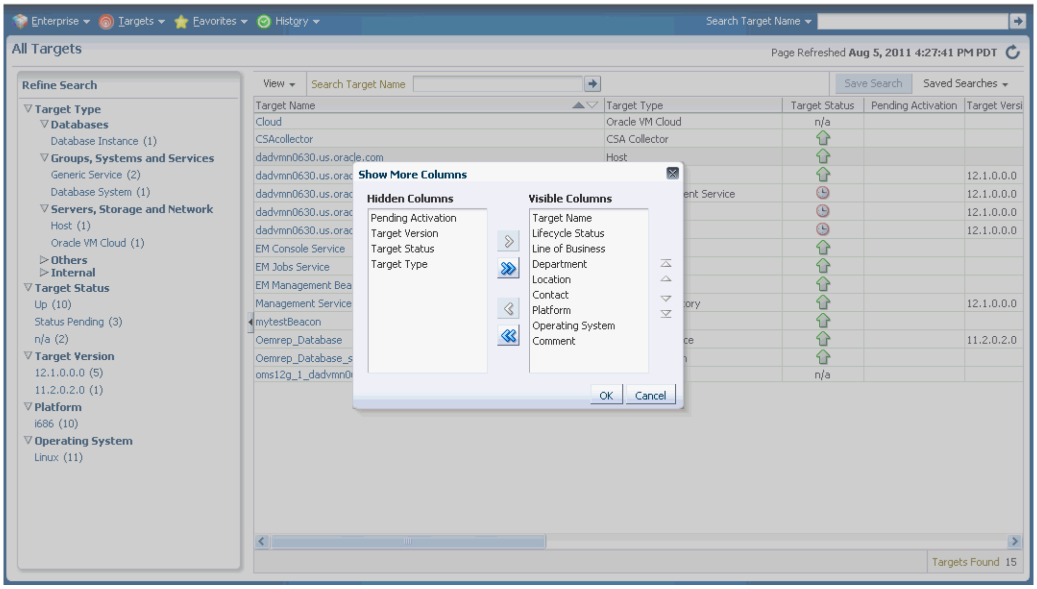
Administration groups are privilege-propagating: Any privilege that you grant on the administration group to a user (or role) automatically applies to all members of the administration group. For example, if you grant Operator privilege on the Production administration group to a user or role, then the user or role automatically has Operator privileges on all targets in the administration group. Because administration groups are always privilege propagating, any aggregate target that is added to an administration group must also be privilege propagating.

> **Note:** An aggregate target is a target containing other member targets. For example, a Cluster Database (RAC) is an aggregate target has RAC instances.

A good example of aggregate target is the Privilege Propagating Group. See "Managing Groups" on page 6-1 for more information.

At any time, you can use the **All Targets** page to view properties across all targets. To view target properties:

1. From the **Targets** menu, select **All Targets** to display the All Targets page.
2. From the **View** menu, select **Columns**, then select **Show All**.
3. Alternatively, if you are interested in specific target properties, choose **Columns** and then select **Show More Columns** to display column selector, as shown in following graphic.



Target Name	Target Type	Target Status	Pending Activation	Target Versi
Cloud	Oracle VM Cloud	n/a		
CSAcollector	CSA Collector	⇧		
dadvmn0630.us.oracle.com	Host	⇧		
dadvmn0630.us.orac		⇧		12.1.0.0.0
dadvmn0630.us.orac	ent Service	🕒		12.1.0.0.0
dadvmn0630.us.orac		🕒		12.1.0.0.0
dadvmn0630.us.orac		🕒		12.1.0.0.0
EM Console Service		⇧		
EM Jobs Service		⇧		
EM Management Bea		⇧		
Management Service	ory	⇧		12.1.0.0.0
mytestBeacon		⇧		
Oemrep_Database	ce	⇧		11.2.0.2.0
Oemrep_Database_s	n	⇧		
oms12g_1_dadvmn0		n/a		

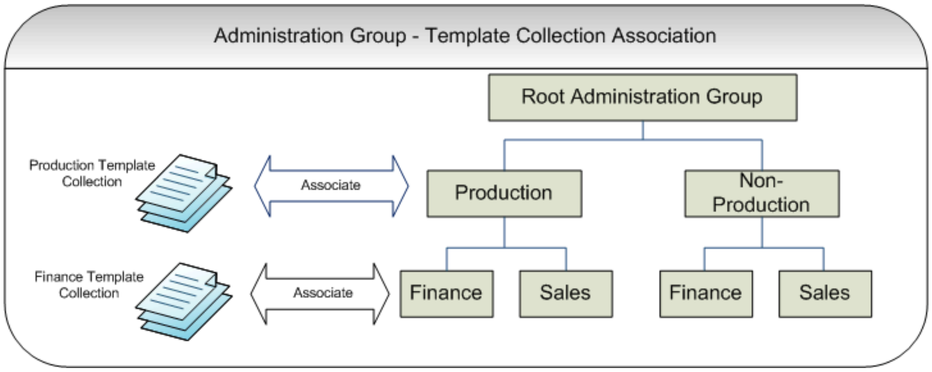
Show More Columns

Hidden Columns	Visible Columns
Pending Activation	Target Name
Target Version	Lifecycle Status
Target Status	Line of Business
Target Type	Department
	Location
	Contact
	Platform
	Operating System
	Comment

Step 3: Prepare for Creating Template Collections

Template collections contain the monitoring settings and other management settings that are meant to be applied to targets as they join the administration group. Monitoring settings for targets are defined in monitoring templates. Monitoring templates are defined on a per target type basis, so you will need to create monitoring templates for each of the different target types in your administration group. You will most likely create multiple monitoring templates to define the appropriate monitoring settings for an administration group. For example, you might create a database Monitoring template containing the metric settings for your production databases and a separate monitoring template containing the settings for your non-production databases. Other management settings that can be added to a template collection include Compliance Standards and Cloud Policies. Ensure all of these entities that you want to add to your template collection are correctly defined in Enterprise Manager before adding them to template collections.

If you have an administration group hierarchy defined with more than two levels, such as the hierarchy shown in the following figure, it is important to understand how management settings are applied to the targets in the administration group.


Administration Group - Template Collection Association
Root Administration Group
Production Template Collection
Associate
Production
Non-Production
Finance Template Collection
Associate
Finance
Sales
Finance
Sales

Each group in the administration group hierarchy can be associated with a template collection (containing monitoring templates, compliance standards, and cloud policies). If you associate a template collection containing monitoring settings with the *Production* group, then the monitoring settings will apply to the *Finance* and *Sales* subgroup under *Production*. If the *Finance* group under *Production* has additional monitoring settings, then you can create a monitoring template with only those additional monitoring settings. (Later, this monitoring template should be added to another template collection and associated with the *Finance* group). The monitoring settings from the *Finance Template Collection* will be logically combined with the monitoring settings from the *Production Template Collection*. In case there are duplicate metric settings in both template collections, then the metric settings from the *Finance Template Collection* takes precedence and will be applied to the targets in the *Finance* group.   This precedence rule only applies to the case of metric settings. In the case of compliance standard rules and cloud policies, even if there are duplicate compliance standard rules and cloud policies in both template collections, they will be all applied to the targets in the *Finance* group.

Once you have completed all the planning and preparation steps, you are ready to begin creating an administration group.

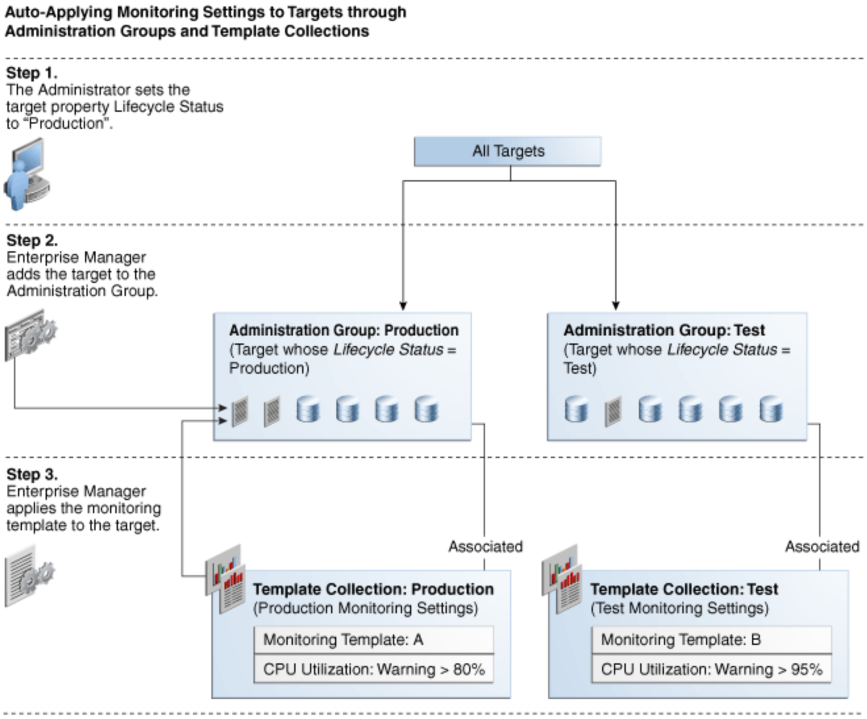
7.3 Implementing Administration Groups and Template Collections

With the preparatory work complete, you are ready to begin the four step process of creating an administration group hierarchy and template collections. The administration group user interface is organized to guide you through the creation process, with each tab containing the requisite operations to perform each step.

This process involves:

1. Creating the administration group hierarchy.
2. Create monitoring templates.
3. Creating template collections.
4. Associating template collections to administration group.
5. Synchronizing the targets with the selected items.

The following graphic shows a completed administration group hierarchy with associated template collections. It illustrates how Enterprise Manager uses this to automate the application of target monitoring settings.


Auto-Applying Monitoring Settings to Targets through Administration Groups and Template Collections
Step 1.
The Administrator sets the target property Lifecycle Status to "Production".
All Targets
Step 2.
Enterprise Manager adds the target to the Administration Group.
Administration Group: Production
(Target whose *Lifecycle Status* = Production)
Administration Group: Test
(Target whose *Lifecycle Status* = Test)
Step 3.
Enterprise Manager applies the monitoring template to the target.
Associated
Associated
Template Collection: Production
(Production Monitoring Settings)
Monitoring Template: A
CPU Utilization: Warning > 80%
Template Collection: Test
(Test Monitoring Settings)
Monitoring Template: B
CPU Utilization: Warning > 95%

7.3.1 Creating the Administration Group Hierarchy

The following four primary tasks summarize the administration group creation process. These tasks are conveniently arranged in sequence via tabbed pages.

> **Important:** In order to create the administration group hierarchy, you must have both **Full Any Target** and **Create Privilege Propagating Group** target privileges.

Task 1: Access the Administration Group and Template Collections page.

Task 2: Define the hierarchy.

From the **Hierarchy** tab, you define the administration group hierarchy that matches the way you manage your targets. See Section 7.3.1.2, "Defining the Hierarchy".

Task 3: Define the Template Collections.

From the **Template Collections** tab, you define the monitoring and management settings you want applied to targets. See Section 7.3.1.3, "Defining Template Collections".

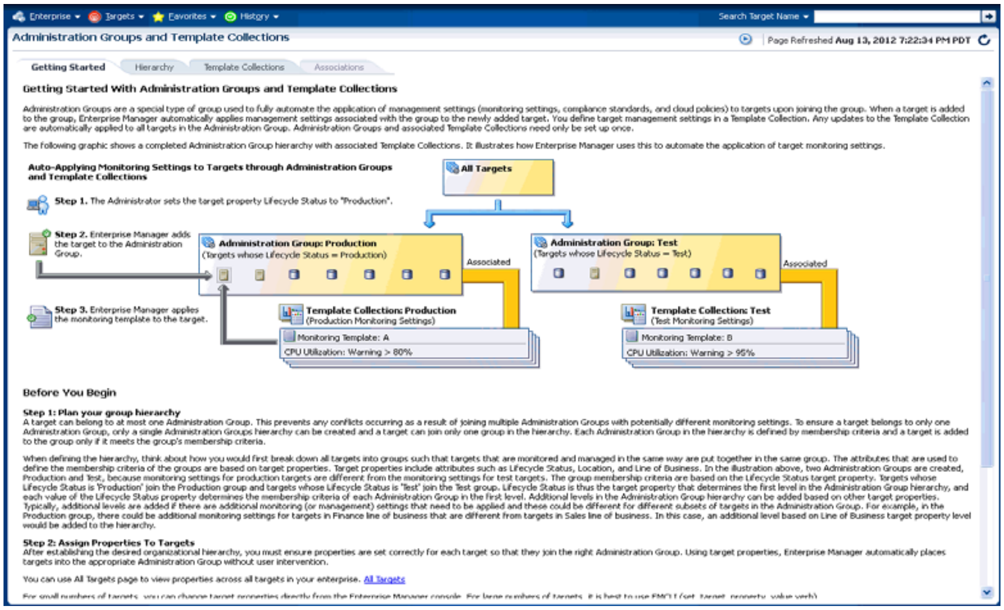
Task 4: Associate the Template Collections with the Administration Groups

From the **Associations** tab, you tie the monitoring and management settings to the appropriate administration group. See Section 7.3.1.4, "Associating Template Collections with Administration Groups".

7.3.1.1 Accessing the Administration Group Home Page

All administration group operations are performed from the Administration Groups home page.

From the **Setup** menu, select **Add Target** and then select **Administration Groups**. The Administration Groups home page displays.


Enterprise ▾
Targets ▾
Favorites ▾
History ▾
Search Target Name ▾
Administration Groups and Template Collections
Page Refreshed Aug 13, 2012 7:22:34 PM PDT
Getting Started
Hierarchy
Template Collections
Associations
All Targets
Administration Group: Production
(Targets whose Lifecycle Status = Production)
Associated
Administration Group: Test
(Targets whose Lifecycle Status = Test)
Associated
Template Collection: Production
(Production Monitoring Settings)
Monitoring Template: A
CPU Utilization: Warning > 80%
Template Collection: Test
(Test Monitoring Settings)
Monitoring Template: B
CPU Utilization: Warning > 95%

Getting Started With Administration Groups and Template Collections

Administration Groups are a special type of group used to fully automate the application of management settings (monitoring settings, compliance standards, and cloud policies) to targets upon joining the group. When a target is added to the group, Enterprise Manager automatically applies management settings associated with the group to the newly added target. You define target management settings in a Template Collection. Any updates to the Template Collection are automatically applied to all targets in the Administration Group. Administration Groups and associated Template Collections need only be set up once.

The following graphic shows a completed Administration Group hierarchy with associated Template Collections. It illustrates how Enterprise Manager uses this to automate the application of target monitoring settings.

Auto-Applying Monitoring Settings to Targets through Administration Groups and Template Collections

Step 1. The Administrator sets the target property Lifecycle Status to "Production".

Step 2. Enterprise Manager adds the target to the Administration Group.

Step 3. Enterprise Manager applies the monitoring template to the target.

Before You Begin

Step 1: Plan your group hierarchy
A target can belong to at most one Administration Group. This prevents any conflicts occurring as a result of joining multiple Administration Groups with potentially different monitoring settings. To ensure a target belongs to only one Administration Group, only a single Administration Groups hierarchy can be created and a target can join only one group in the hierarchy. Each Administration Group in the hierarchy is defined by membership criteria and a target is added to the group only if it meets the group's membership criteria.

When defining the hierarchy, think about how you would first break down all targets into groups such that targets that are monitored and managed in the same way are put together in the same group. The attributes that are used to define the membership criteria of the groups are based on target properties. Target properties include attributes such as Lifecycle Status, Location, and Line of Business. In the illustration above, two Administration Groups are created, Production and Test, because monitoring settings for production targets are different from the monitoring settings for test targets. The group membership criteria are based on the Lifecycle Status target property. Targets whose Lifecycle Status is 'Production' join the Production group and targets whose Lifecycle Status is 'Test' join the Test group. Lifecycle Status is thus the target property that determines the first level in the Administration Group hierarchy, and each value of the Lifecycle Status property determines the membership criteria of each Administration Group in the first level. Additional levels in the Administration Group hierarchy can be added based on other target properties. Typically, additional levels are added if there are additional monitoring (or management) settings that need to be applied and these could be different for different subsets of targets in the Administration Group. For example, in the Production group, there could be additional monitoring settings for targets in Finance line of business that are different from targets in Sales line of business. In this case, an additional level based on Line of Business target property level would be added to the hierarchy.

Step 2: Assign Properties To Targets
After establishing the desired organizational hierarchy, you must ensure properties are set correctly for each target so that they join the right Administration Group. Using target properties, Enterprise Manager automatically places targets into the appropriate Administration Group without user intervention.

You can use All Targets page to view properties across all targets in your enterprise. All Targets

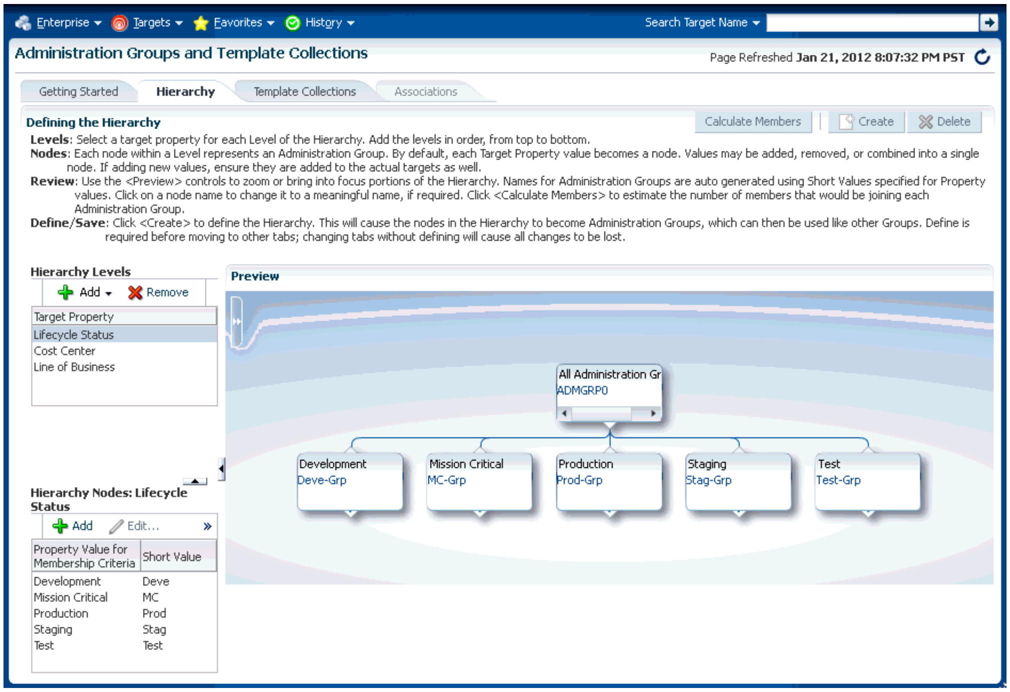
For small numbers of targets, you can change target properties directly from the Enterprise Manager console. For large numbers of targets, it is best to use EMCLI (set_target_property_value verb)

Read the relevant information on the **Getting Started** page. The information contained in this page summarizes the steps outlined in this chapter. For your convenience, links are provided that take you to appropriate administration group functions, as well as the Enterprise Manager **All Targets** page where you can view target properties.

7.3.1.2 Defining the Hierarchy

On this page you define the administration group hierarchy that reflects the organizational hierarchy you planned earlier and which target properties are associated with a particular hierarchy level.

On the left side of the page are two tables: Hierarchy Levels and Hierarchy Nodes.



Administration Groups and Template Collections

Defining the Hierarchy

Levels: Select a target property for each Level of the Hierarchy. Add the levels in order, from top to bottom.

Nodes: Each node within a Level represents an Administration Group. By default, each Target Property value becomes a node. Values may be added, removed, or combined into a single node. If adding new values, ensure they are added to the actual targets as well.

Review: Use the <Preview> controls to zoom or bring into focus portions of the Hierarchy. Names for Administration Groups are auto generated using Short Values specified for Property values. Click on a node name to change it to a meaningful name, if required. Click <Calculate Members> to estimate the number of members that would be joining each Administration Group.

Define/Save: Click <Create> to define the Hierarchy. This will cause the nodes in the Hierarchy to become Administration Groups, which can then be used like other Groups. Define is required before moving to other tabs; changing tabs without defining will cause all changes to be lost.

Hierarchy Levels

Target Property
Lifecycle Status
Cost Center
Line of Business

Hierarchy Nodes: Lifecycle Status

Property Value for Membership Criteria	Short Value
Development	Deve
Mission Critical	MC
Production	Prod
Staging	Stag
Test	Test

The **Hierarchy Levels** table allows you to add the target properties that define administration group hierarchy. The **Hierarchy Nodes** table allows you to define the values associated with the target properties in the **Hierarchy Levels** table. When you select a target property, the related property values are made available in the **Hierarchy Nodes** table, where you can add/remove/merge/split the values. In the **Hierarchy Nodes** table, each row corresponds to a single administration group. The Short Value column displays abbreviated value names that are used to auto-generate group names.

The **Hierarchy Levels** table allows you to add the target properties that define each level in the administration group hierarchy. The **Hierarchy Nodes** table allows you to define the values associated with the target properties in the **Hierarchy Levels** table. Each row in the **Hierarchy Nodes** table will correspond to a node or group in the administration group hierarchy for that level. When you select a target property in the **Hierarchy Levels** table, the related property values are made available in the **Hierarchy Nodes** table, where you can add/remove/merge/split the values. Merge two or more values if either value should be used as membership criteria for the corresponding administration group. The Short Value column displays abbreviated value names that are used to auto-generate group names.

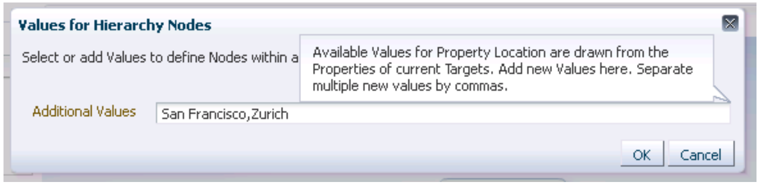
Adding a Hierarchy Level

1. On the **Administration Group** page, click the **Hierarchy** tab.
2. From the **Hierarchy Levels** table, click **Add** and choose one of the available target properties. You should add one property/level at a time instead of all properties at once.
3. With the target property selected in the **Hierarchy Levels** table, review the list of values shown in the **Hierarchy Nodes** table. The values of the target property in the **Hierarchy Nodes** table.

   Enterprise Manager finds all existing values of the target property across all targets and displays them in the **Hierarchy Nodes** table. For some target properties, such as Lifecycle Status, predefined property values already exist and are automatically displayed in the **Hierarchy Nodes** table. You can select and remove target property values that will not be used as membership criteria in any administration group. However, property values that are not yet available but will be used as administration group membership criteria, will need to be added.

The next step shows you how to add property values.

4. From the **Hierarchy Nodes** table, click **Add**. The associated property value add dialog containing existing values from various targets displays. Add the requisite value(s). Multiple values can be specified using a comma separated list. For example, to add multiple locations such as San Francisco and Zurich, add the **Location** target property to the **Hierarchy Level** table. Select **Location** and then click **Add** in the **Hierarchy Nodes** table. The **Values for Hierarchy Nodes** dialog displays. Enter "San Francisco,Zurich" as shown in the following graphic.



Values for Hierarchy Nodes

Select or add Values to define Nodes within a

Available Values for Property Location are drawn from the Properties of current Targets. Add new Values here. Separate multiple new values by commas.

Additional Values: San Francisco,Zurich

Extending Administration Group Hierarchy Maximum Limits

There is a default maximum for the number of values that can be supported for a target property as administration group criteria. If you see a warning message indicating that you have reached this maximum value, you can extend it using the OMS property *admin_groups_width_limit*. Specify the maximum number of values that should be supported for a target property. For example, to support up to 30 values for a target property that will be used in administration group criteria, set the admin_groups_width_limit as follows (using the OMS `emctl` utility):

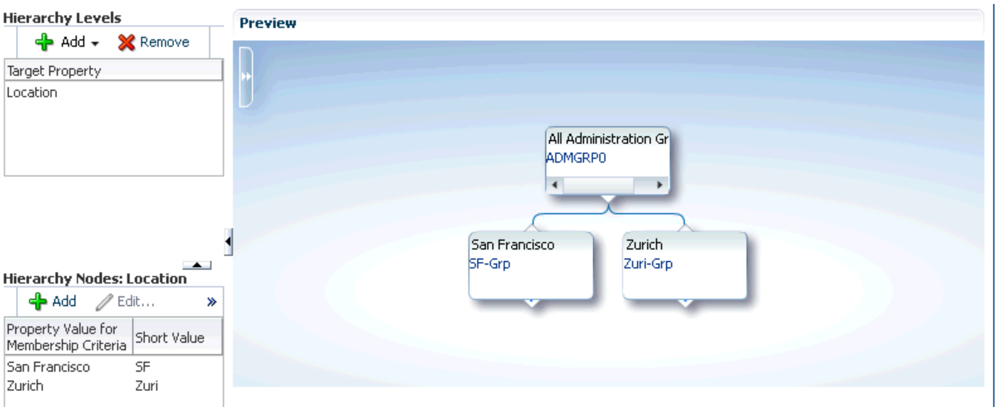
```
emctl set property -name admin_groups_width_limit -value 30 -module emoms
```

You can also add up to four levels after the root node of an administration group hierarchy. If there is a need to add additional level, you will first need to change the OMS *admin_groups_height_limit* property to the maximum height limit. For example, if you want to create to administration group hierarchy consisting of five levels after the root node, set the *admin_groups_height_limit* property as follows (using the OMS emctl utility):

```
emctl set property -name admin_groups_height_limit -value 5 -module emoms
```

This is a global property and only needs to be set once using the emctl utility of any OMS. This is also a dynamic property and does not require a stop/restart of the OMS in order to take effect.

Click **OK**. The two locations "San Francisco" and "Zurich" appear as nodes in the **Preview** pane as shown in the following graphic.



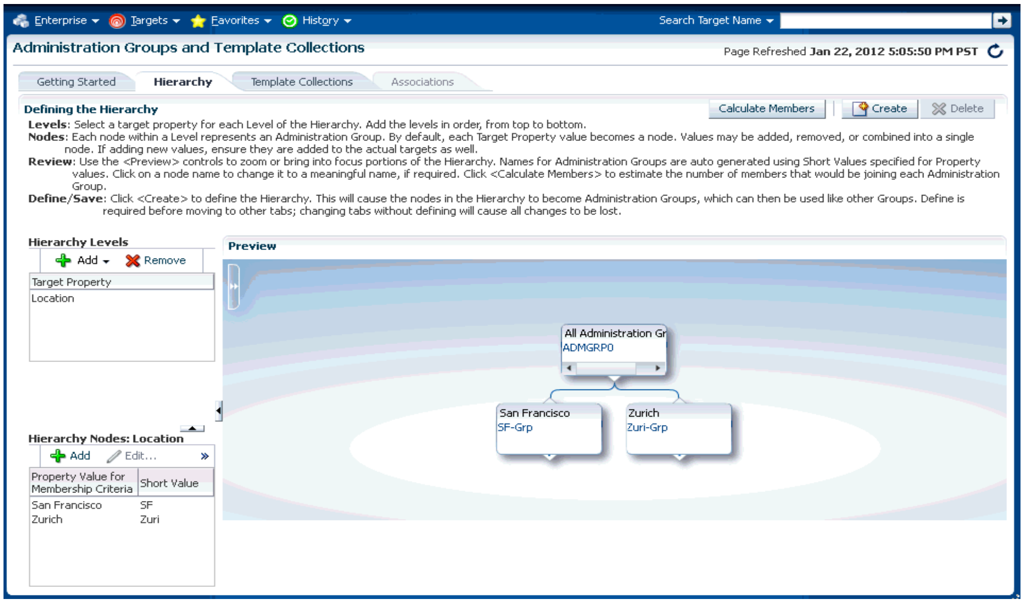
Property Value for Membership Criteria	Short Value
San Francisco	SF
Zurich	Zuri

Under certain circumstances, it may be useful to treat multiple property values as one: Targets may have different target property values, but should belong to the same administration group because they have same monitoring profile/settings. For example, if a combination of values is needed, such as *Production* or *Mission Critical* for the *Lifecycle Statu*s property, they need to be merged (combined into a single node).

To merge property values:

1. Select a target property from the list of chosen properties in the **Hierarchy Levels** table. The associated property values are displayed.
2. Select two or more property values by holding down the *Shift* key and clicking on the desired values.
3. Click **Merge**.

5. Continue adding hierarchy levels until the group hierarchy is complete. The **Preview** pane dynamically displays any changes you make to your administration group hierarchy.

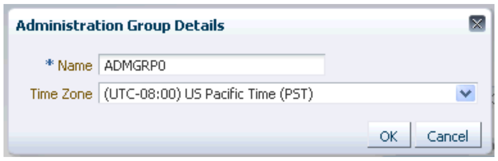


Defining the Hierarchy

Levels: Select a target property for each Level of the Hierarchy. Add the levels in order, from top to bottom.
Nodes: Each node within a Level represents an Administration Group. By default, each Target Property value becomes a node. Values may be added, removed, or combined into a single node. If adding new values, ensure they are added to the actual targets as well.
Review: Use the <Preview> controls to zoom or bring into focus portions of the Hierarchy. Names for Administration Groups are auto generated using Short Values specified for Property values. Click on a node name to change it to a meaningful name, if required. Click <Calculate Members> to estimate the number of members that would be joining each Administration Group.
Define/Save: Click <Create> to define the Hierarchy. This will cause the nodes in the Hierarchy to become Administration Groups, which can then be used like other Groups. Define is required before moving to other tabs; changing tabs without defining will cause all changes to be lost.

Property Value for Membership Criteria	Short Value
San Francisco	SF
Zurich	Zuri

6. Set the time zone for the group.
   1. Click on the group name. The Administration Group Details dialog displays allowing you to select the appropriate time zone.



Administration Group Details

* Name: ADMGRP0

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

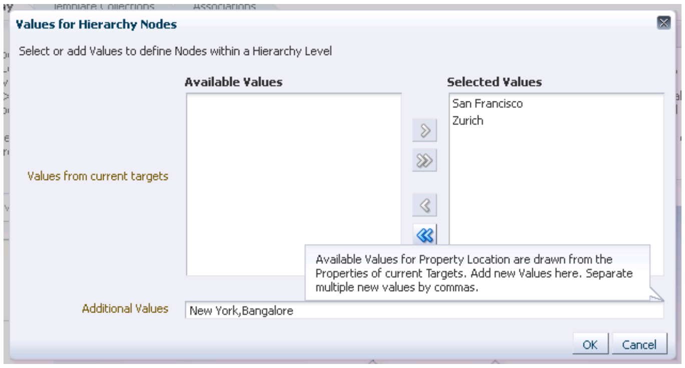
The administration group time zone is used for displaying group charts and also for scheduling operations on the group. Because this is also the default time zone for all subgroups that may be created under this group, you should specify the time zone at the highest level group in the administration group hierarchy before the subgroups are created. Note that the parent group time zone will be used when creating any child subgroups, but user can always select a child subgroup and change its time zone.

The auto-generated name can also be changed.

7. Click **Create** to define the hierarchy.

IMPORTANT: Review and define the complete hierarchy before clicking **Create**.

Even after your administration group hierarchy has been created, you can always make future updates if organizational needs change. For example, adding/removing group membership criteria property values, which equates to creating/deleting additional administration groups for a given level. Using the previous example, if in addition to San Francisco and Zurich you add more locations, say New York and Bangalore, you can click **Add** in the **Hierarchy Node** table to add additional locations, as shown in the following graphic. For more information about changing the administration group hierarchy, see "Changing the Administration Group Hierarchy" on page 7-28.



Values for Hierarchy Nodes

Select or add Values to define Nodes within a Hierarchy Level

Values from current targets — Available Values: (none); Selected Values: San Francisco, Zurich

Available Values for Property Location are drawn from the Properties of current Targets. Add new Values here. Separate multiple new values by commas.

Additional Values: New York,Bangalore

Click **Update** to save your changes.

7.3.1.3 Defining Template Collections

A template collection is an assemblage of monitoring/management settings to be applied to targets in the administration group. Multiple monitoring templates can be added to a template collection that in turn is associated with an administration group. However, you can only have one monitoring template of a particular target type in the template collection. The monitoring template should contain the complete set of metric settings for the target in the administration group. You should create one monitoring template for each type of target in the administration group. For example, you can have a template collection containing a template for database and a template for listener, but you cannot have a template collection containing two templates for databases. When members targets are added to an administration group, the template monitoring and management settings are automatically applied. A template will completely replace all metric settings in the target. This means applying the template copies over metric settings (thresholds, corrective actions, collection schedule) to the target, removes the thresholds of the metrics that are present in the target, but not included in the template. Removing of thresholds disables alert functionality for these metrics. Metric data will continue to be collected.

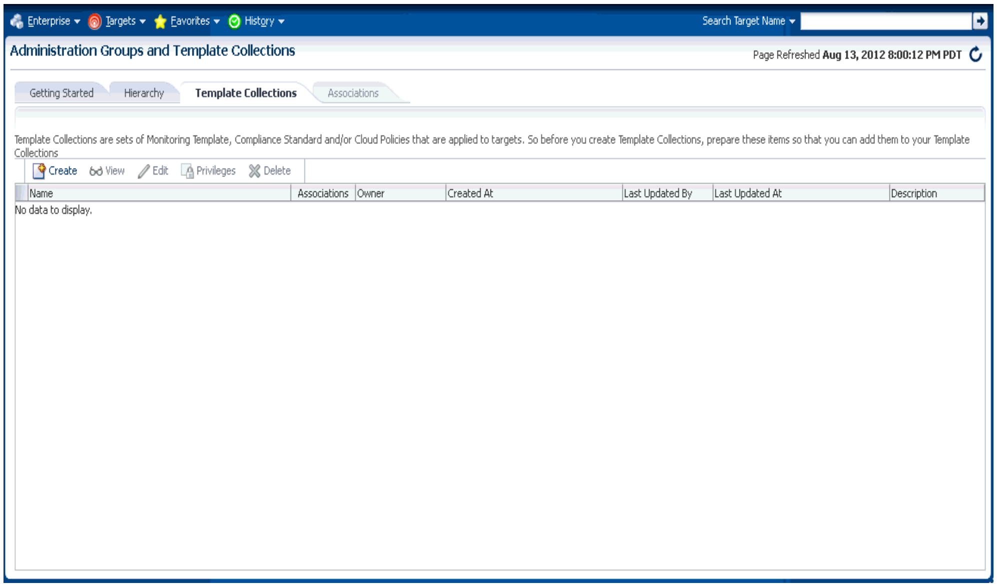
Template collections may consist of three types of monitoring/management setting categories:

- Monitoring Templates (monitoring settings)
- Compliance Standards (compliance policy rules)
- Cloud Policies (cloud policies such as determining when to start virtual machines or scale out clusters).

When creating a template collection, you can use the default monitoring templates, compliance standards, or cloud templates supplied with Enterprise Manager or you can create your own. For more information, see Chapter 8, "Using Monitoring Templates."

To create a template collection:

1. Click the **Template Collections** tab. The Template Collection page displays.



Administration Groups and Template Collections

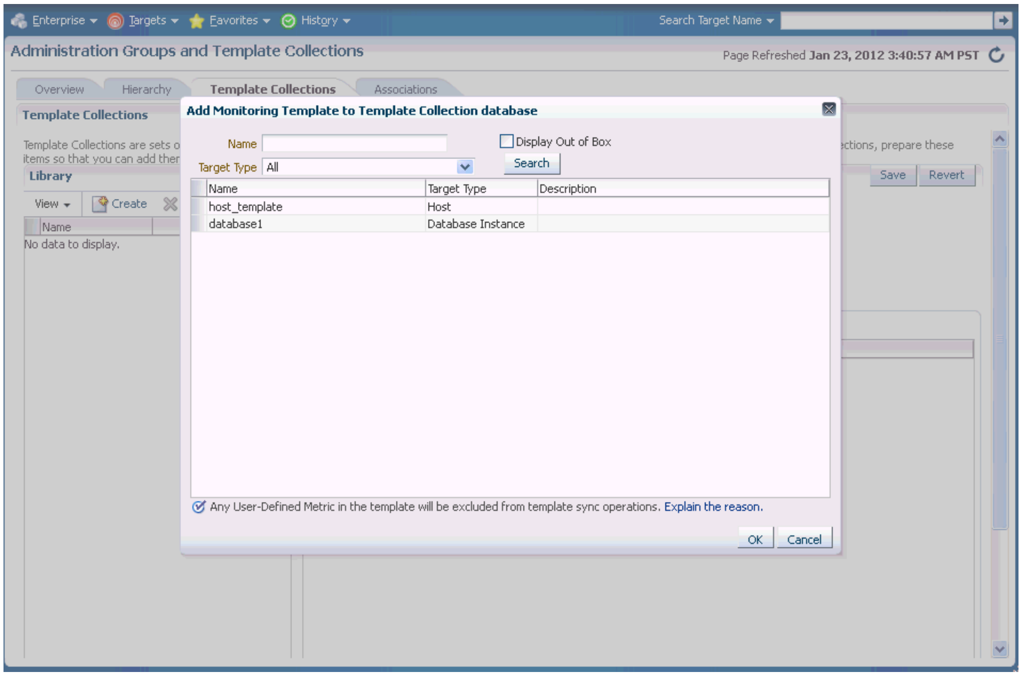
Page Refreshed **Aug 13, 2012 8:00:12 PM PDT**

Template Collections are sets of Monitoring Template, Compliance Standard and/or Cloud Policies that are applied to targets. So before you create Template Collections, prepare these items so that you can add them to your Template Collections

Name	Associations	Owner	Created At	Last Updated By	Last Updated At	Description

No data to display.

2. Click **Create**.
3. In the **Name** field, specify the template collection name.
4. Click the template collection member type you want to add (Monitoring Template, Compliance Standard, Cloud Polices). The requisite definition page appears.
5. Click **Add**. A list of available template entities appears.



Name	Target Type	Description
host_template	Host	
database1	Database Instance	

Any User-Defined Metric in the template will be excluded from template sync operations. Explain the reason.

6. Select the desired template entities you want added to the template collection.
7. Click **OK**.
8. Continue adding template entities (Monitoring Template, Compliance Standard, Cloud Policies) as required.
9. Click **Save**. The newly defined collection appears in the **Template Collections Library**.
10. To create another template collection, click **Create** and create and repeat steps two through eight. Repeat this process until you have created all required template collections.

> **Note:** When editing existing template collections, you can back out of any changes made during the editing session by clicking **Cancel**. This restores the template collection to its state when it was last saved.

7.3.1.3.1 Required Privileges To create a template collection, you must have the *Create Template Collection* resource privilege. To include a monitoring template into a template collection, you need at least *View* privilege on the specific monitoring template or *View Any Monitoring Template* privilege, which allows you to view any monitoring template and add it to the template collection. The following table summarizes privilege requirements for all Enterprise Manager operations related to template collection creation.

Enterprise Manager Operation	Minimum Privilege Requirement
Create administration group hierarchy.	Full Any Target Create Privilege Propagating Group
Create monitoring templates.	Create Monitoring Template

Enterprise Manager Operation	Minimum Privilege Requirement
Create template collection.	Create template collection (resource privilege). VIEW on the monitoring template to be added to the template collection or View any monitoring template (resource privilege).
Create compliance standards.	Create Compliance Entity No privileges are required to view compliance standards.
Create cloud policies.	Create Any Policy View Cloud Policy
Associate template collection with administration group.	VIEW on the specific template collection. Manage Target Metrics on the group.
Perform on-demand synchronization.	OPERATOR on the group or Manage Target Metrics.
Define global synchronization schedule.	Enterprise Manager Super Administrator privileges.
Set the value of target properties for a target (allows the target to "join" an administration group).	Configure Target on the specific target
Delete an administration group hierarchy.	Full Any Target

7.3.1.3.2 Corrective Action Credentials A corrective action is an automated task that is executed in response to a metric alert. When a corrective action is part of a monitoring template/template collection, the credentials required to execute the corrective action will vary depending on how the template is applied.

The two situations below illustrate the different credential requirements.

- *The corrective action is part of a monitoring template that is manually applied to a target.*

  When the corrective action runs, it can use one of the following:

  - The preferred credentials of the user who is applying the template

    or

  - The user-specified named credentials.

  The user selects the desired credential option during the template apply operation.

- *The corrective action is part of a monitoring template within a template collection that is associated with an administration group.*

  When the corrective action runs, the preferred credentials of the user who is associating the template collection with the administration group is used.

7.3.1.4 Associating Template Collections with Administration Groups

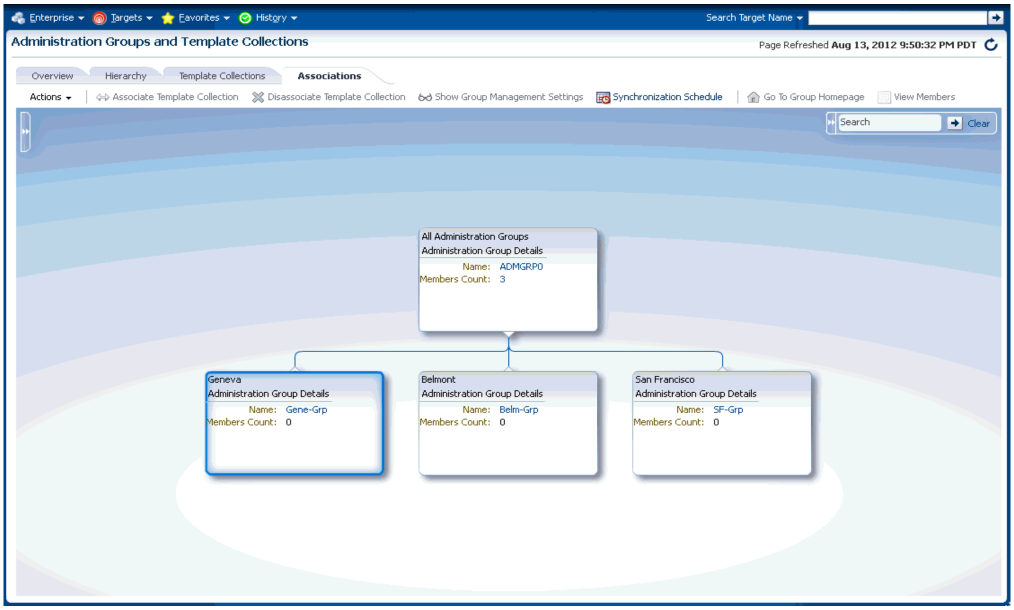
Once you have defined one or more template collections, you need to associate them to administration groups in the hierarchy. You can associate a template collection with one or more administration groups. As a rule, you should associate the template collection with the applicable administration group residing at the highest level in the hierarchy as the template collection will also be applied to targets joining any subgroup.

The **Associations** page displays the current administration group hierarchy diagram. Each administration group in the hierarchy can only be associated with one template collection.

Associating a Template Collection with an administration group

> **Note:** For users that do not have View privilege on all administration groups, you can also perform the association/disassociation operation from the Groups page (from the **Targets** menu, select **Groups**).

1. Click the **Associations** tab. The Associations page displays.



Administration Groups and Template Collections

Page Refreshed **Aug 13, 2012 9:50:32 PM PDT**

All Administration Groups
Administration Group Details
Name: ADMGRP0
Members Count: 3

Geneva
Administration Group Details
Name: Gene-Grp
Members Count: 0

Belmont
Administration Group Details
Name: Belm-Grp
Members Count: 0

San Francisco
Administration Group Details
Name: SF-Grp
Members Count: 0

2. Select the desired administration group in the hierarchy.
3. Click **Associate Template Collection**. The **Choose a Template Collection** dialog displays.
4. Choose the desired template collection and click **Select**. The list of targets affected by this operation is displayed. Confirm or discard the operation.

> **Note:** All sub-nodes in the hierarchy will inherit the selected template collection.

5. Repeat steps 1-3 until template collections have been associated with the desired groups.

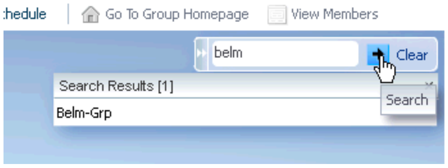
> **Note:** The target privileges of the administrator who performs the association will be used when Enterprise Manager applies the template to the group. The administrator needs at least Manage Target Metrics privileges on the group.

Note: Settings from monitoring templates applied at lower levels in the hierarchy override settings inherited from higher levels. This does not apply to compliance standards or cloud policies.

Searching for Administration Groups

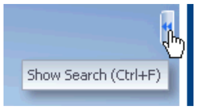
While the administration group UI is easy to navigate, there may be cases where the administration group hierarchy is inordinately large, thus making it difficult to find individual groups. At the upper right corner of the Associations page is a search function that greatly simplifies finding groups in a large hierarchy.

Figure 7–1 Administration Group Search Dialog

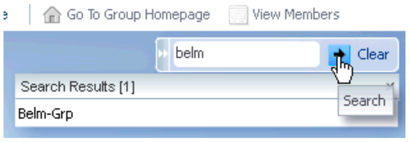


To search for a specific administration group:

1. If not already displayed, expand the Search interface.

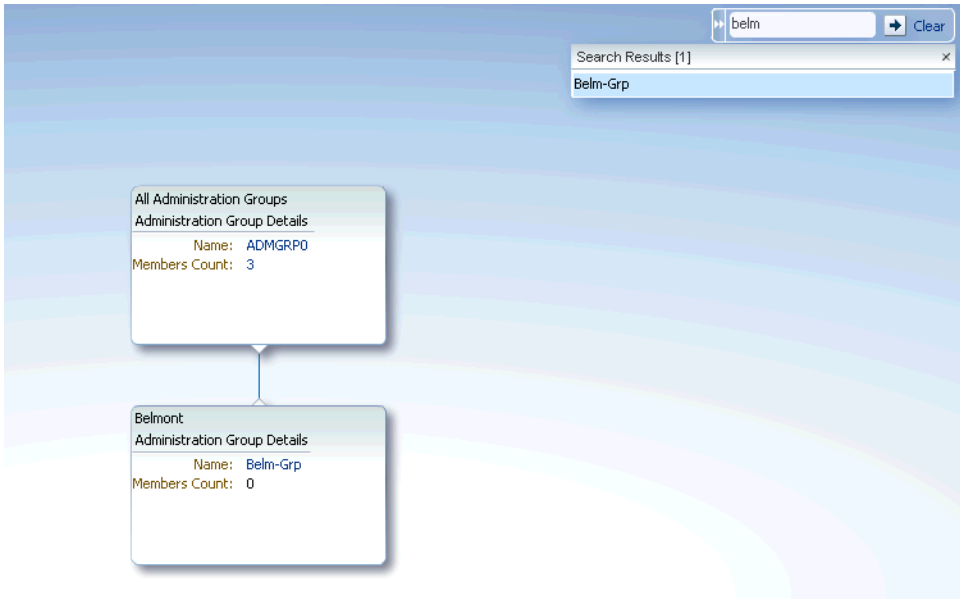


2. Enter either a full or partial group name and click **Search**.



As shown in the graphic, the search results display a list of administration groups that match the search criteria. You can then choose an administration group from the list by double-clicking on the entry. The administration group hierarchy will then display a vertical slice (subset) of the administration group hierarchy from the root node to the group you selected.

Figure 7–2 Administration Group Search: Graphical Display



To restore the full administration group hierarchy, click **Clear**.

Group Names and Searches

In order to perform effective searches for specific administration groups, it is helpful to know how Enterprise Manager constructs an administration group name: Enterprise Manger uses the administration group criteria to generate names. For example, you have an administration group with the following criteria:

- Lifecycle Status: Development or Mission Critical
- Department: DEV
- Line of Business: Finance or HR
- Location: Bangalore

Enterprise Manager assembles a group name based on truncated abbreviations. In this example, the generated administration group name is *DC-DEV-FH-Bang-Grp*

As you are building the hierarchy, you can change the abbreviation associated with each value (this is the Short Value column next to the property value in the Hierarchy Nodes table. Hence, you can specify a short value and Enterprise Manager will use that value when constructing new names for any subgroups created.

During the design phase of an administration group, you have the option of specifying a custom name. However, if there is large number of groups, it is easier to allow Enterprise Manager to generate unique names.

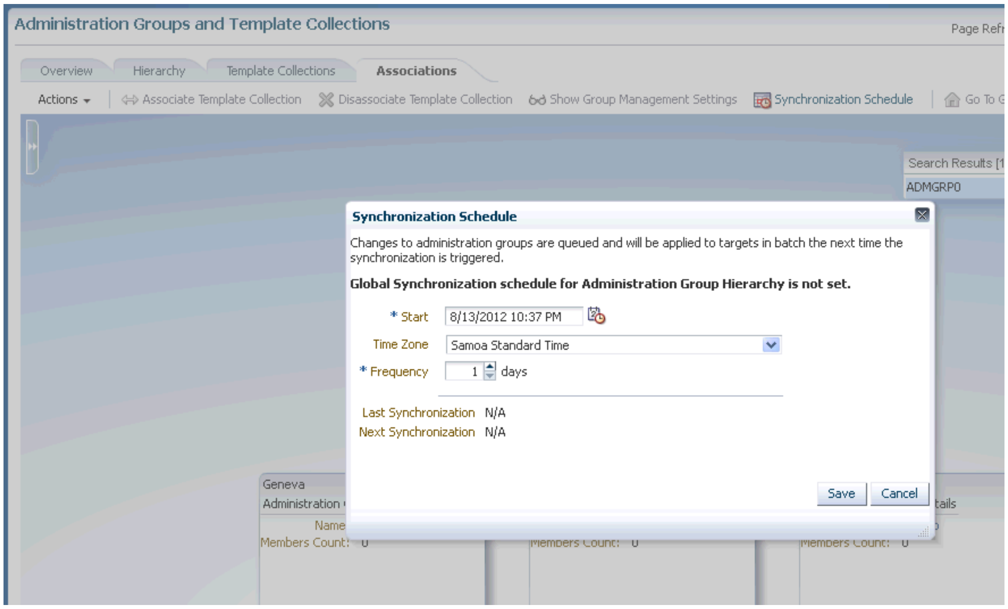
Setting the Global Synchronization Schedule

In order to apply the template collection/administration group association, you must set up a global synchronization schedule. This schedule is used to perform synchronization operations, such as applying templates to targets in administration groups. If no synchronization schedule is set up, when a target joins an administration group, Enterprise Manager will auto-apply the associated template. However, if there are changes to the template later on, then Enterprise Manager will only apply these based on synchronization schedule, otherwise these operations are pending.When there are any pending synchronization operations, they will be scheduled on the next available date based on the synchronization schedule.

> **Important:** You **must** set the synchronization schedule as there is no default setting. You can specify a non-peak time such as weekends.

To set up the synchronization schedule:

1. Click **Synchronization Schedule**. The Synchronization Schedule dialog displays.



Synchronization Schedule

Changes to administration groups are queued and will be applied to targets in batch the next time the synchronization is triggered.

Global Synchronization schedule for Administration Group Hierarchy is not set.

* Start: 8/13/2012 10:37 PM

Time Zone: Samoa Standard Time

* Frequency: 1 days

Last Synchronization: N/A

Next Synchronization: N/A

2. Click **Edit** and then choose a date and time you want any pending sync operations (For example, template apply operations) to occur. By default, the current date and time is shown.

> **Note:** You can specify a start date for synchronization operations and interval in days. Whenever there are any pending sync operations, then they will be scheduled on the next available date based on this schedule.

3. Click **Save**.

When Template Collection Synchronization Occurs

The following table summarizes when Template Collection Synchronization operations (such as apply operations) occur on targets in administration groups.

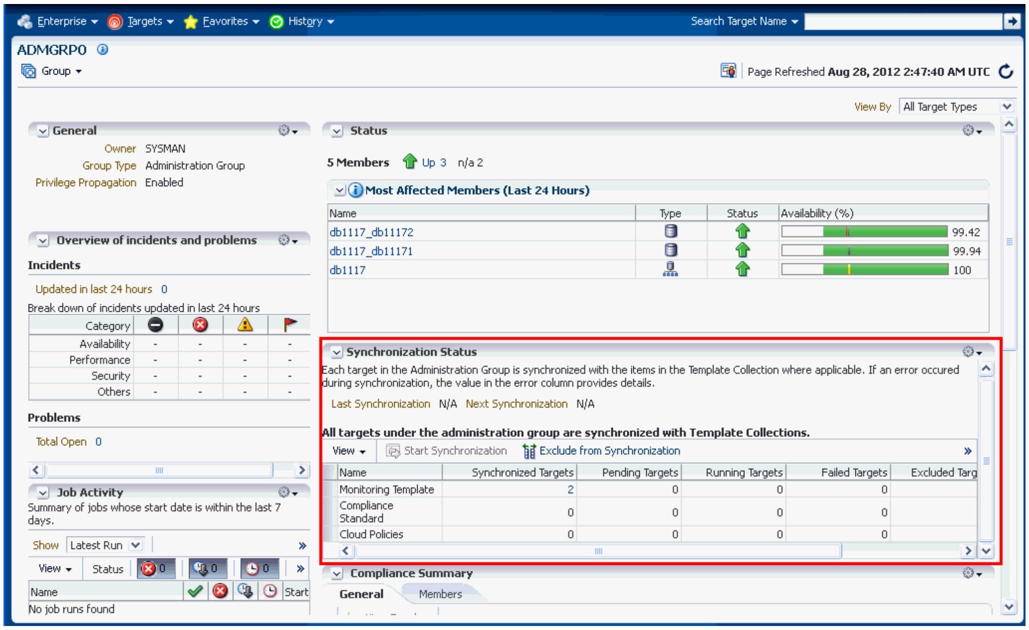
Action	When Synchronization Occurs
Target is added to an administration group (by setting its target properties)	Immediate upon joining the administration group.
Template collection is associated with the administration group.	Targets in an administration group will be synchronized based on next scheduled date in global Synchronization Schedule.

Action	When Synchronization Occurs
Changes are made to any of the templates in the template collection.	Targets in an administration group will be synchronized based on the next scheduled date in global Synchronization Schedule.
Target is removed from an administration group (by changing its target properties).	No change in target's monitoring settings. Compliance Standards and Cloud Policies will be disassociated with the target. Immediate synchronization operation occurs.
Template collection is disassociated with administration group.	No change in target's monitoring settings for all the targets in the administration group. Compliance Standards and Cloud Policies will be disassociated with the target. Targets under the administration group will be synchronized based on next schedule date in Global Synchronization Schedule.
User performs an on-demand synchronization by clicking on the **Start Synchronization** button in the **Synchronization Status** region in the administration group's homepage.	Immediate synchronization operation occurs.

Viewing Synchronization Status

You can check the current synchronization status for a specific administration group directly from the group's homepage.

1. Select an administration group in the hierarchy.
2. Click **Goto Group Homepage**.
3. From the **Synchronization Status** region, you can view the status of the monitoring template, compliance standard, and/or cloud policies synchronization (In Sync, Pending, or Failed).



ADMGRP0

Page Refreshed **Aug 28, 2012 2:47:40 AM UTC**

Owner SYSMAN
Group Type Administration Group
Privilege Propagation Enabled

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

Summary of jobs whose start date is within the last 7 days.

Name	✓	⊗			Start
No job runs found					

5 Members Up 3 n/a 2

Name	Type	Status	Availability (%)
db1117_db11172		↑	99.42
db1117_db11171		↑	99.94
db1117		↑	100

Each target in the Administration Group is synchronized with the items in the Template Collection where applicable. If an error occured during synchronization, the value in the error column provides details.

Last Synchronization N/A Next Synchronization N/A

All targets under the administration group are synchronized with Template Collections.

Name	Synchronized Targets	Pending Targets	Running Targets	Failed Targets	Excluded Targ
Monitoring Template	2	0	0	0	
Compliance Standard	0	0	0	0	
Cloud Policies	0	0	0	0	

You can initiate an immediate synchronization by clicking **Start Synchronization**.

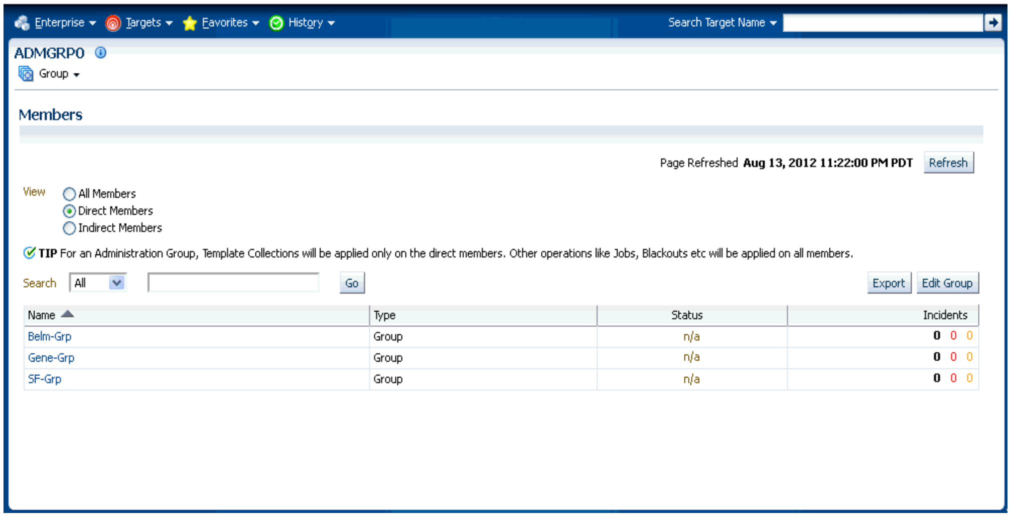
Group Member Type and Synchronization

There are two types of administration group member targets: Direct and Indirect

- Direct Members: Group members whose target properties match the administration group criteria. Monitoring settings, compliance standards, cloud policies from the associated template collection are applied to direct members.
- Indirect Members: Indirect members are targets whose target properties DO NOT match administration group criteria. However, they have been added to the administration group because their parent target are direct members of the administration group. These targets are categorized as aggregate targets because they have other member targets. When such targets are added to a group (administration group or other types of groups), all members of the aggregate target are also added to the group. An example of an aggregate target is Oracle WebLogic Server. If that is added to a group, then all Application Deployment targets on it are also pulled into the group. Indirect group members will NOT be part of any template apply/sync operations.

Only direct members are represented in the targets count in the Synchronization Status region.

1. From the hierarchy diagram, click on a group name to access the group's home page. You can also access this information from **All Targets** groups page.
2. From the **Group** menu, select **Members**. The Members page displays.



Members

Page Refreshed **Aug 13, 2012 11:22:00 PM PDT** Refresh

View
○ All Members
● Direct Members
○ Indirect Members

✓ **TIP** For an Administration Group, Template Collections will be applied only on the direct members. Other operations like Jobs, Blackouts etc will be applied on all members.

Search All ▾ Go Export Edit Group

Name ▲	Type	Status	Incidents
Belm-Grp	Group	n/a	0 0 0
Gene-Grp	Group	n/a	0 0 0
SF-Grp	Group	n/a	0 0 0

System Targets and Administration Groups

If a system target gets added to an administration group because it matches group criteria, then the system target and its constituent members are also added. However, for template apply purposes, it will only operate on the direct members that also match the administration group criteria. Template apply operations will not occur on member targets whose target properties do not match administration group criteria. All other group operations, such as jobs and blackouts, will apply on all members, both direct and indirect.

Disassociating a Template Collection from a Group

To disassociate a template collection from an administration group.

1. From the **Setup** menu, select **Add Target** and then **Administration Groups**. The Administration Group home page displays.

2. Click on the **Associations** tab to view the administration group hierarchy diagram.
3. From the hierarchy diagram, select the administration group with the template collection you wish to remove. If necessary, use the **Search** option to locate the administration group.
4. Click **Disassociate Template Collection**. The number of targets affected by this operation is displayed. Click **Continue** or **Cancel**.

The template collection is immediately removed. See "When Template Collection Synchronization Occurs" on page 7-22 for more information.

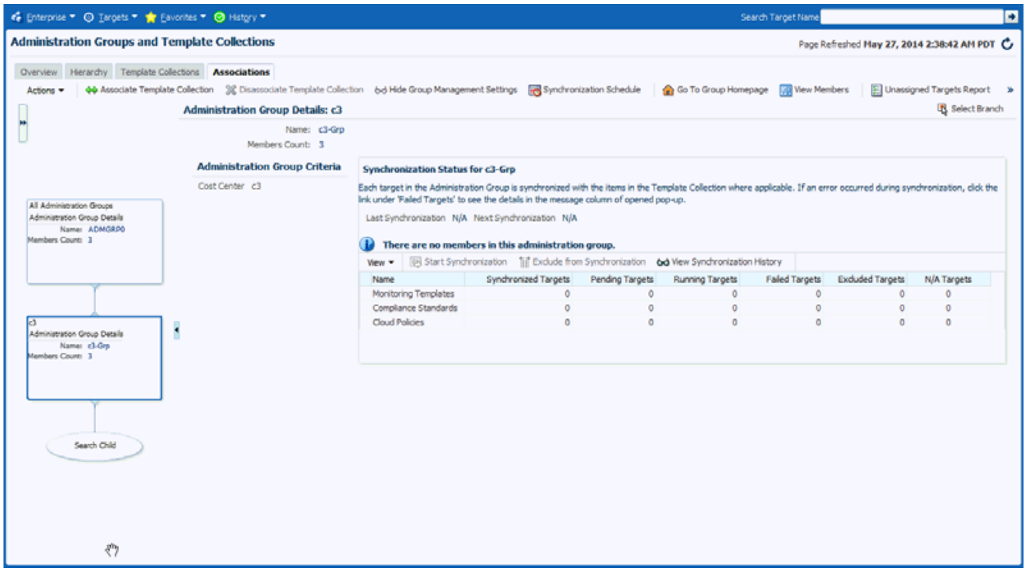
Viewing Aggregate (Group Management) Settings

For any administration group, you can easily view what template collection components (monitoring templates, compliance standards, and/or cloud policies) are associated with individual group members.

> **Note:** For monitoring templates, the settings for a target could be a union of two or more monitoring templates from different template collections.

1. From the **Setup** menu, select **Add Target** and then **Administration Groups**. The Administration Group home page displays.
2. Click on the **Associations** tab to view the administration group hierarchy diagram.
3. From the hierarchy diagram, select the desired administration group.
4. Click **Show Group Management Settings**.

   The **Administration Group Details** page displays.


Enterprise
Targets
Favorites
History
Search Target Name
Administration Groups and Template Collections
Page Refreshed May 27, 2014 2:38:42 AM PDT
Overview
Hierarchy
Template Collections
Associations
Actions
Associate Template Collection
Disassociate Template Collection
Hide Group Management Settings
Synchronization Schedule
Go To Group Homepage
View Members
Unassigned Targets Report
Select Branch
All Administration Groups
Administration Group Details
Name: ADMGRP0
Members Count: 3
c3
Administration Group Details
Name: c3-Grp
Members Count: 3
Search Child
View
Start Synchronization
Exclude from Synchronization
View Synchronization History

Administration Group Details: c3

Name: c3-Grp

Members Count: 3

Administration Group Criteria

Cost Center c3

Synchronization Status for c3-Grp

Each target in the Administration Group is synchronized with the items in the Template Collection where applicable. If an error occurred during synchronization, click the link under 'Failed Targets' to see the details in the message column of opened pop-up.

Last Synchronization N/A Next Synchronization N/A

There are no members in this administration group.

Name	Synchronized Targets	Pending Targets	Running Targets	Failed Targets	Excluded Targets	N/A Targets
Monitoring Templates	0	0	0	0	0	0
Compliance Standards	0	0	0	0	0	0
Cloud Policies	0	0	0	0	0	0

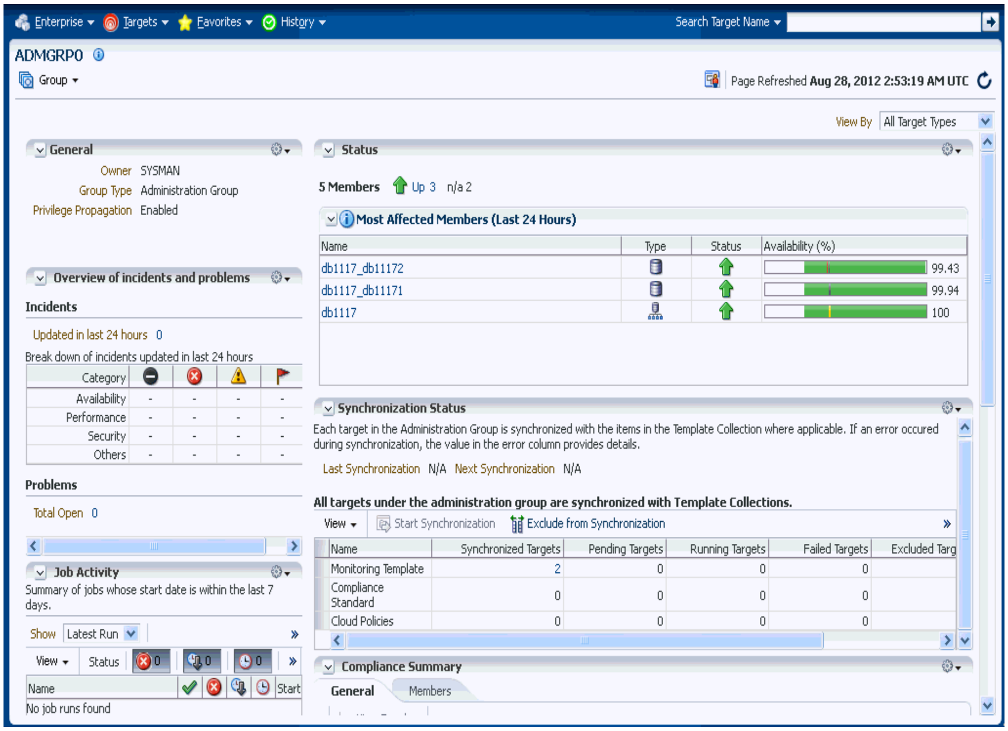
This page displays all aggregate settings for monitoring templates, compliance standards and cloud policies that will be applied to members of the selected administration group (listed by target type). The page also displays the synchronization status of group members.

To can change the display to show a different branch of the administration group hierarchy, click **Select Branch** at the upper-right area of the page. This function lets you display hierarchy branches by choosing different target property values

Viewing the Administration Group Homepage

Like regular groups, each administration group has an associated group homepage providing a comprehensive overview of group member status and/or activity such as synchronization status, details of the Associated Template Collection for the group selected in hierarchy viewer, job activity, or critical patch advisories. To view administration group home pages:

1. From the hierarchy diagram, select an administration group.
2. Click **Goto Group Homepage.** The homepage for that particular administration group displays.



Page Refreshed **Aug 28, 2012 2:53:19 AM UTC**

Owner SYSMAN
Group Type Administration Group
Privilege Propagation Enabled

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

Summary of jobs whose start date is within the last 7 days.

Show Latest Run

View Status ⊗ 0 0 0

Name	✓	⊗			Start
No job runs found					

5 Members Up 3 n/a 2

Most Affected Members (Last 24 Hours)

Name	Type	Status	Availability (%)
db1117_db11172		↑	99.43
db1117_db11171		↑	99.94
db1117		↑	100

Each target in the Administration Group is synchronized with the items in the Template Collection where applicable. If an error occured during synchronization, the value in the error column provides details.

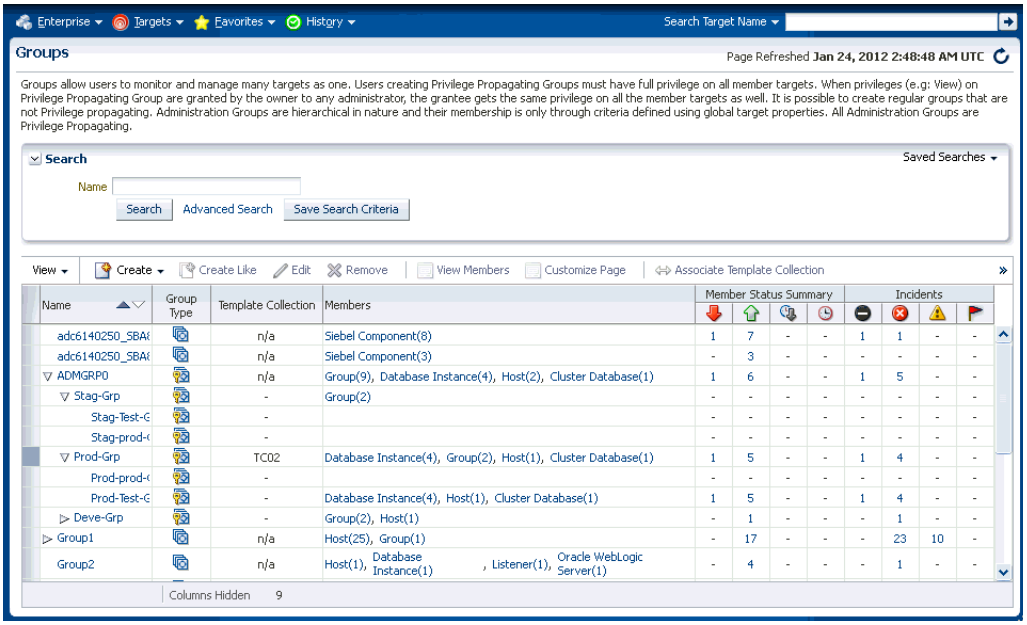
Last Synchronization N/A Next Synchronization N/A

All targets under the administration group are synchronized with Template Collections.

View Start Synchronization Exclude from Synchronization

Name	Synchronized Targets	Pending Targets	Running Targets	Failed Targets	Excluded Targ
Monitoring Template	2	0	0	0	
Compliance Standard	0	0	0	0	
Cloud Policies	0	0	0	0	

Alternatively, from the Enterprise Manger **Targets** menu, choose **Groups**. From the table, you can expand the group hierarchy.



Groups

Page Refreshed **Jan 24, 2012 2:48:48 AM UTC**

Groups allow users to monitor and manage many targets as one. Users creating Privilege Propagating Groups must have full privilege on all member targets. When privileges (e.g: View) on Privilege Propagating Group are granted by the owner to any administrator, the grantee gets the same privilege on all the member targets as well. It is possible to create regular groups that are not Privilege propagating. Administration Groups are hierarchical in nature and their membership is only through criteria defined using global target properties. All Administration Groups are Privilege Propagating.

Search

Name

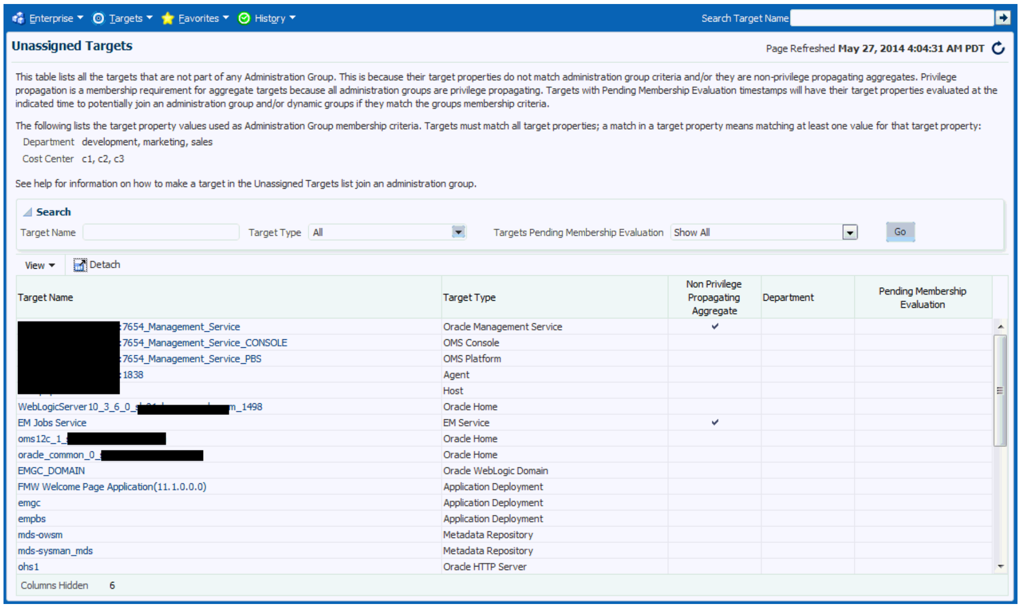
Name	Group Type	Template Collection	Members	Member Status Summary				Incidents			
				↓	↑	⏬	🕒	⛔	⊗	⚠	🚩
adc6140250_SBA(		n/a	Siebel Component(8)	1	7	-	-	1	1	-	-
adc6140250_SBA(		n/a	Siebel Component(3)	-	3	-	-	-	-	-	-
▽ ADMGRP0		n/a	Group(9), Database Instance(4), Host(2), Cluster Database(1)	1	6	-	-	1	5	-	-
▽ Stag-Grp		-	Group(2)	-	-	-	-	-	-	-	-
Stag-Test-G		-		-	-	-	-	-	-	-	-
Stag-prod-(		-		-	-	-	-	-	-	-	-
▽ Prod-Grp		TC02	Database Instance(4), Group(2), Host(1), Cluster Database(1)	1	5	-	-	1	4	-	-
Prod-prod-(		-		-	-	-	-	-	-	-	-
Prod-Test-G		-	Database Instance(4), Host(1), Cluster Database(1)	1	5	-	-	1	4	-	-
▷ Deve-Grp		-	Group(2), Host(1)	-	1	-	-	-	1	-	-
▷ Group1		n/a	Host(25), Group(1)	-	17	-	-	-	23	10	-
Group2		n/a	Host(1), Database Instance(1) , Listener(1), Oracle WebLogic Server(1)	-	4	-	-	-	1	-	-

Columns Hidden 9

Identifying Targets Not Part of Any Administration Group

From the **Associations** page, you can determine which targets do not belong to any administration group by generating an *Unassigned Targets Report*.

1. From the **Actions** menu, select **Unassigned Targets Report**. The report lists all the targets that are not part of any administration group. The values for the target properties defining the administration groups hierarchy are shown.



Unassigned Targets

Page Refreshed **May 27, 2014 4:04:31 AM PDT**

This table lists all the targets that are not part of any Administration Group. This is because their target properties do not match administration group criteria and/or they are non-privilege propagating aggregates. Privilege propagation is a membership requirement for aggregate targets because all administration groups are privilege propagating. Targets with Pending Membership Evaluation timestamps will have their target properties evaluated at the indicated time to potentially join an administration group and/or dynamic groups if they match the groups membership criteria.

The following lists the target property values used as Administration Group membership criteria. Targets must match all target properties; a match in a target property means matching at least one value for that target property:

Department development, marketing, sales
Cost Center c1, c2, c3

See help for information on how to make a target in the Unassigned Targets list join an administration group.

Search

Target Name

Target Type All

Targets Pending Membership Evaluation Show All

Target Name	Target Type	Non Privilege Propagating Aggregate	Department	Pending Membership Evaluation
[redacted]7654_Management_Service	Oracle Management Service	✓		
[redacted]7654_Management_Service_CONSOLE	OMS Console			
[redacted]7654_Management_Service_PBS	OMS Platform			
[redacted]1838	Agent			
[redacted]	Host			
WebLogicServer10_3_6_0_[redacted]m_1498	Oracle Home			
EM Jobs Service	EM Service	✓		
oms12c_1_[redacted]	Oracle Home			
oracle_common_0_[redacted]	Oracle Home			
EMGC_DOMAIN	Oracle WebLogic Domain			
FMW Welcome Page Application(11.1.0.0.0)	Application Deployment			
emgc	Application Deployment			
empbs	Application Deployment			
mds-owsm	Metadata Repository			
mds-sysman_mds	Metadata Repository			
ohs1	Oracle HTTP Server			

Columns Hidden 6

2. From the **View** menu, choose the customization options to display only the desired information.

Note: The **Non-Privilege Propagating Aggregate** column indicates whether a target is a non-privilege propagating aggregate. This type of target cannot be added to an administration group, which are by design privilege propagating. For this reason, any aggregate target added to administration group must also be privilege propagating. To make an aggregate target privilege propagating, use the EM CLI verb *modify_system* with *-privilege_propagation=true option*. For more information see the Enterprise Manager Command Line Reference.

On this page, you can review the list to see if there any targets that need to be added to the administration group. Click on the target names shown in this page to access the target's **Edit Target Properties** page where you can change the target property values. After making the requisite changes and clicking OK, you are returned to the **Unassigned Targets** page.

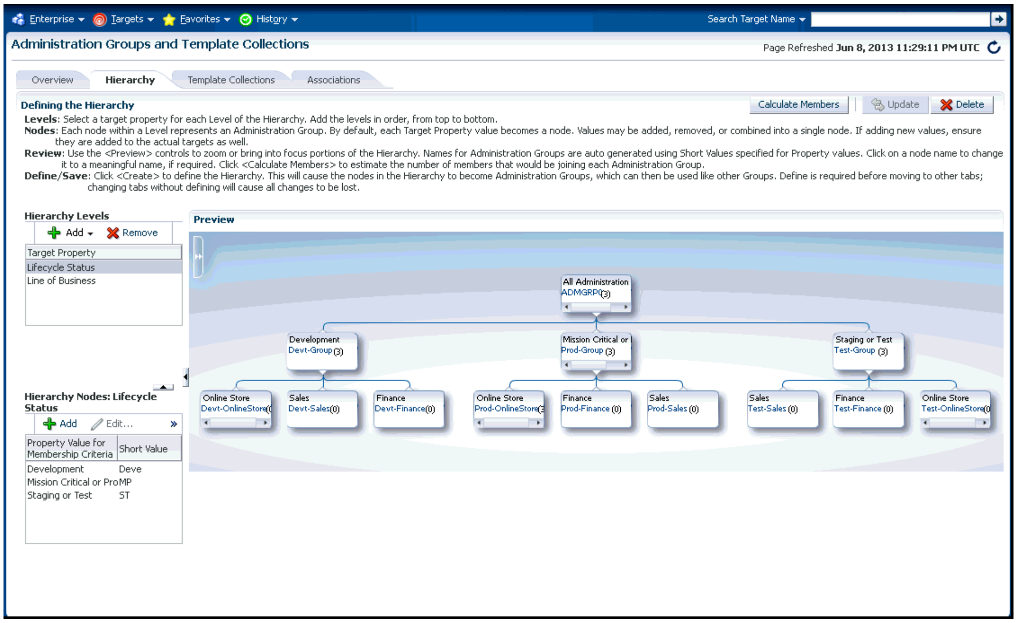
For information on changing target properties, see "Planning" on page 7-3.

3. Click your browser *back* button to return to the **Administration Groups and Template Collections** homepage.

7.4 Changing the Administration Group Hierarchy

Organizations are rarely static--new lines of business may be added or perhaps groups are reorganized due to organizational expansion. To accommodate these changes, you may need to make changes to the existing administration group hierarchy.

Beginning with Enterprise Manager 12*c* Release 12.1.0.3, you can change the administration group hierarchy without having to rebuild the entire hierarchy. You can easily perform administration group alterations such as adding more groups to each hierarchy level, merging two or more groups, or adding/deleting entire hierarchy levels. All of these operations can be performed from the Hierarchy page.



Administration Groups and Template Collections

Page Refreshed **Jun 8, 2013 11:29:11 PM UTC**

Defining the Hierarchy

Levels: Select a target property for each Level of the Hierarchy. Add the levels in order, from top to bottom.
Nodes: Each node within a Level represents an Administration Group. By default, each Target Property value becomes a node. Values may be added, removed, or combined into a single node. If adding new values, ensure they are added to the actual targets as well.
Review: Use the <Preview> controls to zoom or bring into focus portions of the Hierarchy. Names for Administration Groups are auto generated using Short Values specified for Property values. Click on a node name to change it to a meaningful name, if required. Click <Calculate Members> to estimate the number of members that would be joining each Administration Group.
Define/Save: Click <Create> to define the Hierarchy. This will cause the nodes in the Hierarchy to become Administration Groups, which can then be used like other Groups. Define is required before moving to other tabs; changing tabs without defining will cause all changes to be lost.

Hierarchy Levels

Target Property
Lifecycle Status
Line of Business

Hierarchy Nodes: Lifecycle Status

Property Value for Membership Criteria	Short Value
Development	Deve
Mission Critical or Pro	MP
Staging or Test	ST

Important: After making any change to the administration group hierarchy, click **Update** to save your changes.

7.4.1 Adding a New Hierarchy Level

Adding a new hierarchy level equates to adding a new target property to the administration group criteria. For this reason, you must set the value of this target property for all your targets in order for them to continue to be part of the administration group hierarchy. Any new target property added/hierarchy level added will always be added as the bottom-most level of the hierarchy. You cannot insert a new level between levels.

To insert a hierarchy level, you must remove a hierarchy level, then add the levels you want. Think carefully before removing a hierarchy level as removing a level will result in the deletion of groups corresponding to that hierarchy level.

See "Adding a Hierarchy Level" on page 7-12 for step-by-step instructions on adding a new level.

7.4.2 Removing a Hierarchy Level

Removing a hierarchy level equates to deleting a target property, which in turn causes groups at that level to be deleted. For this reason, think carefully about the groups that will be removed when you remove the hierarchy level, especially if those groups are used in other functional areas of Enterprise Manager.

To remove a hierarchy level:

1. On the **Administration Group** page, click the **Hierarchy** tab.
2. From the **Hierarchy Levels** table, select a hierarchy level and click **Remove**
3. Click **Update** to save your changes.

If any of those groups have an associated template collection, then the monitoring settings of the subgroups of the deleted group will be impacted since the subgroups obtained monitoring settings from the associated template collection. You may need to review the remaining template collections and re-associate the template collection with the appropriate administration group.

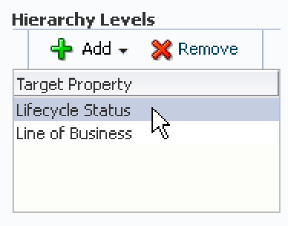
7.4.3 Merging Administration Groups

If you want to merge two or more administration groups, you merge their corresponding target property criteria in the administration group hierarchy definition. The group merge operation consists of retaining one of the groups to be merged and then moving over the targets from the other groups into the group that is retained. Once the targets have been moved, the other groups will be deleted.

You choose which group is retained by choosing its corresponding target property value. The group(s) containing the selected target property value as part of its criteria is retained. If the retained target property criteria corresponds to multiple groups, i.e. group containing subgroups, the movement of targets will actually occur at the lowest level administration groups since the targets only reside in the lowest level administration groups. The upper-level administration groups' criteria will be updated to include the criteria of the other groups that have been merged into it.

To merge groups:

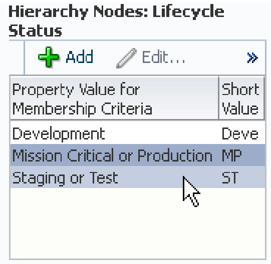
1. Select a target property from the list of chosen properties in the **Hierarchy Levels** table. You choose the target property corresponding to the groups you want to merge.



Target Property
Lifecycle Status
Line of Business

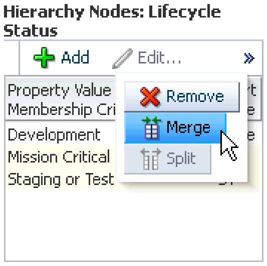
For example, let us assume you want to merge <Devt-Group> with <Test or Stage Group>. In the hierarchy, this corresponds to target property Lifecycle Status. The associated property values are displayed.

2. Select two or more property values corresponding to the groups you would like to merge by holding down the *Shift* or *CTRL* key and clicking on the desired values.

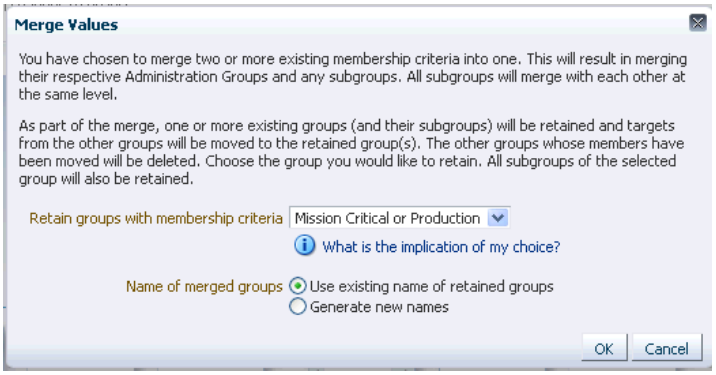


Property Value for Membership Criteria	Short Value
Development	Deve
Mission Critical or Production	MP
Staging or Test	ST

3. Click **Merge**.



The Merge Values dialog displays.



You have chosen to merge two or more existing membership criteria into one. This will result in merging their respective Administration Groups and any subgroups. All subgroups will merge with each other at the same level.

As part of the merge, one or more existing groups (and their subgroups) will be retained and targets from the other groups will be moved to the retained group(s). The other groups whose members have been moved will be deleted. Choose the group you would like to retain. All subgroups of the selected group will also be retained.

Retain groups with membership criteria: Mission Critical or Production

What is the implication of my choice?

Name of merged groups: ● Use existing name of retained groups ○ Generate new names

Again, by merging membership criteria (target properties), you are merging administration groups and their respective subgroups. You choose the administration group to be retained. The other groups will be merged into that group.

4. Choose the group you wish to retain and specify whether you want to use the existing name of the retained group or specify a new name.

> **Important:** When deciding which group to retain, consider choosing the group that is used in most group operations such as incident rule sets, system dashboard, or roles. These groups will be retained and the members of the other merged groups will join the retained groups. After the merge, group operations on the retained groups will also now apply to the members from the other merged groups. Doing so minimizes the impact of the merge.

5. Click **OK** to merge the groups.
6. Click **Update** to save the new hierarchy.

Example

Your administration group consists of the following:

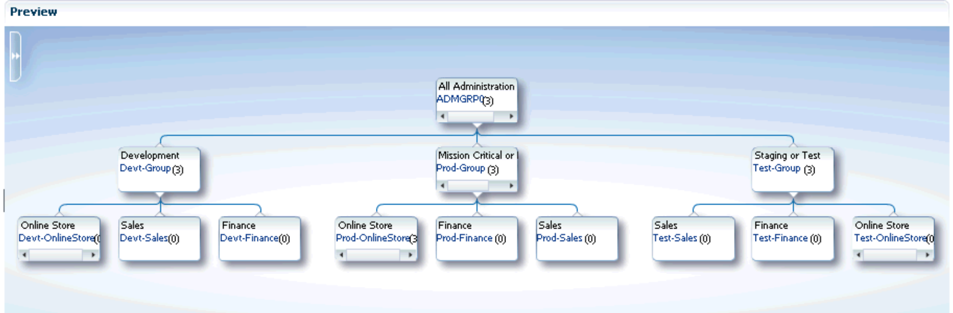
Hierarchy Levels

- Lifecycle Status
- Line of Business

Hierarchy Nodes

- *Lifecycle Status*
  - Development
  - Mission Critical or Production
  - Staging or Test
- *Line of Business*
  - Online Store
  - Sales
  - Finance

The following graphic shows the administration group hierarchy.



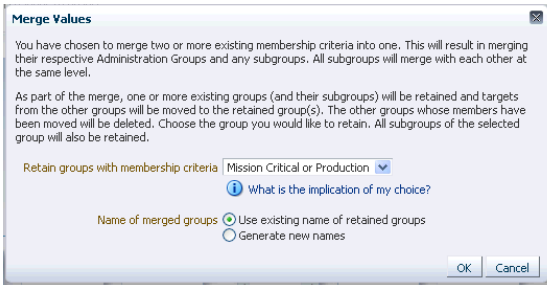
You decide that you want to merge the *Mission Critical or Production* group with the *Staging or Test* group because they have the same monitoring settings.

Choose Lifecycle Status from the **Hierarchy Levels** table.

From the **Hierarchy Nodes** table, choose both *Mission Critical or Production* and *Staging or Test*.

Select **Merge** from the **Hierarchy Nodes** menu.

The **Merge Values** dialog displays. In this case, you want to keep original name (*Mission Critical or Production*) of the retained group.



Merge Values

You have chosen to merge two or more existing membership criteria into one. This will result in merging their respective Administration Groups and any subgroups. All subgroups will merge with each other at the same level.

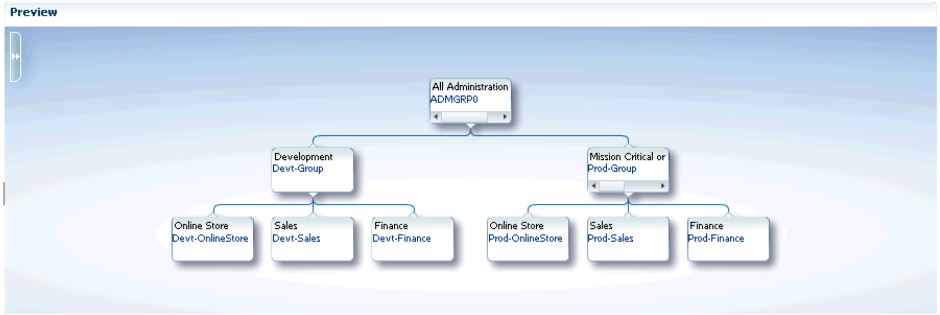
As part of the merge, one or more existing groups (and their subgroups) will be retained and targets from the other groups will be moved to the retained group(s). The other groups whose members have been moved will be deleted. Choose the group you would like to retain. All subgroups of the selected group will also be retained.

Retain groups with membership criteria: Mission Critical or Production

What is the implication of my choice?

Name of merged groups: ● Use existing name of retained groups ○ Generate new names

After clicking **OK** to complete the merge, the resulting administration group hierarchy is displayed. All targets from *Test-Sales* group moved to the *Prod-Sales* group. The *Test-Sales* group was deleted. All targets from the *Test-Finance* group moved to the *Prod-Finance* group. The *Test-Finance* group got deleted.



Click **Update** to save the changes.

7.4.4 Removing Administration Groups

You can completely remove an administration group hierarchy or just individual administration groups from the hierarchy. Deleting an administration group will not delete targets or template collections, but it will remove associations. Any stored membership criteria is removed. When you delete an administration group, any stored membership criteria is removed.

To remove the entire administration group hierarchy:

1. From the **Setup** menu, select **Add Target**, then select **Administration Groups**.
2. Click on the **Hierarchy** tab.
3. Click **Delete**.

To remove individual administration groups from the hierarchy:

1. From the **Setup** menu, choose **Add Target**, then select **Administration Groups**.
2. Click on the **Hierarchy** tab.
3. From the **Hierarchy Levels** table, choose the target property that corresponds to the hierarchy level containing the administration group to be removed.
4. From the **Hierarchy Nodes** table, select the administration group (**Property Value for Membership Criteria**) to be removed.
5. Choose **Remove** from the drop-down menu.
6. Click **Update**.

8

Using Monitoring Templates

Monitoring templates simplify the task of setting up monitoring for large numbers of targets by allowing you to specify the monitoring and Metric and Collection Settings once and applying them to many groups of targets as often as needed.

This chapter covers the following topics:

8.1 About Monitoring Templates

Monitoring templates let you standardize monitoring settings across your enterprise by allowing you to specify the monitoring settings once and apply them to your monitored targets. You can save, edit, and apply these templates across one or more targets or groups. A monitoring template is specified for a particular target type and can only be applied to targets of the same type. For example, you can define one monitoring template for test databases and another monitoring template for production databases.

A monitoring template defines all Enterprise Manager parameters you would normally set to monitor a target, such as:

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

Once a monitoring template is defined, it can be applied to your targets. This can be done either manually through the Enterprise Manager console, via the command line interface (EM CLI), or automatically using template collections. See "Defining Template Collections" on page 7-15 for more information. For any target, you can preserve custom monitoring settings by specifying metric settings that can never be overwritten by a template.

Oracle-Certified Templates

In addition to templates that you create, there are also Oracle-certified templates. These templates contain a specific set of metrics for a specific purpose. The purpose of the template is indicated in the description associated with the template.

Example: The template called *Oracle Certified - Enable AQ Metrics for SI Database* contains metrics related to Advanced Queueing for single instance databases. You can use this Oracle-certified template if you want to use the AQ metrics. Or you can copy the metric settings into your own template.

8.2 Definition of a Monitoring Template

A monitoring template defines all Enterprise Manager parameters you would normally set to monitor a target. A template specifies:

- **Name**: A unique identifier for the template. The template name must be globally unique across all templates defined within Enterprise Manager.
- **Description**: Optional text describing the purpose of the template.
- **Target Type**: Target type to which the template applies.
- **Owner**: Enterprise Manager administrator who created the template.
- **Metrics**: Metrics for the target type. A monitoring template allows you to specify a subset of all metrics for a target type. With these metrics, you can specify thresholds, collection schedules and corrective actions.
- **Other Collected Items**: Additional collected information (non-metric) about your environment.

8.3 Default Templates (Auto Apply Templates)

Under certain circumstances, Oracle's out-of-box monitoring settings may not be appropriate for targets in your monitored environment. Incompatible Metric and Collection Settings for specific target types can result in unwanted/unintended alert notifications. Enterprise Manager allows you to set default monitoring templates that are automatically applied to newly added targets, thus allowing you to apply monitoring settings that are appropriate for your monitored environment.

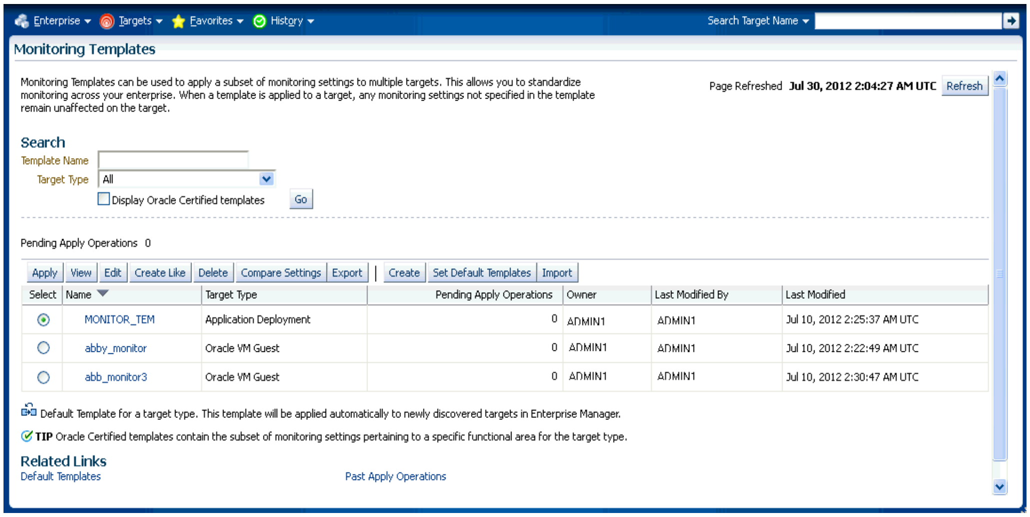
> **Note:** Super Administrator privileges are required to define default monitoring templates.

8.4 Viewing a List of Monitoring Templates

To view a list of all Monitoring Templates, from the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates**.

The Monitoring Templates page displays all the out-of-box templates and the templates for which you have has at least VIEW privilege on. Enterprise Manager Super Administrators can view all templates.

Figure 8–1 Monitoring Templates



Monitoring Templates

Monitoring Templates can be used to apply a subset of monitoring settings to multiple targets. This allows you to standardize monitoring across your enterprise. When a template is applied to a target, any monitoring settings not specified in the template remain unaffected on the target.

Page Refreshed **Jul 30, 2012 2:04:27 AM UTC**

Search

Template Name

Target Type All

□ Display Oracle Certified templates

Pending Apply Operations 0

Select	Name	Target Type	Pending Apply Operations	Owner	Last Modified By	Last Modified
●	MONITOR_TEM	Application Deployment	0	ADMIN1	ADMIN1	Jul 10, 2012 2:25:37 AM UTC
○	abby_monitor	Oracle VM Guest	0	ADMIN1	ADMIN1	Jul 10, 2012 2:22:49 AM UTC
○	abb_monitor3	Oracle VM Guest	0	ADMIN1	ADMIN1	Jul 10, 2012 2:30:47 AM UTC

Default Template for a target type. This template will be applied automatically to newly discovered targets in Enterprise Manager.

✓ TIP Oracle Certified templates contain the subset of monitoring settings pertaining to a specific functional area for the target type.

Related Links

Default Templates

Past Apply Operations

You can begin the monitoring template creation process from this page.

8.5 Creating a Monitoring Template

Monitoring template allow you to define and save monitoring settings for specific target types. To define a new template:

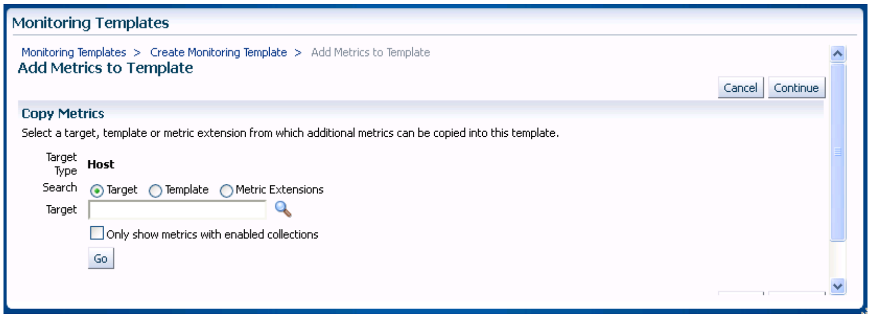
1. From the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates.**
2. Click **Create**. Enterprise Manager gives you the option of selecting either a specific target or a target type. Template monitoring settings are populated according to the selected target or target type. Click **Continue**.

> **Note:** If the selected target type is either Web Application or Service, you will only be able to select those targets for which you have Operator privilege.

3. Enter requisite template information on the General, Metric Thresholds, and Other Collected Items tabs.

   On the Metric Thresholds tab, you can delete or add monitoring template metrics. To delete existing metrics, select one or more metrics and click **Remove Metrics from Template**.

   To add metrics, click **Add Metrics to Template**. The Add Metrics to Template page displays as shown in the following graphic.



Monitoring Templates

Monitoring Templates > Create Monitoring Template > Add Metrics to Template

Add Metrics to Template

Copy Metrics

Select a target, template or metric extension from which additional metrics can be copied into this template.

Target Type **Host**

Search ● Target ○ Template ○ Metric Extensions

Target

□ Only show metrics with enabled collections

On this page, you can select a source from which you can copy metrics to the template. Sources include specific targets, other monitoring templates, or metric extensions. Click **Continue** once your have finished modifying the template metrics.

4. Once you have finished entering requisite information, click **OK**.

8.6 Editing a Monitoring Template

The Monitoring Templates page lists all viewable templates. To edit a template, you must have FULL access privileges.

To edit a Monitoring Template:

1. From the **Enterprise** menu, select **Monitoring**, and then **Monitoring Templates**.
2. Choose the desired template from the table.
3. Click **Edit**.
4. Once you have finished making changes, click **OK**.

Sharing Access with Other Users

By default, template owners (creators) have FULL access privileges on the template and Enterprise Manager Super Administrators have FULL access privileges on all templates. Only the template owner can change access to the template. You, as owner, can grant VIEW (view the template) or FULL (edit or delete the template) on the template to a user or role.

8.7 Applying Monitoring Templates to Targets

As mentioned earlier, a monitoring template can be applied to one or more targets of the same target type, or to composite targets such as groups. For composite targets, the template is applied to all member targets that are of the appropriate type. If you applied the template manually or via EM CLI, once a template is applied, future changes made to the template will not be automatically propagated to the targets: You must reapply the template to all affected targets

Administration Groups and Template Collections: Applying Monitoring Templates Automatically

Monitoring templates can be automatically applied whenever a new targets are added to your Enterprise Manager environment. Automation is carried out through Administration Groups and Template Collections Administration Groups are a special type of group used to automate application of monitoring settings to targets upon joining the group. When a target is added to the administration group Enterprise Manager applies monitoring settings from the associated template collection consisting of monitoring templates, compliance standards, and cloud policies. If changes are later made to the monitoring template, Enterprise Manager automatically applies the changes to the relevant targets based on the synchronization schedule. For more information, see "Using Administration Groups" on page 7-1.

8.7.1 Applying a Monitoring Template

To apply a template, you must have at least *Manage Target Metrics* target privileges on the destination target(s).

1. From the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates**.

2. Select the desired template from the table.
3. Click **Apply**.
4. Select the desired apply options and the target(s) to which you want the templates applied. See Section 8.7.2, "Monitoring Template Application Options" for additional information.
5. Click **OK**.

8.7.2 Monitoring Template Application Options

You can choose aggregate targets such groups, systems or clusters as destination targets. The templates will apply to the appropriate members of the group/system/cluster as they currently exist. If new members are later added to the group, you will need to re-apply the template to those new members. Template application is performed in the background as asynchronous jobs, so after the apply operation is performed, you can click on the link under the Pending Apply Operations column in the main templates table to see any apply operations that still are pending.

When applying a Monitoring Template, metric settings such as thresholds, comparison operators, and corrective actions are copied to the destination target. In addition, metric collection schedules including collection frequency and upload interval are also copied to the target. You determine how Enterprise Manager applies the metric settings from the template to the target by choosing an apply option.

8.7.2.1 Apply Options

Template apply options control how template metric and policy settings are applied to a target. Two template apply options are available:

- **Template will completely replace all metric settings in the target**: When the template is applied, all metrics and policies defined in the template will be applied to the target. Pre-existing target monitoring settings not defined in the template will be disabled: Metric thresholds will be set to NULL or blank. Policies will be disabled. This effectively eliminates alerts from these metrics and policies by clearing current severities and violations.
- **Template will only override metrics that are common to both template and target**: When the template is applied, only metrics and policies common to both the template and target are updated. Existing target metric and policies that do not exist in the template will remain unaffected. When this option is selected, additional template apply options are made available for metrics with key value settings.

8.7.2.2 Metrics with Key Value Settings

A metric with key value settings is one that can monitor multiple objects at different thresholds. For example, the Filesystem Space Available(%) metric can monitor different mount points using different warning and critical thresholds for each mount point.

When the template contains a metric that has key value settings, you can choose one of three options when applying this template to a target. As an example, consider the case where the template has the following metric:

Filesystem Space Available(%)

Mount Point	Operator	Warning Threshold	Critical Threshold
/	£	40	20
/private	£	30	20
/u1	£	30	20

And a host target has the same metric at different settings:

Mount Point	Operator	Warning Threshold	Critical Threshold
/	£	30	10
/private	£	25	15
/private2	£	20	20
All Others	£	25	15

These are the results for each option:

1) All key value settings in the template will be applied to the target, any additional key values settings on the target will not be removed

When the template is applied to the target using this copy option, all the template settings for the mount points, /, /private, and /U1 will be applied. Existing target settings for mount points not covered by the template remain unaffected. Thus, the resulting settings on the target for this metric will be:

Mount Point	Operator	Warning Threshold	Critical Threshold
/	£	40	20
/private	£	30	20
/u1	£	30	20

2) All key value settings in the template will be applied to target, any additional key value settings on the target will be removed.

When the template is applied to the target using this copy option, all template settings will be applied to the target. Any object-specific threshold settings that exist only on the target will be removed, any object-specific thresholds that are only in the template will be added to the target. Thus, the final settings on the target will be:

Mount Point	Operator	Warning Threshold	Critical Threshold
/	£	40	20
/private	£	30	20
/u1	£	30	20
All Others	£	25	15

3) Only settings for key values common to both template and target will be applied to the target

When the template is applied to the target using this copy option, only the settings for the common mount points, / and /private will be applied. Thus, the resulting settings on the target for this metric will be:

Mount Point	Operator	Warning Threshold	Critical Threshold
/	£	40	20
/private	£	30	20
/private2	£	20	10
All Others	£	25	15

8.8 Comparing Monitoring Templates with Targets

The intended effect of applying Monitoring Templates to destination targets is not always clear. Deciding how and when to apply a template is simplified by using the Compare Monitoring Template feature of Enterprise Manager. This allows you to see at a glance how metric and collection settings defined in the template differ from those defined on the destination target. You can easily determine whether your targets are still compliant with the monitoring settings you have applied in the past. This template comparison capability is especially useful when used with aggregate targets such as groups and systems. For example, you can quickly compare the metric and collection settings of group members with those of a template, and then apply the template as appropriate.

Performing a Monitoring Template-Target comparison:

1. From the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates**.
2. Choose the desired template from the table.
3. Click **Compare Settings**. The Compare Monitoring Template page displays.
4. Click **Add** to add one or more destination targets. The Search and Select dialog displays.
5. Select a one or more destination targets and then click **Select**. The selected targets are added to the list of destination targets.
6. Select the newly added destination targets and then click **Continue**. A confirmation message displays indicating the *Compare Template Settings* job was successfully submitted.
7. Click **OK** to view the job results. Note: Depending on the complexity of the job run, it may take time for the job to complete.

8.8.1 When is a metric between a template and a target considered "different"?

The metric is said to be different when any or all the following conditions are true (provided the target does not have "Template Override" set for that metric):

- The Warning Threshold settings are different
- The Critical Threshold settings are different.
- The Collection Schedules are different.
- The Upload Intervals are different.
- The number of occurrences (for which the metric has to remain at a value above the threshold before an alert is raised) are different.)
- For user-defined metrics, in addition to the above, the OS Command/SQL statement used to evaluate the user-defined metric is different. Note that this applies only if the user-defined metric name and the return type are the same.

- The metric extension marked for delete will be shown as "different" on the destination target and the template only if:
  - A metric extension with the same name exists on both the destination target and template.
  - The return type (String, Numeric) of the metric extension is the same on both the destination target and template.
  - The metric type is the same on both the destination target and the template.

8.9 Comparing Metric Settings Using Information Publisher

In addition to viewing metric differences between Monitoring Templates and destination targets using the Compare Monitoring Template user-interface, you can also use Information Publisher to generate reports containing the target-template differences. Using Information Publisher's reporting capabilities gives you more flexibility for displaying and distributing metric comparison data. For more information, see "Using Information Publisher" on page 26-1.

Create a Report Definition

1. From the **Enterprise** menu, select **Reports** and then **Information Publisher Reports**.
2. Click **Create**. The Create Report Definition user interface is displayed.
3. On the General page, specify the report name, how targets should be included, target privileges, report time period, and display options.
4. On the Elements page, click **Add** to access the Add Element page.
5. Select the Monitoring Template Comparison element and click **Continue** to return to the Element page.
6. Once you have added the report element, click the **Set Parameter** icon to specify requisite operational parameters. On this page, you specify a report header, select a monitoring template, destination targets, and template application settings for multiple threshold metrics. Click **Continue** to return to the Elements page.
7. Click **Layout** to specify how information should be arranged in the report.
8. Click **Preview** to validate that you are satisfied with the data and presentation of the report.
9. On the Schedule page, define when reports should be generated, and whether copies should be saved and/or sent via e-mail, and how stored copies should be purged.
10. On the Access page, click **Add** to specify which Enterprise Manager administrators and/or roles will be permitted to view this generated report. Additionally, if you have GRANT_ANY_REPORT_VIEWER system privilege, you can make this report definition accessible to non-credential users via the Enterprise Manager Reports Website
11. Click **OK** when you are finished.
12. Validate the report definition. If the parameters provided conflict, validation errors or warnings will appear and let you know what needs attention.
13. Once the report definition has been saved successfully, it appears in the Report Definition list under the Category and Subcategory you specified on the General page.

Viewing the Report

1. Find the template comparison report definition in the Report Definition list. You can use the Search function to find or filter the list of report definitions.
2. Click on the report definition title. If the report has a specified target, the report will be generated immediately. If the report does not have a specified target, you will be prompted to select a target.

Scheduling Reports for Automatic Generation

1. Create or edit a report definition.
2. On the Schedule page, choose the **Schedule Report** option.
3. Specify a schedule type. The schedule parameters on this page change according to the selected schedule type.

When reports are scheduled for automatic generation, you have the option of saving copies to the Management Repository and/or sending an e-mail version of the report to designated recipients.

If a report has been scheduled to save copies, a copy of the report is saved each time a scheduled report completes. When a user views a report with saved copies by clicking on the report title, the most recently saved copy of the report is rendered. To see the complete list of saved copies click on the Saved Copies link at the top of the report. Enterprise Manager administrators can generate a copy of the report on-demand by clicking on the Refresh icon on the report.

8.10 Exporting and Importing Monitoring Templates

For portability, monitoring templates can be exported to an XML file and then imported into another Enterprise Manager installation as an active template.

> **Important:** You can export templates from Enterprise Manager 10g release 2 or higher and import them into Enterprise Manager 12c. .

Exporting a Monitoring Template

To export a template to an XML file:

1. From the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates**.
2. Select the desired monitoring template from the table.
3. Click **Export**.

   Note: If you are running an Enterprise Manager 11*g* or earlier release, use the EM CLI *export_template* verb to perform the export operation. Note that if the monitoring template contains *policy rules* from earlier Enterprise Manager releases (pre-12*c)* , these will not be imported into Enterprise Manager 12*c* as policy rules no longer exist in this release.

Importing a Monitoring Template

To import a template from an XML file:

1. From the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates**.
2. Click Import. The Import Template page displays.
3. Specify the monitoring template XML file you want to import.

4. Click **Import**.

8.11 Upgrading Enterprise Manager: Comparing Monitoring Templates

When upgrading from one Enterprise Manager release to the next, you will accumulate monitoring templates that have been created for different releases. Beginning with Enterprise Manager release 12.1.0.4, you can generate a post-upgrade Monitoring Template Difference Report that allows you to view what templates had been created for various Enterprise Manager releases. To generate the Monitoring Template Difference Report, from the **Setup** menu, select **Manage Cloud Control**, and then **Post Upgrade Tasks**.

8.12 Changing the Monitoring Template Apply History Retention Period

You can view monitoring template apply history using the predefined report in Information Publisher. From the **Enterprise** menu, select **Reports** and then **Information Publisher.** On the Information Publisher page, you can enter "template" in the **Title** text entry field and click **Go**. The predefined report *Monitoring Template Apply History (last 7 days)* appears in the report list.

By default, Enterprise Manager retains the monitoring template apply history for a period of 180 days. If required, you can change the retention period to a value suitable for your monitoring needs. Although the retention period cannot be indefinite, it can be set to an extremely long period of time. Enterprise Manager provides the following PL/SQL API to change the retention period.

```
mgmt_template_ui.modify_purge_policy(p_retention_days=><num_days>)
```

This procedure takes a NUMBER as input (*num_days*).

9 Using Metric Extensions

Metric extensions provide you with the ability to extend Oracle's monitoring capabilities to monitor conditions specific to your IT environment. This provides you with a comprehensive view of your environment. Furthermore, metric extensions allow you to simplify your IT organization’s operational processes by leveraging Enterprise Manager as the single central monitoring tool for your entire datacenter instead of relying on other monitoring tools to provide this supplementary monitoring.

This chapter covers the following:

Instructional Videos: For video tutorials on using metric extensions, see:

Metric Extensions Part 1: Create Metric Extensions

`https://apex.oracle.com/pls/apex/f?p=44785:24:115515960475402:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5741%2C24`

Metric Extensions Part 2: Deploy Metric Extensions

`https://apex.oracle.com/pls/apex/f?p=44785:24:15296555051584:::24:P24_CONTENT_ID%2CP24_PREV_PAGE:5742%2C24`

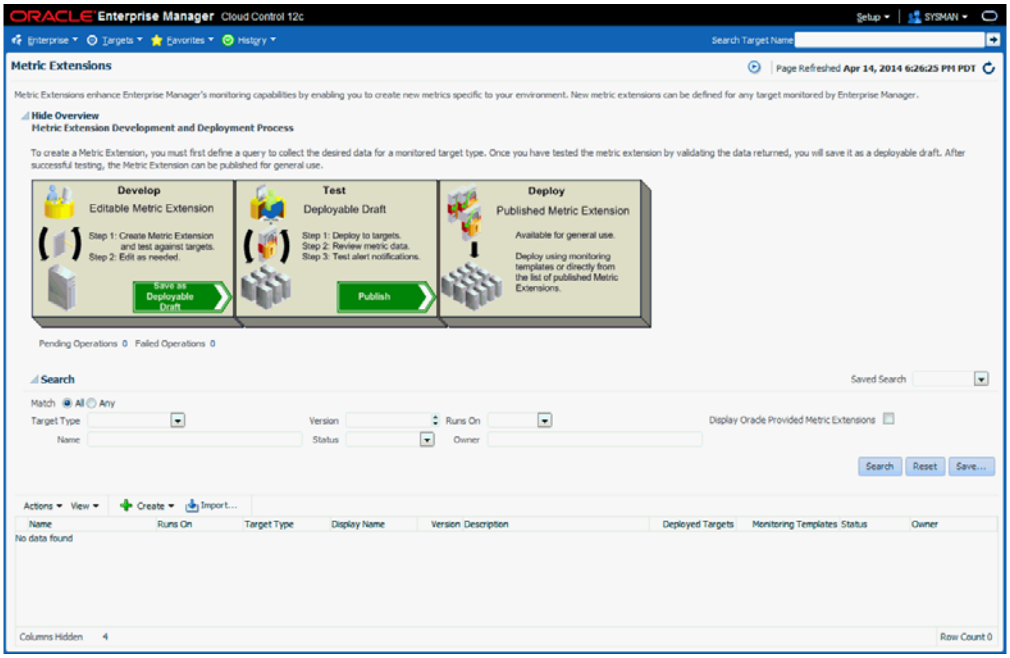
9.1 What are Metric Extensions?

Metric extensions allow you to create metrics on any target type. Unlike user-defined metrics (used to extend monitoring in previous Enterprise Manager releases), metric extensions allow you to create full-fledged metrics for a multitude of target types, such as:

- Hosts
- Databases
- Fusion Applications

- IBM Websphere
- Oracle Exadata databases and storage servers
- Siebel components
- Oracle Business Intelligence components

You manage metric extensions from the Metric Extensions page. This page lists all metric extensions in addition to allowing you to create, edit, import/export, and deploy metric extensions.



Metric Extensions enhance Enterprise Manager's monitoring capabilities by enabling you to create new metrics specific to your environment. New metric extensions can be defined for any target monitored by Enterprise Manager.

To create a Metric Extension, you must first define a query to collect the desired data for a monitored target type. Once you have tested the metric extension by validating the data returned, you will save it as a deployable draft. After successful testing, the Metric Extension can be published for general use.

Step 1: Create Metric Extension and test against targets.
Step 2: Edit as needed.

Step 1: Deploy to targets.
Step 2: Review metric data.
Step 3: Test alert notifications.

Available for general use.

Deploy using monitoring templates or directly from the list of published Metric Extensions.

Pending Operations 0 Failed Operations 0

Name	Runs On	Target Type	Display Name	Version	Description	Deployed Targets	Monitoring Templates	Status	Owner
No data found									

The cornerstone of the metric extension is the Oracle Integration Adapter. Adapters provide a means to gather data about targets using specific protocols. Adapter availability depends on the target type your metric extension monitors.

How Do Metric Extensions Differ from User-defined Metrics?

In previous releases of Enterprise Manager, user-defined metrics were used to extend monitoring capability in a limited fashion: user-defined metrics could be used to collect point values through execution of OS scripts and a somewhat more complex set of values (one per object) through SQL. Unlike metric extensions, user-defined metrics have several limitations:

- **Limited Integration**: If the OS or SQL user-defined metric executed custom scripts, or required atonal dependent files, the user needed to manually transfer these files to the target's file system.
- **Limited Application of Query Protocols**: OS user-defined metrics cannot model child objects of servers by returning multiple rows from a metric (this capability only exists for SQL user-defined metrics).
- **Limited Data Collection**: Full-fledged Enterprise Manager metrics can collect multiple pieces of data with a single query and reflect the associated data in alert context. However, in the case of user-defined metrics, multiple pieces of data must be collected by creating multiple user-defined metrics. Because the data is being collected separately, it is not possible to refer to the associated data when alerts are generated.

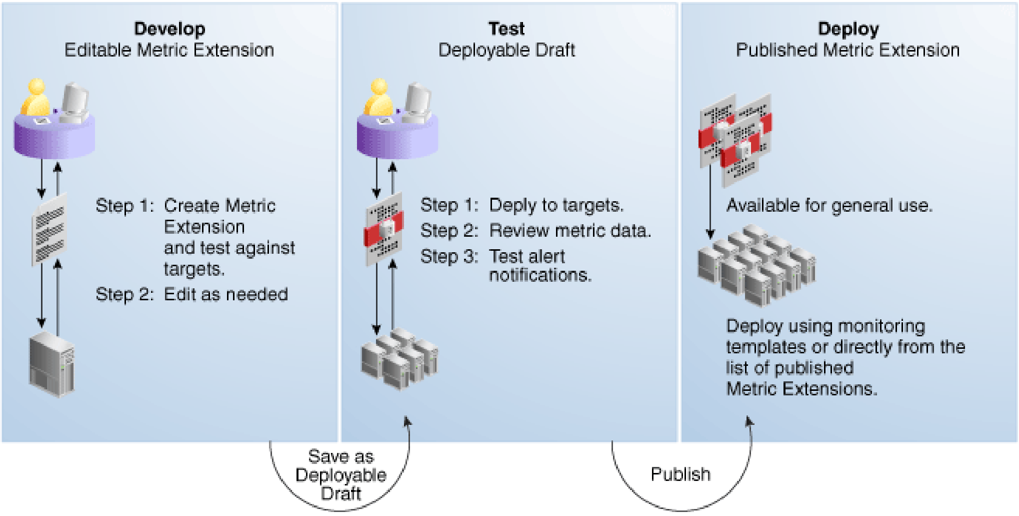
- **Limited Query Protocols**: User-defined metrics can only use the "OS" and "SQL" protocols, unlike metric extensions which can use additional protocols such as SNMP and JMX.
- **Limited Target Application**: User-defined metrics only allow OS user-defined metrics against host targets and SQL user-defined metrics against database targets. No other target types are permitted. If, for example, you want to deploy a user-defined metric against WebLogic instances in your environment, you will not be able to do so since it is neither a host or database target type.

Most importantly, the primary difference between metric extensions and user-defined metrics is that, unlike user-defined metrics, metric extensions are full-fledged metrics similar to Enterprise Manager out-of-box metrics. They are handled and exposed in all Enterprise Manager monitoring features as any Enterprise Manager-provided metric and will automatically apply to any new features introduced.

9.2 Metric Extension Lifecycle

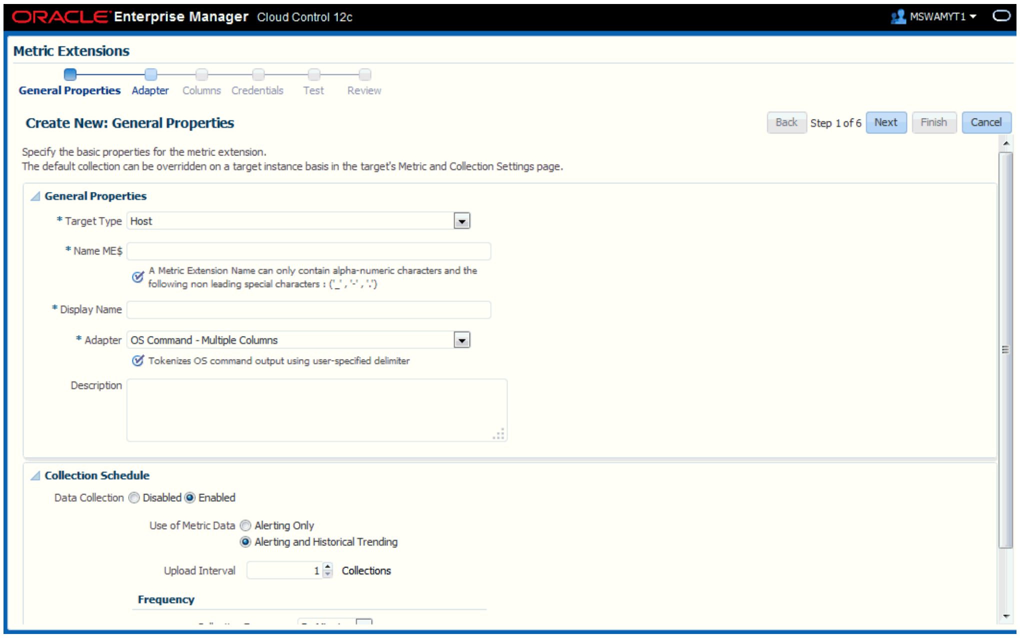
Developing a metric extension involves the same three phases you would expect from any programmatic customization:

- Developing Your Metric Extension
- Testing Your Metric Extension
- Deploying and Publishing Your Metric Extension


Develop
Editable Metric Extension
Step 1: Create Metric Extension and test against targets.
Step 2: Edit as needed
Test
Deployable Draft
Step 1: Deply to targets.
Step 2: Review metric data.
Step 3: Test alert notifications.
Deploy
Published Metric Extension
Available for general use.
Deploy using monitoring templates or directly from the list of published Metric Extensions.
Save as Deployable Draft
Publish

Developing Your Metric Extension

The first step is to define your monitoring requirements. This includes deciding the target type, what data needs to be collected, what mechanism (adapter) can be used to collect that data, and if elevated credentials are required. After making these decisions, you are ready to begin developing your metric extension. Enterprise Manager provides an intuitive user interface to guide you through the creation process.



Create New: General Properties

Specify the basic properties for the metric extension.
The default collection can be overridden on a target instance basis in the target's Metric and Collection Settings page.

General Properties

* Target Type: Host

* Name ME$

A Metric Extension Name can only contain alpha-numeric characters and the following non leading special characters : ('_' , '-' , '.')

* Display Name

* Adapter: OS Command - Multiple Columns

Tokenizes OS command output using user-specified delimiter

Description

Collection Schedule

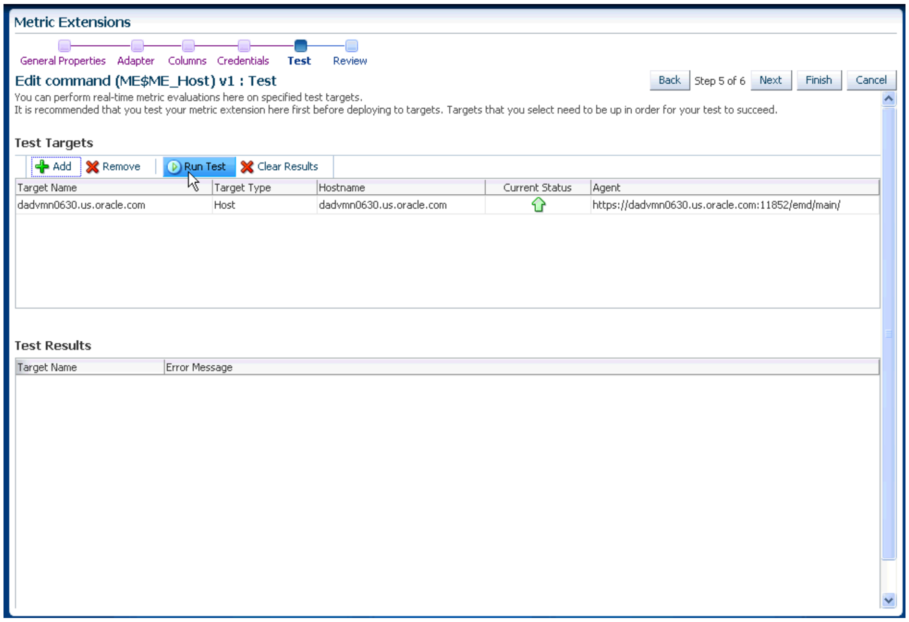
Data Collection ○ Disabled ● Enabled

Use of Metric Data ○ Alerting Only
● Alerting and Historical Trending

Upload Interval 1 Collections

Frequency

The metric extension wizard allows you to develop and refine your metric extension in a completely editable format. And more importantly, allows you to interactively test your metric extension against selected targets without having first to deploy the extension to a dedicated test environment. The **Test** page allows you to run real-time metric evaluations to ensure there are no syntactical errors in your script or metric extension definition.



Edit command (ME$ME_Host) v1 : Test

You can perform real-time metric evaluations here on specified test targets.
It is recommended that you test your metric extension here first before deploying to targets. Targets that you select need to be up in order for your test to succeed.

Test Targets

Target Name	Target Type	Hostname	Current Status	Agent
dadvmn0630.us.oracle.com	Host	dadvmn0630.us.oracle.com	⇧	https://dadvmn0630.us.oracle.com:11852/emd/main/

Test Results

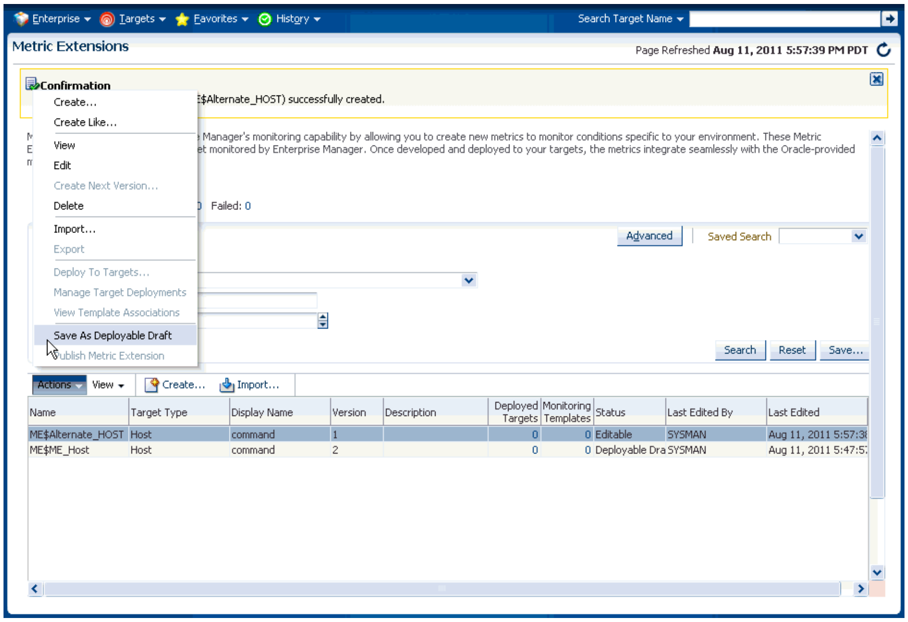
Target Name	Error Message

When you have completed working on your metric extension, you can click Finish to exit the wizard. The newly created metric extension appears in the Metric Extension Library where you can edit can be opened for further editing or saved as a deployable draft that can be tested against multiple targets.

Note: You can edit a metric extension only if its status is *editable*. Once it is saved as a deployable draft, you must create a new version to implement further edits.

Testing Your Metric Extension

Once your metric extension returns the expected data during real-time target testing, you are ready to test its robustness and actual behavior in Enterprise Manager by deploying it against targets and start collecting data. At this point, the metric extension is still private (only the developer can deploy to targets), but is identical to Oracle out-of-box metrics behavior wise. This step involves selecting your editable metric extension in the library and generating a deployable draft.



Metric Extensions

Page Refreshed **Aug 11, 2011 5:57:39 PM PDT**

Confirmation

E$Alternate_HOST) successfully created.

Manager's monitoring capability by allowing you to create new metrics to monitor conditions specific to your environment. These Metric
et monitored by Enterprise Manager. Once developed and deployed to your targets, the metrics integrate seamlessly with the Oracle-provided

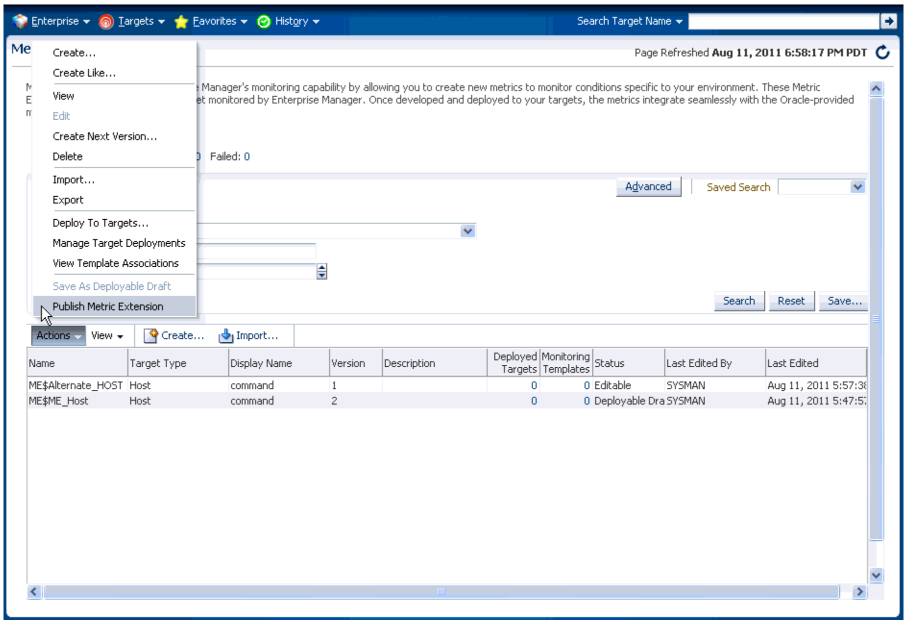
Failed: 0

Name	Target Type	Display Name	Version	Description	Deployed Targets	Monitoring Templates	Status	Last Edited By	Last Edited
ME$Alternate_HOST	Host	command	1		0	0	Editable	SYSMAN	Aug 11, 2011 5:57:3
ME$ME_Host	Host	command	2		0	0	Deployable Dra	SYSMAN	Aug 11, 2011 5:47:5

You can now deploy the metric extension to actual targets by going through the “Deploy To Targets…” action. After target deployment, you can review the metric data returned and test alert notifications. As mentioned previously, you will not be able to edit the metric extension once a deployable draft is created: You must create a new version of the metric extension.

Deploying Your Metric Extension

After rigorous testing through multiple metric extension versions and target deployments, your metric extension is ready for deployment to your production environment. Until this point, your metric extension is only viewable by you, the metric extension creator. To make it accessible to all Enterprise Manager administrators, it must be published.



Page Refreshed **Aug 11, 2011 6:58:17 PM PDT**

Manager's monitoring capability by allowing you to create new metrics to monitor conditions specific to your environment. These Metric et monitored by Enterprise Manager. Once developed and deployed to your targets, the metrics integrate seamlessly with the Oracle-provided

Failed: 0

Name	Target Type	Display Name	Version	Description	Deployed Targets	Monitoring Templates	Status	Last Edited By	Last Edited
ME$Alternate_HOST	Host	command	1		0	0	Editable	SYSMAN	Aug 11, 2011 5:57:3
ME$ME_Host	Host	command	2		0	0	Deployable Dra	SYSMAN	Aug 11, 2011 5:47:5

Now that your metric extension has been made public, your metric extension can be deployed to intended production targets. If you are monitoring a small number of targets, you can select the **Deploy To Targets** menu option and add targets one at a time. For large numbers of targets, you deploy metric extensions to targets using monitoring templates. An extension is added to a monitoring template in the same way a full-fledged metric is added. The monitoring template is then deployed to the targets.

Note: You cannot add metric extensions to monitoring templates before publishing the extension. If you attempt to do so, the monitoring template page will warn you about it, and will not proceed until you remove the metric extension.

Updating Metric Extensions

Beginning with Enterprise Manager Release 12.1.0.4, metric extensions can be updated using the Enterprise Manager Self-update feature. See Chapter 14, "Updating Cloud Control" for more information.

9.3 Working with Metric Extensions

Most all metric extension operations can be carried out from the Metric Extension home page. If you need to perform operations on published extensions outside of the UI, Enterprise Manger also provides EM CLI verbs to handle such operations as importing/exporting metric extensions to archive files and migrating legacy user-defined metrics to metric extensions. This section covers metric extension operations carried out from the UI.

9.3.1 Administrator Privilege Requirements

In order to create, edit, view, deploy or undeploy metric extensions, you must have the requisite administrator privileges. Enterprise Manager administrators must have the following privileges:

- **Create Metric Extension**: System level access that:

  Lets administrators view and deploy metric extensions

  Allows administrators to edit and delete extensions.

- **Edit Metric Extension**: Lets users with "Create Metric Extension" privilege edit and create next versions of a particular metric extensions. The metric extension creator has this privilege by default. This privilege must be granted on a per-metric extension basis.

- **Full Metric Extension**: Allows users with 'Create Metric Extension' privilege to edit and create new versions of a particular metric extension.

- **Manage Metrics**: Lets users deploy and un-deploy extensions on targets

  Note: The Manage Metrics privilege must be granted on a per-target basis.

9.3.2 Granting Create Metric Extension Privilege

To grant create metric extension privileges to another administrator:

1. From the **Setup** menu, select **Security**, then select **Administrators**.
2. Choose the Administrator you would like to grant the privilege to.
3. Click **Edit**.
4. Go to the Resource Privileges tab, and click **Manage Privilege Grants** for the Metric Extension resource type.
5. Under Resource Type Privileges, click the **Create Metric Extension** check box.
6. Click **Continue**, review changes, and click **Finish** in the Review tab.

9.3.3 Managing Administrator Privileges

Before an Enterprise Manager administrator can edit or delete a metric extension created by another administrator, that administrator must have been granted requisite access privileges. *Edit* privilege allows editing and creating next versions of the extension. *Full* privilege allows the above operations and deletion of the extension.

To grant edit/full access to an existing metric extension to another administrator:

1. From the **Setup** menu, select **Security**, then select **Administrators**.
2. Choose the Administrator you would like to grant access to.
3. Click **Edit**.
4. Go to **Resource Privileges** and click Manage Privilege Grants (pencil icon) for the Metric Extensions resource type.
5. Under **Resource Privileges**, you can search for and add existing metric extensions. Add the metric extensions you would like to grant privileges to. This allows the user to edit and create next versions of the metric extension.

   On this page, you can also grant an administrator the *Create Metric Extension* privilege, which will allow them to manage metric extension access. See "Managing Administrator Access to Metric Extensions" for more information.
6. If you would additionally like to allow delete operations, then click the pencil icon in the **Manage Resource Privilege Grants** column, and select **Full Metric Extension** privilege in the page that shows up.
7. Click **Continue**, review changes, and click **Finish** in the review tab.

9.3.4 Managing Administrator Access to Metric Extensions

Administrators commonly share the responsibility of monitoring and managing targets within the IT environment. Consequently, creating and maintaining metric extensions becomes a collaborative effort involving multiple administrators. Metric extension owners can control access directly from the metric extension UI.

9.3.4.1 Granting Full/Edit Privileges on a Metric Extension

As metric extension owner or Super Administrator, perform the following actions to assign full/edit privileges on a metric extension to another administrator:

1. From the **Enterprise** menu, select **Monitoring,** then select **Metric Extensions.**
2. Choose a metric extension requiring update.
3. From the **Actions** menu, select **Manage Access**.
4. Click **Add**. The administrator selection dialog box appears. You can filter the list by administrator, role, or both.
5. Choose one or more administrators/roles from the list.
6. Click **Select**. The chosen administrators/roles appear in the access list.

   In the **Privilege** column, **Edit** is set by default. Choose **Full** from the drop-down menu to assign **Full** privileges on the metric extension.

   Edit Privilege: Allows an administrator to make changes to the metric extension but not delete it.

   Full Privilege: Allows an administrator to edit and also delete the metric extension. The privilege granted to a user or role applies to all versions of the metric extension.
7. Click **OK**.

9.3.4.2 Revoking Access Privileges on a Metric Extension

As metric extension owner or Super Administrator, perform the following actions to revoke metric extension privileges assigned to another administrator:

1. From the **Enterprise** menu, select **Monitoring,** then select **Metric Extensions.**
2. Choose a metric extension requiring update.
3. From the **Actions** menu, select **Manage Access**.
4. Choose one or more administrators/roles from the list.
5. Click **Remove**. The chosen administrators/roles is deleted from the access list.
6. Click **OK**.

Enterprise Manager allows metric extension ownership to be transferred from the current owner of the metric extension to another administrator as long as that administrator has been granted the *Create Metric Extension* privilege.

> **Note:** The Enterprise Manager Super Administrator has full managerial access to all metric extensions (view, edit, and ownership transfer).

As mentioned above, *manage access* is only enabled for the owner of the extension or an Enterprise Manager Super User. Once the ownership is transferred, the previous owner does not have any management privileges on the metric extension unless explicitly granted before ownership transfer. The **Change Owner** option is only available to users and not roles.

Manage access allows the metric extension owner or Super Administrator to grant other Enterprise Manager users or roles the ability to edit, modify, or delete metric extensions.

9.3.4.3 Transferring Metric Extension Ownership

Enterprise Manager allows metric extension ownership to be transferred from the current owner of the metric extension to another administrator as long as that administrator has been granted the *Create Metric Extension* privilege.

> **Note:** The Enterprise Manager Super Administrator has full managerial access to all metric extensions (view, edit, and ownership transfer).

As mentioned above, *manage access* is only enabled for the owner of the extension or an Enterprise Manager Super User. Once the ownership is transferred, the previous owner does not have any management privileges on the metric extension unless explicitly granted before ownership transfer. The **Change Owner** option is only available to users and not roles.

Manage access allows the metric extension owner or Super Administrator to grant other Enterprise Manager users or roles the ability to edit, modify, or delete metric extensions.

9.3.5 Creating a New Metric Extension

To create a new metric extension:

1. From the **Enterprise** menu, select **Monitoring,** then select **Metric Extensions.**
2. From the **Create** menu, select **Metric Extension**. Enterprise Manager will determine whether you have the Create Extension privilege and guide you through the creation process.
3. Decide on a metric extension name. Be aware that the name (and Display Name) must be unique across a target type.
4. Enter the general parameters.

   The selected Adapter type defines the properties you must specify in the next step of the metric extension wizard. The following adapter types are available:

   - OS Command Adapter - Single Column

     Executes the specified OS command and returns the command output as a single value. The metric result is a 1 row, 1 column table.

   - OS Command Adapter- Multiple Values

     Executes the specified OS command and returns each command output line as a separate value. The metric result is a multi-row, 1 column table.

   - OS Command Adapter - Multiple Columns

     Executes the specified OS command and parses each command output line (delimited by a user-specified string) into multiple values. The metric result is a mult-row, multi-column table.

- SQL Adapter

  Executes custom SQL queries or function calls against single instance databases and instances on Real Application Clusters (RAC).

- SNMP (Simple Network Management Protocol) Adapter

  Allow Enterprise Manager Management Agents to query SNMP agents for Management Information Base (MIB) variable information to be used as metric data.

- JMX (Java Management Extensions) Adapter

  Retrieves JMX attributes from JMX-enabled servers and returns these attributes as a metric table.

Refer to the Adapters section for specific information on the selected adapter needed in the Adapter page (step 2) of the wizard.

> **Note:** Be aware that if you change the metric extension Adapter, all your previous adapter properties (in Step 2) will be cleared.

Collection Schedule

You defined the frequency with which metric data is collected and how it is used (Alerting Only or Alerting and Historical Trending) by specifying collection schedule properties.

Depending on the target type selected, an *Advanced* option region may appear. This region may (depending on the selected target type) contain one or two options that determine whether metric data continues to be collected under certain target availability/alert conditions. The options are:

- **Option 1**: Continue metric data collection even if the target is down. This option is visible for all target types except for *Host* target types as it is not possible to collect metric data when the host is down.

- **Option 2**: Continue metric data collection when an alert severity is raised for a specific target metric. This metric is defined in such a way (AltSkipCondition element is defined on this metric) that when a severity is generated on this metric, the metric collections for other target metrics are stopped. The explanatory text above the checkbox for this option varies depending on the selected target type.

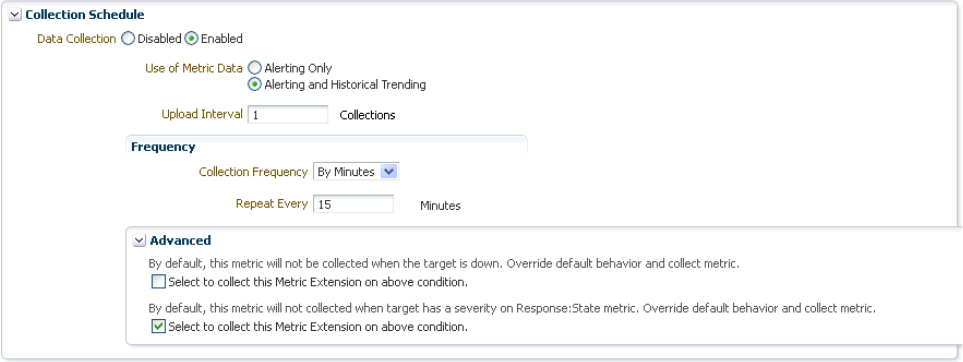
  The Management Agent has logic to skip evaluation of metrics for targets that are known to be down to reduce generation of metric errors due to connection failures. If the AltSkipCondition element is defined for that target metric, other metrics are skipped whenever there is an error in evaluating the Response metric or there is a non-clear severity on the Response:Status metric. There are two situations where a metric collection will be skipped or not happen:

  - When a target is down (option 1). This is same as the Severity on Response/Status metric.

  - When a target is UP, but there is a severity on any other metric. Such conditions are called Alt Skip (Alternate Skip) conditions.

  Option 2 is only visible if an AltSkipCondition defined for one of the target's metrics. For example, this option will not be visible if the selected target type is *Oracle Weblogic Domain*, but will be visible if the selected target type is *Database Instance*.

The following graphic shows the Advanced collection schedule options.



Collection Schedule

Data Collection ○ Disabled ● Enabled

Use of Metric Data ○ Alerting Only
● Alerting and Historical Trending

Upload Interval 1 Collections

Frequency

Collection Frequency By Minutes

Repeat Every 15 Minutes

Advanced

By default, this metric will not be collected when the target is down. Override default behavior and collect metric.
□ Select to collect this Metric Extension on above condition.

By default, this metric will not collected when target has a severity on Response:State metric. Override default behavior and collect metric.
☑ Select to collect this Metric Extension on above condition.

5. From the Columns page, add metric columns defining the data returned from the adapter. Note that the column order should match the order with which the adapter returns the data.

   - **Column Type**

     A column is either a Key column, or Data column. A Key column uniquely identifies a row in the table. For example, employee ID is a unique identifier of a table of employees. A Data column is any non-unique data in a row. For example, the first and last names of an employee. You can also create rate and delta metric columns based on an existing data column. See *Rate and Delta Metric Columns* below.

   - **Value Type**

     A value type is Number or String. This determines the alert comparison operators that are available, and how Enterprise Manager renders collection data for this metric column.

   - **Alert Thresholds**

     The Comparison Operation, Warning, and Critical fields define an alert threshold.

   - **Alert Thresholds By Key**

     The Comparison Operation, Warning Thresholds By Key, and Critical Thresholds By Key fields allow you to specify distinct alert thresholds for different rows in a table. This option becomes available if there are any Key columns defined. For example, if your metric is monitoring CPU Usage, you can specify a different alert threshold for each distinct CPU. The syntax is to specify the key column values in a comma separated list, the "=" symbol, followed by the alert threshold. Multiple thresholds for different rows can be separated by the semi-colon symbol ";". For example, if the key columns of the CPU Usage metric are cpu_id and core_id, and you want to add a warning threshold of 50% for procecessor1, core1, and a threshold of 60% for processor2, core2, you would specify: procecessor1,core1=50;processor2,core2=60

   - **Manually Clearable Alert**

     Note: You must expand the Advanced region in order to view the Manually Clearable Alert option.

If this option is set to true, then the alert will not automatically clear when the alert threshold is no longer satisfied. For example, if your metric is counting the number of errors in the system log files, and you set an alert threshold of 50, if an alert is raised once the threshold is met, the alert will not automatically clear once the error count falls back below 50. The alert will need to be manually cleared in the Alerts UI in the target home page or Incident Manager.

- **Number of Occurrences Before Alert**

  The number of consecutive metric collections where the alert threshold is met, before an alert is raised.

- **Alert Message / Clear Message**

  The message that is sent when the alert is raised / cleared. Variables that are available for use are: %columnName%, %keyValue%, %value%, %warning_threshold%, %critical_threshold%

  You can also retrieve the value of another column by surrounding the desired column name with "%". For example, if you are creating an alert for the cpu_usage column, you can get the value of the core_temperature column by using %core_temperature%. Note that the same alert / clear message is used for warning or critical alerts.

Note: Think carefully and make sure all Key columns are added, because you cannot create additional Key columns in newer versions of the metric extension. Once you click **Save As Deployable Draft**, the Key columns are final (edits to column display name, alert thresholds are still allowed). You can still add new Data columns in newer versions. Also be aware that some properties of existing Data columns cannot be changed later, including Column Type, Value Type, Comparison Operator (you can add a new operator, but not change an existing operator), and Manually Clearable Alert.

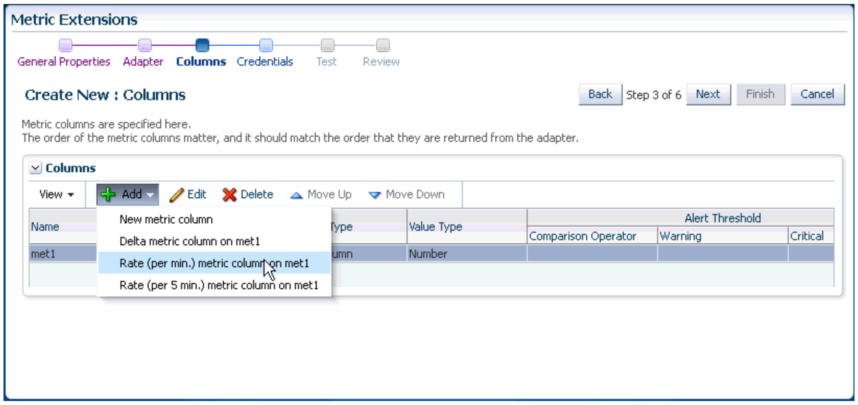
- **Metric Category**

  The metric category this column belongs to.

Rate and Delta Metric Columns

You can create additional metric columns based on an existing data column that measures the rate at which data changes or the difference in value (delta) since the last metric collection. The rate/delta metric definition will be allowed when a metric's collection frequency is periodic. For example, collected every 10 minutes. Converseley, a metric that is computed every Monday and Tuesday only cannot have a rate/delta metric as data sampling is too infrequent.

After at least one data column has been created, three additional options appear in the **Add** menu as shown in the following graphic.



Create New : Columns

Metric columns are specified here.
The order of the metric columns matter, and it should match the order that they are returned from the adapter.

Name	Type	Value Type	Alert Threshold		
			Comparison Operator	Warning	Critical
met1	umn	Number			

- Add Delta metric columns based on another metric column

  Example: You want to know the difference in the table space used since the last collection.

  Delta Calculation:

  current metric value - previous metric value

- Add Rate Per Minute metric column based on another metric column

  Example: You want to know the average table space usage per minute based on the table space column metric which is collected every 1 hr.

  Rate Per Minute Calculation:

  (current metric value - previous metric value)/ collection schedule

  where the *collection schedule* is in minutes.

- Add Rate Per Five Minutes metric column based on another metric column

  Example: You want to know the average table space usage every five minutes based on the table space column which is collected say every 1 hour]

  Rate Per Five Minute Calculation:

  *[(current metric value - previous metric value)/ collection schedule] * 5*

  where the *collection schedule* is in minutes.

To create a rate/delta metric column, click on an existing data column in the table and then select one of the rate/delta column options from the **Add** menu.

6. From the Credentials page, you can override the default monitoring credentials by using custom monitoring credential sets. By default, the metric extension wizard chooses the existing credentials used by Oracle out-of-box metrics for the particular target type. For example, metric extensions will use the dbsnmp user for database targets. You have the option to override the default credentials, by creating a custom monitoring credential set through the "emcli create_credential_set" command. Refer to the *Enterprise Manager Command Line Interface Guide* for additional details. Some adapters may use additional credentials, refer to the Adapters section for specific information.

7. From the Test page, add available test targets.

8. Click **Run Test** to validate the metric extension. The extension is deployed to the test targets specified by the user and a real-time collection is executed. Afterwards, the metric extension is automatically undeployed. The results and any errors are added to the **Test Results** region.

9. Repeat the edit /test cycle until the metric extension returns data as expected.
10. Click **Finish**.

9.3.6 Creating a New Metric Extension (Create Like)

To create a new metric extension based on an existing metric extension:

1. From the **Enterprise** menu, select **Monitoring**, then select **Metric Extensions.**
2. From the **Metric Extensions** page, determine which extensions are accessible. The page displays the list of metric extensions along with target type, owner, production version and deployment information.
3. Select an existing metric extension.
4. From the **Actions** menu, select **Create Like**. Enterprise Manager will determine whether you have the Create Extension privilege and guide you through the creation process.
5. Make desired modifications.
6. From the **Test** page, add available test targets.
7. Click **Run Test** to validate the metric extension. The extension is deployed to the test targets specified by the user and a real-time collection is executed. Afterwards, the metric extension is automatically undeployed. The results and any errors are added to the **Test Results** region.
8. Repeat the edit /test cycle until the metric extension returns data as expected.
9. Click **Finish**.

9.3.7 Editing a Metric Extension

Before editing an existing metric extension, you must have Edit privileges on the extension you are editing or be the extension creator. Note: Once a metric extension is saved as a deployable draft, it cannot be edited, you can only create a new version.

To edit an existing metric extension:

1. From the **Enterprise** menu, select **Monitoring**, then select **Metric Extensions.**
2. From the **Metric Extensions** page, determine which extensions are accessible. The page displays the list of metric extensions along with target type, owner, production version and deployment information.
3. Select the metric extension to be edited.
4. From the **Actions** menu, select **Edit**.
5. Update the metric extension as needed.
6. From the **Test** page, add available test targets.
7. Click **Run Test** to validate the metric extension. The extension is deployed to the test targets specified by the user and a real-time collection is executed. Afterwards, the metric extension is automatically undeployed. The results and any errors are added to the **Test Results** region.
8. Repeat the edit /test cycle until the metric extension returns data as expected.
9. Click **Finish**.

9.3.8 Creating the Next Version of an Existing Metric Extension

Before creating the next version of an existing metric extension, you must have Edit privileges on the extension you are versioning or be the extension creator.

To create next version of an existing metric extension:

1. From the **Enterprise** menu, select **Monitoring**, then select **Metric Extensions**.
2. From the Metric Extensions page, determine which extensions are accessible. The page displays the list of metric extensions along with target type, owner, production version and deployment information.
3. Select the metric extension to be versioned.
4. From the **Actions** menu, select **Create Next Version**.
5. Update the metric extension as needed. The target type, and extension name cannot be edited, but all other general properties can be modified. There are also restrictions on metric columns modifications. See Note in Creating a New Metric Extension section for more details.
6. From the Test page, add available test targets.
7. Click **Run Test** to validate the metric extension. The extension is deployed to the test targets specified by the user and a real-time collection is executed. Afterwards, the metric extension is automatically undeployed. The results and any errors are added to the **Test Results** region.
8. Repeat the edit /test cycle until the metric extension returns data as expected.
9. Click **Finish**.

9.3.9 Importing a Metric Extension

Metric extensions can be converted to portable, self-contained packages that allow you to move the metric extension to other Enterprise Manager installations, or for storage/backup. These packages are called Metric Extension Archives (MEA) files.

MEA files are zip files containing all components that make up the metric extension: metric metadata, collections, and associated scripts/jar files. Each MEA file can contain only one metric extension. To add the metric extension back to your Enterprise Manager installation, you must import the metric extension from the MEA.

To import a metric extension from an MEA file:

1. From the **Enterprise** menu, select **Monitoring**, then select **Metric Extensions.**
2. Click **Import**.
3. Browse to file location, and select the MEA file. Enterprise Manager checks if the target type and metric extension name combination is already used in the system. If not, the system will create a new metric extension. If the extension name is already in use, the system will attempt to create a new version of the existing extension using the MEA contents. This will require the MEA to contain a superset of all the existing metric extension's metric columns. You also have the option to rename the metric extension.
4. Clicking on OK creates the new metric extension or the new version of an existing metric extension.
5. From the **Actions** menu, select **Edit** to verify the entries.
6. From the **Test** page, add available test targets.

7. Click **Run Test** to validate the metric extension. The extension is deployed to the test targets specified by the user and a real-time collection is executed. Afterwards, the metric extension is automatically undeployed. The results and any errors are added to the **Test Results** region.
8. Repeat the edit /test cycle until the metric extension returns data as expected.
9. Click **Finish**.

9.3.10 Exporting a Metric Extension

Existing metric extensions can be package as self-contained zip files (exported) for portability and/or backup and storage.

To export an existing metric extension:

1. From the **Enterprise** menu, select **Monitoring**, then select **Metric Extensions.**
2. From the **Metric Extensions** page, determine which extensions are accessible. The page displays the list of metric extensions along with target type, owner, production version and deployment information.
3. Select the metric extension to be exported.
4. From the **Actions** menu, select **Export**. Enterprise Manager prompts you to enter the name and location of the MEA file that is to be created.
5. Enter the name and location of the package. Enterprise Manager displays the confirmation page after the export is complete.

   Note: You can only export Production, Deployable Draft and Published metric extension versions.
6. Confirm the export file is downloaded.

9.3.11 Deleting a Metric Extension

Initiating the deletion of a metric extension is simple. However, the actual deletion triggers a cascade of activity by Enterprise Manager to completely purge the metric extension from the system. This includes closing open metric alerts, and purging collected metric data (if the latest metric extension version is deleted).

Before a metric extension version can be deleted, it must be undeployed from all targets, and removed from all monitoring templates (including templates in pending apply status).

To delete a metric extension:

1. From the **Enterprise** menu, select **Monitoring**, then select **Metric Extensions.**
2. From the **Metric Extensions** page, determine which extensions are accessible. The page displays the list of metric extensions along with target type, owner, production version and deployment information.
3. Select the metric extension that is to be deleted.
4. From the **Actions** menu, select **Delete**. Enterprise Manager prompts you to confirm the deletion.
5. Confirm the deletion.

9.3.12 Deploying Metric Extensions to a Group of Targets

A metric extension must be deployed to a target in order for it to begin collecting data.

To deploy a metric extension to one or more targets:

1. From the **Enterprise** menu, select **Monitoring**, then select **Metric Extensions.**
2. From the **Metric Extensions** page, determine which extensions are accessible. The page displays the list of metric extensions along with target type, owner, production version and deployment information.
3. Select the metric extension that is to be deployed.
4. From the **Actions** menu, select **Manage Target Deployments**. The **Manage Target Deployments** page appears showing you on which target(s) the selected metric extension is already deployed.
5. Return to the **Metric Extensions** page.
6. Select the metric extension.
7. From the **Actions** menu, select **Deploy to Targets**. Enterprise Manager determines whether you have "Manage Target Metrics" privilege, and only those targets where you do show up in the target selector.
8. Add the targets where the metric extension is to be deployed and click Submit. Enterprise Manager submits a job deploying the metric extension to each of the targets. A single job is submitted per deployment request.
9. You are automatically redirected to the Pending Operations page, which shows a list of currently scheduled, executing, or failed metric extension deploy operations. Once the deploy operation completes, the entry is removed from the pending operations table.

9.3.13 Creating an Incident Rule to Send Email from Metric Extensions

One of the most common tasks administrators want Enterprise Manager to perform is to send an email notification when a metric alert condition occurs. Specifically, Enterprise Manager monitors for alert conditions defined as incidents. For a given incident you create an incident rule set to tell Enterprise Manager what actions to take when an incident occurs. In this case, when an incident consisting of an alert condition defined by a metric extension occurs, you need to create an incident rule to send email to administrators. For instructions on sending email for metric alerts, see "Sending Email for Metric Alerts" on page 3-78.

For information incident management see Chapter 3, "Using Incident Management."

9.3.14 Updating Older Versions of Metric Extensions Already deployed to a Group of Targets

When a newer metric extension version is published, you may want to update any older deployed instances of the metric extension.

To update old versions of the metric extension already deployed to targets:

1. From the **Enterprise** menu, select **Monitoring**, then select **Metric Extensions.**
2. From the **Metric Extensions** page, determine which extensions are accessible. The page displays the list of metric extensions along with target type, owner, production version and deployment information.
3. Select the metric extension to be upgraded.

4. From the **Actions** menu, select **Manage Target Deployments**. The **Manage Target Deployments** page appears showing a list of targets where the metric extension is already deployed.
5. Select the list of targets where the extension is to be upgraded and click **Upgrade**. Enterprise Manager submits a job for the deployment of the newest Published metric extension to the selected targets. A single job is submitted per deployment request.
6. You are automatically redirected to the Pending Operations page, which shows a list of currently scheduled, executing, or failed metric extension deploy operations. Once the deploy operation completes, the entry is removed from the pending operations table.

9.3.15 Creating Repository-side Metric Extensions

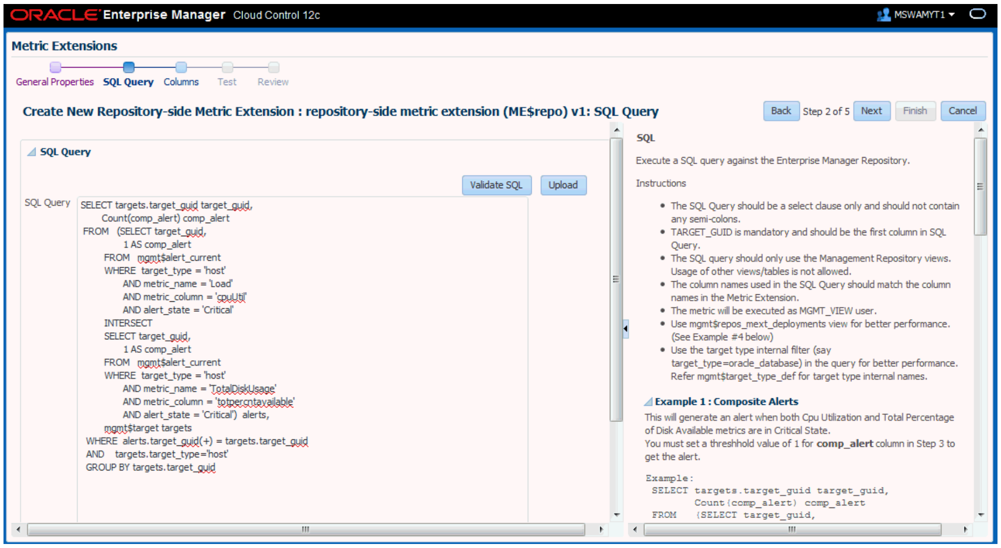
Beginning with Enterprise Manager Release 12.1.0.4, you can create repository-side metric extensions. This type of metric extension allows you to use SQL scripts to extract information directly from the Enterprise Manager repository and raise alerts for the target against which the repository-side extension is run. For example, you can use repository-side metric extensions to raise an alert if the total number of alerts for a host target is greater than 5. Or perhaps, raise an alert if the CPU utilization on that host is greater than 95% AND the number of process running on that host is greater than 500. Repository-side metrics allows you to monitor your Enterprise Manager infrastructure with greater flexibility.

To create a repository-side metric:

1. From the **Enterprise** menu, select **Monitoring,** then select **Metric Extensions.**
2. From the **Create** menu, select **Repository-side Metric Extension**. Enterprise Manager will determine whether you have the Create Extension privilege and guide you through the creation process.
3. Decide on a target type and metric extension name. Be aware that the name (and Display Name) must be unique across a target type.
4. Enter the general parameters.

   Collection Schedule

   You defined the frequency with which metric data is collected and how it is used (Alerting Only or Alerting and Historical Trending) by specifying collection schedule properties.
5. Create the SQL query to be run against the Enterprise Manager Repository. Explicit instructions for developing the query as well as examples are provide on the SQL Query page.



Create New Repository-side Metric Extension : repository-side metric extension (ME$repo) v1: SQL Query

SQL Query

SQL Query

```
SELECT targets.target_guid target_guid,
      Count(comp_alert) comp_alert
 FROM   (SELECT target_guid,
             1 AS comp_alert
        FROM   mgmt$alert_current
        WHERE  target_type = 'host'
             AND metric_name = 'Load'
             AND metric_column = 'cpuUtil'
             AND alert_state = 'Critical'
        INTERSECT
        SELECT target_guid,
             1 AS comp_alert
        FROM   mgmt$alert_current
        WHERE  target_type = 'host'
             AND metric_name = 'TotalDiskUsage'
             AND metric_column = 'totpercntavailable'
             AND alert_state = 'Critical')  alerts,
        mgmt$target targets
  WHERE  alerts.target_guid(+) = targets.target_guid
  AND    targets.target_type='host'
  GROUP BY targets.target_guid
```

SQL

Execute a SQL query against the Enterprise Manager Repository.

Instructions

- The SQL Query should be a select clause only and should not contain any semi-colons.
- TARGET_GUID is mandatory and should be the first column in SQL Query.
- The SQL query should only use the Management Repository views. Usage of other views/tables is not allowed.
- The column names used in the SQL Query should match the column names in the Metric Extension.
- The metric will be executed as MGMT_VIEW user.
- Use mgmt$repos_mext_deployments view for better performance. (See Example #4 below)
- Use the target type internal filter (say target_type=oracle_database) in the query for better performance. Refer mgmt$target_type_def for target type internal names.

Example 1 : Composite Alerts

This will generate an alert when both Cpu Utilization and Total Percentage of Disk Available metrics are in Critical State.
You must set a threshhold value of 1 for **comp_alert** column in Step 3 to get the alert.

```
Example:
 SELECT targets.target_guid target_guid,
        Count(comp_alert) comp_alert
 FROM   (SELECT target_guid,
```

Click **Validate SQL** to test the query.

If you already have a SQL script, you can click **Upload** to load the SQL from an external file.

6. From the Columns page, you can view/edit columns returned by the SQL query. You may edit the columns, however, you cannot add or delete columns from this page.

   - **Column Type**

     A column is either a Key column, or Data column. A Key column uniquely identifies a row in the table. For example, employee ID is a unique identifier of a table of employees. A Data column is any non-unique data in a row. For example, the first and last names of an employee. You can also create rate and delta metric columns based on an existing data column. See *Rate and Delta Metric Columns* below.

   - **Value Type**

     A value type is Number or String. This determines the alert comparison operators that are available, and how Enterprise Manager renders collection data for this metric column.

   - **Alert Thresholds**

     The Comparison Operation, Warning, and Critical fields define an alert threshold.

   - **Alert Thresholds By Key**

     The Comparison Operation, Warning Thresholds By Key, and Critical Thresholds By Key fields allow you to specify distinct alert thresholds for different rows in a table. This option becomes available if there are any Key columns defined. For example, if your metric is monitoring CPU Usage, you can specify a different alert threshold for each distinct CPU. The syntax is to specify the key column values in a comma separated list, the "=" symbol, followed by the alert threshold. Multiple thresholds for different rows can be separated by the semi-colon symbol ";". For example, if the key columns of the CPU Usage metric are cpu_id and core_id, and you want to add a warning threshold of 50% for procecessor1, core1, and a threshold of 60% for

processor2, core2, you would specify:
procecessor1,core1=50;processor2,core2=60

- **Manually Clearable Alert**

  Note: You must expand the Advanced region in order to view the Manually Clearable Alert option.

  If this option is set to true, then the alert will not automatically clear when the alert threshold is no longer satisfied. For example, if your metric is counting the number of errors in the system log files, and you set an alert threshold of 50, if an alert is raised once the threshold is met, the alert will not automatically clear once the error count falls back below 50. The alert will need to be manually cleared in the Alerts UI in the target home page or Incident Manager.

- **Number of Occurrences Before Alert**

  The number of consecutive metric collections where the alert threshold is met, before an alert is raised.

- **Alert Message / Clear Message**

  The message that is sent when the alert is raised / cleared. Variables that are available for use are: %columnName%, %keyValue%, %value%, %warning_threshold%, %critical_threshold%

  You can also retrieve the value of another column by surrounding the desired column name with "%". For example, if you are creating an alert for the cpu_usage column, you can get the value of the core_temperature column by using %core_temperature%. Note that the same alert / clear message is used for warning or critical alerts.

  Note: Think carefully and make sure all Key columns are added, because you cannot create additional Key columns in newer versions of the metric extension. Once you click **Save As Deployable Draft**, the Key columns are final (edits to column display name, alert thresholds are still allowed). You can still add new Data columns in newer versions. Also be aware that some properties of existing Data columns cannot be changed later, including Column Type, Value Type, Comparison Operator (you can add a new operator, but not change an existing operator), and Manually Clearable Alert.

- **Metric Category**

  The metric category this column belongs to.

- Add Delta metric columns based on another metric column

  Example: You want to know the difference in the table space used since the last collection.

  Delta Calculation:

  current metric value - previous metric value

- Add Rate Per Minute metric column based on another metric column

Example: You want to know the average table space usage per minute based on the table space column metric which is collected every 1 hr.

Rate Per Minute Calculation:

(current metric value - previous metric value)/ collection schedule

where the *collection schedule* is in minutes.

- Add Rate Per Five Minutes metric column based on another metric column

  Example: You want to know the average table space usage every five minutes based on the table space column which is collected say every 1 hour]

  Rate Per Five Minute Calculation:

  *[(current metric value - previous metric value)/ collection schedule] * 5*

  where the *collection schedule* is in minutes.

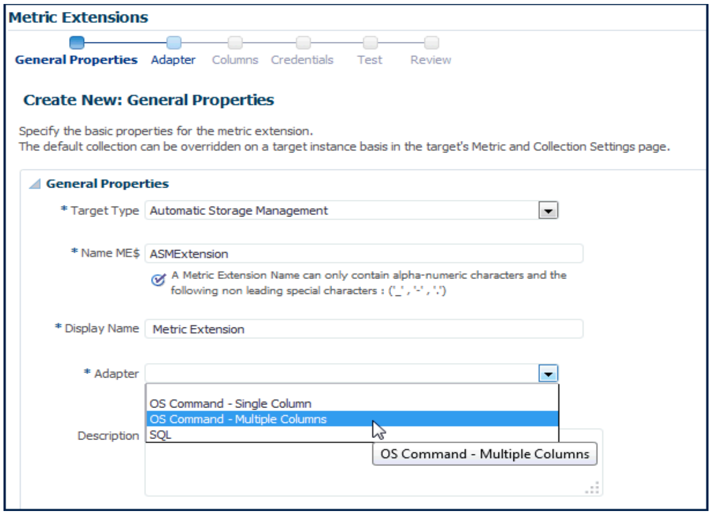
To create a rate/delta metric column, click on an existing data column in the table and then select one of the rate/delta column options from the **Add** menu.

7. From the Test page, add available test targets.
8. Click **Run Test** to validate the metric extension. The extension is deployed to the test targets specified by the user and a real-time collection is executed. Afterwards, the metric extension is automatically undeployed. The results and any errors are added to the **Test Results** region.
9. Repeat the edit /test cycle until the metric extension returns data as expected.
10. Click **Finish**.

9.4 Adapters

Oracle Integration Adapters provide comprehensive, easy-to-use monitoring connectivity with a variety of target types. The adapter enables communication with an enterprise application and translates the application data to standards-compliant XML and back.

The metric extension target type determines which adapters are made available from the UI. For example, when creating a metric extension for an Automatic Storage Management target type, only three adapters (OS Command-Single Column, OS Command-Multiple Columns, and SQL) are available from the UI.



Metric Extensions

Create New: General Properties

Specify the basic properties for the metric extension.
The default collection can be overridden on a target instance basis in the target's Metric and Collection Settings page.

General Properties

* Target Type: Automatic Storage Management

* Name ME$: ASMExtension

A Metric Extension Name can only contain alpha-numeric characters and the following non leading special characters : ('_' , '-' , '.')

* Display Name: Metric Extension

* Adapter:

OS Command - Single Column
OS Command - Multiple Columns
SQL
OS Command - Multiple Columns

Description

A target type's out-of-box metric definition defines the adapters for which it has native support, and only those adapters will be shown in the UI. No other adapters are supported for that target type.

A complete list of all adapters is shown below.

- OS Command Adapter - Single Column
- OS Command Adapter- Multiple Values
- OS Command Adapter - Multiple Columns
- SQL Adapter
- SNMP (Simple Network Management Protocol) Adapter
- JMX Adapter

9.4.1 OS Command Adapter - Single Column

Executes the specified OS command and returns the command output as a single value. The metric result is a 1 row, 1 column table.

Basic Properties

The complete command line will be constructed as: Command + Script + Arguments.

- **Command** - The command to execute. For example, `%perlBin%/perl`. The complete command line will be constructed as: Command + Script + Arguments.
- **Script** - A script to pass to the command. For example, `%scriptsDir%/myscript.pl`. You can upload custom files to the agent, which will be accessible under the `%scriptsDir%` directory.
- **Arguments** - Additional arguments to be appended to the Command.

Advance Properties

- **Input Properties** - Additional properties can be passed to the command through its standard input stream. This is usually used for secure content, such as username or passwords, that you don't want to be visible to other users. For example, you can add the following Input Property:

  `Name=targetName, Value=%NAME%`

  which the command can read through it's standard input stream as "STDINtargetName=<target name>".
- **Environment Variables** - Additional properties can be accessible to the command from environment variables. For example, you can add Environment Variable: `Name=targetType, Value="%TYPE%"`, and the command can access the target type from environment variable "ENVtargetType".

Credentials

- **Host Credentials** - The credential used to launch the OS Command.
- **Input Credentials** - Additional credentials passed to the OS Command's standard input stream.

Example 1

Read the contents of a log file, and dump out all lines containing references to the target.

- **Approach 1** - Use the grep command, and specify the target name using %NAME% parameter.

  ```
  Command = /bin/grep %NAME% mytrace.log
  ```

- **Approach 2** - Run a perl script

  ```
  Command = %perlBin%/perl
  ```

  ```
  Script = %scriptsDir%/filterLog.pl
  ```

  Input Properties:

  ```
    targetName = %NAME%

    targetType = %TYPE%
  ```

filterLog.pl:

```
require "emd_common.pl";

my %stdinVars = get_stdinvars();
my $targetName = $stdinVars{"targetName"};
my $targetType = $stdinVars{"targetType"};
open (MYTRACE, mytrace.log);
foreach $line (<MYTRACE >)
{
    # Do line-by-line processing
}

close (MYTRACE);
```

Example 2

Connect to a database instance from a PERL script and query the HR.JOBS sample schema table.

- Approach 1 - Pass credentials from target type properties into using Input Properties:

  ```
  Command = %perlBin%/perl
  ```

  ```
  Script = %scriptsDir%/connectDB.pl
  ```

  Input Properties:

  ```
    EM_DB_USERNAME = %Username%

    EM_DB_PASSWORD = %Password%

    EM_DB_MACHINE = %MachineName%

    EM_DB_PORT = %Port%

    EM_DB_SID = %SID%
  ```

  connectDB.pl

  ```
  use DBI;
  require "emd_common.pl";

  my %stdinVars = get_stdinvars();
  my $dbUsername = $stdinVars{"EM_DB_USERNAME"};
  my $dbPassword = $stdinVars{"EM_DB_PASSWORD"};
  my $dbMachine = $stdinVars{"EM_DB_MACHINE"};
  ```

```
my $dbPort = $stdinVars{"EM_DB_PORT"};
my $dbSID = $stdinVars{"EM_DB_SID"};

my $dbAddress =
"(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=$dbMachine)(Port=$dbPort))(CONNECT_
DATA=(SID=$dbSID)))";

# Establish Target DB Connection
my $db = DBI->connect('dbi:Oracle:', "$dbUsername@".$dbAddress, "$dbPassword",
    {PrintError => 0, RaiseError => 0, AutoCommit => 0})
    or die (filterOraError("em_error=Could not connect to
$dbUsername/$dbAddress: $DBI::errstr\n", $DBI::err));

my $query = "SELECT JOB_TITLE, MIN_SALARY FROM HR.JOBS";
my $st = $db->prepare($query);
$st->execute();

while ( my ($job_title, $min_sal) = $st->fetchrow_array() )
{
    print "$job_title|$min_sal\n";
}

$db->disconnect
    or warn "disconnect $DBI::errstr\n";

exit 0;
```

- Approach 2 - Pass monitoring credential set using Input Credentials

  `Command = %perlBin%/perl`

  `Script = %scriptsDir%/connectDB.pl`

  Input Credentials:

  `dbCreds = MyCustomDBCreds`

  connectDB.pl

```
use DBI;

require "emd_common.pl";


my %stdinVars = get_stdinvars();
my $credType = getCredType("dbCred", \%stdinVars);
my %credProps = getCredProps("dbCreds", \%stdinVars);
my $dbUsername = $credProps{"DBUserName"};
my $dbPassword = $credProps{"DBPassword"};
```

Example 3

Overriding default monitoring credentials by creating and using a custom monitoring credential set for host target.

Creating host credentials for the host target type:

```
> emcli create_credential_set -set_name=myCustomCreds -target_type=host -auth_
target_type=host -supported_cred_types=HostCreds -monitoring -description='My
Custom Credentials'
```

When you go to the Credentials page of the Metric Extension wizard, and choose to "Specify Credential Set" for Host Credentials, you will see "My Custom Credentials" show up as an option in the drop down list.

Note that this step only creates the Monitoring Credential Set for the host target type, and you need to set the credentials on each target you plan on deploying this metric extension to. You can set credentials from Enterprise Manager by going to Setup, then Security, then Monitoring Credentials. Alternatively, this can be done from the command line.

```
> emcli set_monitoring_credential -target_name=target1 -target_type=host -set_
name=myCustomCreds -cred_type=HostCreds -auth_target_type=host
-attributes='HostUserName:myusername;HostPassword:mypassword'
```

9.4.2 OS Command Adapter- Multiple Values

Executes the specified OS command and returns each command output line as a separate value. The metric result is a multi-row, 1 column table.

For example, if the command output is:

```
em_result=out_x
em_result=out_y
```

then three columns are populated with values 1,2,3 respectively.

Basic Properties

- **Command** - The command to execute. For example, %perlBin%/perl.
- **Script** - A script to pass to the command. For example, `%scriptsDir%/myscript.pl`. You can upload custom files to the agent, which will be accessible under the `%scriptsDir%` directory.
- **Arguments** - Additional arguments to be appended to the Command.
- **Starts With** - The starting string of metric result lines.

  Example: If the command output is:

  ```
  em_result=4354
  update
  test
  ```

  setting *Starts With* = *em_result* specifies that only lines starting with *em_result* will be parsed.

Advanced Properties

- **Input Properties** - Additional properties to be passed to the command through its standard input stream. For example, you can add Input Property: Name=targetName, Value=%NAME%, which the command can read through its standard input stream as "STDINtargetName=<target name>". See usage examples in OS Command Adapter - Single Columns.
- **Environment Variables** - Additional properties can be accessible to the command from environment variables. For example, you can add Environment Variable: Name=targetType, Value="%TYPE%", and the command can access the target type from environment variable "ENVtargetType". See usage examples in OS Command Adapter - Single Columns.

Credentials

- **Host Credentials** - The credential used to launch the OS Command. See usage examples in OS Command Adapter - Single Columns.

- **Input Credentials** - Additional credentials passed to the OS Command's standard input stream. See usage examples in OS Command Adapter - Single Columns.

9.4.3 OS Command Adapter - Multiple Columns

Executes the specified OS command and parses each command output line (delimited by a user-specified string) into multiple values. The metric result is a mult-row, multi-column table.

Example: If the command output is

```
em_result=1|2|3
em_result=4|5|6
```

and the Delimiter is set as "|", then there are two rows of three columns each:

Table 9–1 Multi-Column Output

1	2	3
4	5	6

Basic Properties

The complete command line will be constructed as: Command + Script + Arguments

- **Command** - The command to execute. For example, %perlBin%/perl.
- **Script** - A script to pass to the command. For example, %scriptsDir%/myscript.pl. You can upload custom files to the agent, which will be accessible under the %scriptsDir% directory.
- **Arguments** - Additional arguments.
- **Delimiter** - The string used to delimit the command output.
- **Starts With** - The starting string of metric result lines.

  Example: If the command output is

  ```
  em_result=4354
  out_x
  out_y
  ```

  setting *Starts With = em_result* specifies that only lines starting with *em_result* will be parsed.
- **Input Properties** - Additional properties can be passed to the command through its standard input stream. For example, you can add Input Property: *Name=targetName*, *Value=%NAME%*, which the command can read through it's standard input stream as *STDINtargetName=<target name>*. To specify multiple Input Properties, enter each property on its own line.
- **Environment Variables** - Additional properties can be accessible to the command from environment variables. For example, you can add Environment Variable: *Name=targetType*, *Value="%TYPE%*, and the command can access the target type from environment variable "ENVtargetType".

Advanced Properties

- **Input Properties** - Additional properties can be passed to the command through its standard input stream. For example, you can add Input Property:

Name=targetName, Value=%NAME%, which the command can read through its standard input stream as STDINtargetName=<target name>. See usage examples in OS Command Adapter - Single Columns.

- **Environment Variables** - Additional properties can be accessible to the command from environment variables. For example, you can add Environment Variable: *Name=targetType*, *Value="%TYPE%*, and the command can access the target type from environment variable "ENVtargetType". See usage examples in OS Command Adapter - Single Columns.

Credentials

- **Host Credentials** - The credential used to launch the OS Command. See usage examples in OS Command Adapter - Single Columns
- **Input Credentials** - Additional credentials passed to the OS Command's standard input stream. See usage examples in OS Command Adapter - Single Columns.

9.4.4 SQL Adapter

Executes custom SQL queries or function calls supported against single instance databases and instances on Real Application Clusters (RAC).

Properties

- **SQL Query** - The SQL query to execute. Normal SQL statements should not be semi-colon terminated. For example, SQL Query = "select a.ename, (select count(*) from emp p where p.mgr=a.empno) directs from emp a". PL/SQL statements are also supported, and if used, the "Out Parameter Position" and "Out Parameter Type" properties should be populated.
- **SQL Query File** - A SQL query file. Note that only one of "SQL Query" or "SQL Query File" should be used. For example, %scriptsDir%/myquery.sql. You can upload custom files to the agent, which will be accessible under the %scriptsDir% directory.
- **Transpose Result** - Transpose the SQL query result.
- **Bind Variables** - Declare bind variables used in normal SQL statements here. For example, if the SQL Query = "select a.ename from emp a where a.mgr = :1", then you can declare the bind variable as Name=1, Value=Bob.
- **Out Parameter Position** - The bind variable used for PL/SQL output. Only integers can be specified.

  Example: If the SQL Query is

  ```
  DECLARE
      l_output1 NUMBER;
      l_output2 NUMBER;
  BEGIN
      .....
      OPEN :1 FOR
          SELECT l_output1, l_output2 FROM dual;
  END;
  ```

  you can set Out Parameter Position = 1, and Out Parameter Type = SQL_CURSOR

- **Out Parameter Type** - The SQL type of the PL/SQL output parameter. See comment for Out Parameter Position

Credentials

- **Database Credentials** - The credential used to connect to the database.

Example

Overriding default monitoring credentials by creating and using a custom monitoring credential set for database target.

Creating host credentials for the database target type:

```
> emcli create_credential_set -set_name=myCustomDBCreds -target_type=oracle_
database -auth_target_type=oracle_database -supported_cred_types=DBCreds
-monitoring -description='My Custom DB Credentials'
```

When you go to the Credentials page of the Metric Extension wizard, and choose to "Specify Credential Set" for Database Credentials, you will see "My Custom DB Credentials" show up as an option in the drop down list.

Note that this step only creates the Monitoring Credential Set for the host target type, and you need to set the credentials on each target you plan on deploying this metric extension to. You can set credentials from Enterprise Manager by going to **Setup**, then selecting **Security**, then selecting **Monitoring Credentials**. Alternatively, this can be performed using the Enterprise Manager Command Line Interface.

```
> emcli set_monitoring_credential -target_name=db1 -target_type=oracle_database
-set_name=myCustomDBCreds -cred_type=DBCreds -auth_target_type=oracle_database
-attributes='DBUserName:myusername;DBPassword:mypassword'
```

9.4.5 SNMP (Simple Network Management Protocol) Adapter

Allow Enterprise Manager Management Agents to query SNMP agents for Management Information Base (MIB) variable information to be used as metric data.

Basic Properties

- **Object Identifiers (OIDs)**: Object Identifiers uniquely identify managed objects in a MIB hierarchy. One or more OIDs can be specified. The SNMP adapter will collect data for the specified OIDs. For example, 1.3.6.1.4.1.111.4.1.7.1.1

Advanced Properties

- **Delimiter** - The delimiter value used when specifying multiple OID values for an OID's attribute. The default value is space or \n or \t
- **Tabular Data** - Indicates whether the expected result for a metric will have multiple rows or not. Possible values are TRUE or FALSE. The default value is FALSE
- **Contains V2 Types** - Indicates whether any of the OIDs specified is of SNMPV2 data type. Possible values are TRUE or FALSE. The default value is FALSE. For example, if an OID value specified is of counter64 type, then this attribute will be set to TRUE.

9.4.6 JMX Adapter

Retrieves JMX attributes from JMX-enabled servers and returns these attributes as a metric table.

Properties

- **Metric** -- The MBean ObjectName or ObjectName pattern whose attributes are to be queried. Since this is specified as metric metadata, it needs to be instance-agnostic. Instance-specific key properties (such as *servername*) on the MBean ObjectName may need to be replaced with wildcards.
- **ColumnOrder** -- A semi-colon separated list of JMX attributes in the order they need to be presented in the metric.

Advanced Properties

- **IdentityCol** -- The MBean key property that needs to be surfaced as a column when it is not available as a JMX attribute. For example:

  ```
  com.myCompany:Name=myName,Dept=deptName, prop1=prop1Val, prop2=prop2Val
  ```

  In this example, setting *identityCol* as *Name;Dept* will result in two additional key columns representing Name and Dept besides the columns representing the JMX attributes specified in the *columnOrder* property.
- **AutoRowPrefix** -- Prefix used for an automatically generated row. Rows are automatically generated in situations where the MBean *ObjectName* pattern specified in metric property matches multiple MBeans and none of the JMX attributes specified in the *columnOrder* are unique for each. The *autoRowId* value specified here will be used as a prefix for the additional key column created. For example, if the metric is defined as:

  ```
  com.myCompany:Type=CustomerOrder,* columnOrder
  ```

  is

  ```
  CustomerName;OrderNumber;DateShipped
  ```

  and assuming *CustomerName;OrderNumber;Amount* may not be unique if an order is shipped in two parts, setting *autoRowId* as "ShipItem-" will populate an additional key column for the metric for each row with ShipItem-0, ShipItem-1, ShipItem-2...ShipItem-n.
- **Metric Service** -- True/False. Indicate whether *MetricService* is enabled on a target Weblogic domain. This property would be false (unchecked) in most cases for Metric Extensions except when metrics that are exposed via the Oracle DMS MBean needs to be collected. If *MetricService* is set to true, then the basic property *metric* becomes the *MetricService* table name and the basic property *columnOrder* becomes a semicolon-separated list of column names in the *MetricService* table.

> **Note:** Refer to the Monitoring Using Web Services and JMX chapter in the *Oracle® Enterprise Manager Extensibility Programmer's Reference* for an in-depth example of creating a JMX based Metric Extension.

9.5 Converting User-defined Metrics to Metric Extensions

For targets monitored by Enterprise Manager 12c Agents, both older user-defined metrics and metric extensions will be supported. After release 12c, only metric extensions will be supported. If you have existing user-defined metrics, it is recommended that you migrate them to metric extensions as soon as possible to prevent potential monitoring disruptions in your managed environment.

Migration of user-defined metric definitions to metric extensions is not automatic and must be initiated by an administrator. The migration process involves migrating user-defined metric metadata to metric extension metadata.

Note: Migration of collected user-defined metric historic data is not supported.

After the user-defined metric is migrated to the metric extension and the metric extension has been deployed successfully on the target, the user-defined metric should be either disabled or deleted. Disabling the collection of the user-defined metric will retain the metadata definition of the user-defined metric) but will clear all the open alerts, remove the metric errors and prevent further collections of the user-defined metric. Deleting the user-defined metric will delete the metadata, historic data, clear open alerts and remove metric errors.

9.5.1 Overview

The User Defined Metric (UDM) to Metric Extension (ME) migration replaces an existing UDM with a new or existing ME. The idea behind the migration process is to consolidate UDMs with the same definition that have been created on different targets into a single ME. In addition, MEs support multiple metric columns, allowing the user to combine multiple related UDMs into a single ME.

This migration process is comprised of the following steps:

1. Identify the UDMs that need to be migrated.
2. Use the provided EM CLI commands to create or select a compatible metric extension.
3. Test and publish the metric extension.
4. Deploy the metric extension to all targets and templates where the original UDMs are located. Also update the existing notification rules to refer to the ME.
5. Delete the original UDMs. Note that the historical data and alerts from the old UDM is still accessible from the UI, but the new ME will not inherit them.

Note that the credentials being used by the UDM are NOT migrated to the newly created ME. The user interface allows a user to specify the credential set required by the metric extension. If the ME does not use the default monitoring credentials, the user will need to create a new credential set to accommodate the necessary credentials through the relevant EM CLI commands. This set will then be available in the credentials page of the metric extension wizard.

The migration process is categorized by migration sessions. Each session is responsible for migrating one or more UDMs. The process of migrating an individual session is referred to as a task. Therefore, a session is comprised of one or more tasks. In general terms, the migration involves creating a session and providing the necessary input to complete each tasks within that session. The status of the session and tasks is viewable throughout the workflow.

9.5.2 Commands

A number of EM CLI commands are responsible for completing the various steps of this process. For a more detailed explanation of the command definition, please use the 'EM CLI help <command>' option.

- **list_unconverted_udms** - Lists the UDMs that have yet to be migrated and not in a session
- **create_udmmig_session** - Creates a session to migrate one or more UDMs
- **udmmig_summary** - Lists the migration sessions in progress
- **udmmig_session_details** - Provides the details of a specific session
- **udmmig_submit_metricpics** - Provides a mapping between the UDM and the ME in order to create a new ME or use an existing one
- **udmmig_retry_deploys** - Deploys the ME to the targets where the UDM is present. Note that the ME has to be in a deployable draft or published state for this command to succeed
- **udmmig_request_udmdelete** - Deletes the UDM and completing the migration process

Usage Examples

The following exercise outlines a simple use case to showcase the migration

Consider a system with one host (host1) that has one host UDM (hostudm1) on it. The goal is to create a new ME (me1) that represents the UDM. The sequence of commands would be as follows

```
$ emcli list_unconverted_udms

-------------+----------------------+-----------+--------------------
Type         | Name                 | Metric    | UDM
-------------+----------------------+-----------+--------------------
host         | host1                |UDM        | hostudm1
```

The command indicates that there is only one UDM that has not been migrated or in the process of migration at this stage. Now proceed with the creation of a session.

```
$ emcli create_udmmig_session -name=migration1 -desc="Convert UDMs for host
target" -udm_choice=hostudm1 -target=host:host1

Migration session created - session id is 1
```

The command creates a migration session with name migration1 and the description "convert UDMs for host target". The udm_choice flag indicates the UDM chosen and the target flag describes the target type and the target on which the UDM resides. Migration sessions are identified by session IDs. The current session has an ID of 1.

```
$ emcli udmmig_summary

------+--------------+------------------+------+------+--------+------+--------
ID    | Name         | Description      |#Tgts |Todo  |#Tmpls  |Todo  |IncRules
------+--------------+------------------+------+------+--------+------+--------
1     |migration1    |Convert UDMS      |      | 1/1  |  0     | -/0  | -/0
------+--------------+------------------+------+------+--------+------+--------
```

The command summarizes all the migrations sessions currently in progress. The name and description fields identify the session. The remaining columns outline the number of targets, templates and incident rules that contain references to the UDM that is being converted to a metric extension. The 'Todo' columns indicate the number of targets, templates and incident rules whose references to the UDM are yet to be updated. Since a migration session can be completed over a protracted period of time, the command provides an overview of the portion of the session that was been completed.

```
$ emcli list_unconverted_udms

There are no unconverted udms
```

Since the UDM is part of a migration session, it no longer shows up in the list of unconverted UDMs.

```
$ emcli udmmig_session_details -session_id=1

Name: migration1
Desc: Convert UDMs for host target
Created: <date> <time>
UDM Pick: [hostudm1]
UDMs being converted:
----------+----------+---------+------+------------+---------+---------+-----
Type      |Name      |UDM      |#MC   |Metric      |Column   |DepS     |DelS
----------+----------+---------+------+------------+---------+---------+-----
host      |host1     |hostudm1 |  0   |            |         |WAIT     |WAIT
----------+----------+---------+------+------------+---------+---------+-----
```

The command provides the status of a single migration session. It lists the name of the UDM and the target type and name of the target on which the UDM resides. In addition, it also outlines the metric extensions currently in the EM instance that match the UDM. The user can elect to use one of the existing choices or create an entirely new metric extension.

The system attempts to find compatible metric extensions by matching the properties of the UDM. For example, in the case of a host UDM, the system tries to find a metric extension that has the same command, script and argument fields. In the case of a database UDM, the system attempts to match the SQL query.

Finally, the DepS column indicates whether the metric extension that was matched to the UDM has been deployed to the target on which the UDM is defined. The DelS column tells the user whether the UDM has been deleted after the metric extension has been deployed. As the user proceeds with the migration, the above table is updated from left to right. When the delete status column is set to complete, the migration session has ended.

```
$ emcli udmmig_submit_metricpicks -session_id=1 -input_file=metric_picks:filename

Successfully submitted metric picks for migration session
```

The command instructs the Enterprise Manager instance to use an existing metric extension or create a new one to replace the UDM. The various options are presented through a file, which is filename in the above command. The contents of the file are shown below

"host,host1,hostudm1,N,ME$me1,Usage"

Each line in the file represents a mapping from n UDM to an ME. The line provides the target type, the name of the target, the name of the UDM, a flag to indicate whether the metric extension is new (N) or existing (E), the name of the metric extension (note that ME$ must be prefixed) and the column name.

The types of UDMs supported are:

- Host (host)
- Database (oracle_database)

- RAC (rac_database)

A user can only specify the names of the data columns via the collection item portion of the file. A metric extension created through migration will always have two columns to represent the structure of the UDM. The first column is an index column for single column UDMs while the second column uses the column name mentioned in the file. In the case of two column UDMs, the first column of the ME is termed as the 'KEY' column and the collection name is used for the second column.

At this stage, the metric extension has been created and is visible in the metric extensions library.

```
$ emcli udmmig_session_details -session_id=1

Name: migration1
Desc: Convert UDMs for host target
Created: <date> <time>
UDM Pick: [hostudm1]
Udms being converted:
----------+--------+---------+------+----------+------------+---------+-----
Type      |Name    |UDM      |#MC   |Metric    |Column      |DepS     |DelS
----------+--------+---------+------+----------+------------+---------+-----
host      |host1   |hostudm1 |   1  | ME$me1   | Usage      |WAIT     |WAIT
----------+--------+---------+------+----------+------------+---------+-----

        #MC : There are 1 matches for udms in this session.
        Use emcli udmmig_list_matches to list available matches
```

The session details command indicates that there is one matching metric extension for this UDM (the value of the MC column is 1) and that metric extension is named as ME$me1. At this stage, we are ready to test the metric extension through the library page. Once the testing is complete and the user is satisfied with the metric extension that has been created, it is ready to be deployed. In order to deploy, the metric extension has to be minimally saved as a deployable draft.

```
$ emcli udmmig_retry_deploys -session_id=1 -input_file=metric_tasks:filename2

Metric Deployments successfully submitted
```

Note that the system will trigger a job to automatically deploy the metric extension to all targets where the UDM was present once the metric extension is published. If the user is interested in manually controlling the operation, the above command will perform the necessary steps. The command is similar to the submit_metricpicks option in that a file with the UDM to target mapping is provided. It is referred to by filename2 above. The contents of the file are as follows

"host,host1,hostudm1"

Each line in the file is a mapping from the UDM to the targets type and target on which it resides. Once the command is executed, jobs to deploy the metric extensions to various targets have been launched and can be tracked through the user interface.

```
$ emcli udmmig_request_udmdelete -session_id=1 -input_file=metric_tasks:demo_tasks

Udm deletes successfully submitted
```

The final command deletes the UDMs that were migrated to metric extensions. Note that this command might partially finish based on how many of the deployments were completed when the command was run.

```
$ emcli udmmig_session_details -session_id=1
```

```
Name: migration1
Desc: Convert UDMs for host target
Created: <date > <time>
Completed: <date > <time>
UDM Pick: [hostudm1]
Udms being converted:
--------+----------+---------+------+------------+------------+---------+-----
Type    |Name      |UDM      |#MC   |Metric      |Column      |DepS     |DelS
--------+----------+---------+------+------  ----+------------+---------+-----
host    |host1     |hostudm1 |  1   | ME$me1     | Usage      |COMP   |COMP
--------+----------+---------+------+------------+------------+---------+-----

        #MC : There are 1 matches for udms in this session.
          Use emcli udmmig_list_matches to list available matches
```

The session details command shows that the migration process is indeed complete.

9.6 Metric Extension Command Line Verbs

Metric extensions can be manipulated outside the UI via the Enterprise Manager Command Line Interface (EM CLI). Two categories of verbs are available:

- Metric Extension Verbs
  - *export_metric_extension*: Export a metric extension to an archive file
  - *get_unused_metric_extensions*: Get a list of unused metric extensions.
  - *import_metric_extension*: Import a metric extension archive file.
  - *publish_metric_extension*: Publish a metric extension for use by all administrators.
  - *save_metric_extension_draft*: Save a deployable draft of a metric extension.
- User-defined Metric Migration Verbs
  - *abort_udmmig_session*: Abort (partially) user-defined metric migration session.
  - *analyze_unconverted_udms*: Analyze the unconverted user-defined metrics.
  - *create_udmmig_session*: Create a user-defined metric migration session.
  - *list_unconverted_udms*: List the user-defined metrics that are not yet in a migration session.
  - *udmmig_list_matches*: List the matching metrics per user-defined metric in a specific user-defined metric migration session.
  - *udmmig_request_udmdelete*: Request deletion of user-defined metrics from targets.
  - *udmmig_retry_deploys*: Retry deployment of metric extensions to targets.
  - *udmmig_session_details*: Retrieve the details of a specific user-defined metric migration session.
  - *udmmig_submit_metricpicks*: Select the metrics to replace user-defined metrics in a session.
  - *udmmig_summary*: Summarize the status of all user-defined metric migration sessions.

- *udmmig_update_incrules*: Update user-defined metric incident rules to include replacement metric references.

Metric Extension Verbs

```
  emcli export_metric_extension
       -file_name=<name of the metric extension archive>
       -target_type=<target type of the metric extension>
       -name=<name of the metric extension
       -version=<version of the metric extension>

  Description:
    Export a metric extension archive file.

  Options:
    -file_name=<file name>
      The name of the metric extension archive file to export into.
    -target_type=<target type>
      Target type of the metric extension.
    -name=<name>
      Name of the metric extension.
    -version=<version>
      Version of the metric extension to be exported.


  emcli get_unused_metric_extensions

  Description:
    Get a  list of metric extensions that are deployed to agents but not attached
to any targets.


  emcli import_metric_extension
        -file_name=<name of the metric extension archive>
        -rename_as=<name of the metric extension to import as>

  Description:
    Import a metric extension archive file.

  Options:
    -file_name=<file name>
      The name of the metric extension archive file to be imported.
    -rename_as=<metric extension name>
      Import the metric extension using the specified name, replacing the name
given in the archive.


  emcli publish_metric_extension
       -target_type=<target type of the metric extension>
       -name=<name of the metric extension
       -version=<version of the metric extension>

  Description:
    Publish a metric extension for use by all administrators.
  The metric extension must currently be a deployable draft.

  Options:
    -target_type=<target type>
      Target type of the metric extension.
    -name=<name>
      Name of the metric extension.
    -version=<version>
      Version of the metric extension to be published.


  emcli save_metric_extension_draft
       -target_type=<target type of the metric extension>
       -name=<name of the metric extension
       -version=<version of the metric extension>

  Description:
    Save a deployable draft of a metric extension. The metric
  extension must currently be in editable state. Once saved as
  draft, the metric extension will no longer be editable.

  Options:
    -target_type=<target type>
      Target type of the metric extension.
    -name=<name>
      Name of the metric extension.
    -version=<version>
      Version of the metric extension to be saved to draft.
```

User-Defined Metric Verbs

```
  emcli abort_udmmig_session
        -session_id=<sessionId>
        [-input_file=specific_tasks:<complete path to file>]

  Description:
    Abort the migration of user-defined metrics to MEs in a session

  Options:
    -session_id=<id of the session>
      Specify the id that was returned at time of session created,
      or from the output of udmmig_summary
    [-input_file=specific_tasks:<complete file path>]
      This optional parameter points at a file name that contains a
         target, user-defined metric,
      one per line in the following format:
      <targetType>,<targetName>,<collection name>
      Use targetType=Template to indicate a template
      Use * for collection name to abort all user-defined metrics for a target


  emcli analyze_unconverted_udms [-session_id=<sessionId>]

  Description:
    Analyze user-defined metrics and list unique user-defined metrics, any
possible matches, and
    templates that can apply these matching metric extensions
  Options:
    -session_id=<id of a session to be reanalyzed>
      Not specifying a session id causes the creation of a analysis
      session that contains all unconverted user-defined metrics. You can specify
      this session id in future invocations to get fresh analysis.


  emcli create_udmmig_session
      -name=<name of the session>
      -desc=<description of the session>
      [-udm_choice=<specific udm to convert>]*
      {-target=<type:name of the target to migrate> }*
      | {-input_file=targetList:<complete path to file>};      {-template=<name of
the template to update> }*
      | {-input_file=templateList:<complete path to file>}
      [-allUdms]

  Description:
    Creates a session to migrate user-defined metrics to metric extensions for
targets.

  Options:
    -name=<session name>
      The name of the migration session to be created.
    -desc=<session session description>
      A description of the migration session to be created.
    -udm_choice=<udm name>
      If the session should migrate specific user-defined metrics, specify them
      Otherwise, all user-defined metrics will be migrated
    -target=<type:name of target to migrate>
      The type:name of the target to be updated.
      Multiple values may be specified.
    -input_file=targetList:<complete file path>
      This takes a file name that contains a list of targets,
      one per line in the following format:
      <targetType>:<targetName>
    -template=<name of template to migrate>
      The name of the template to update.Multiple values may be specified
    -input_file=templateList:<complete file path>
      This takes a file name that contains a list of templates,
      one name per line
    -allUdms
      This forces the session to contain all user-defined metrics from targets and
      templates (default behavior just picks those not in a session)

  emcli list_unconverted_udms [-templates_only]

  Description:
    Get the list of all user-defined metrics that are not yet in a migration
session

  Options:
    -templates_only
      Only lists unconverted user-defined metrics in templates.


  emcli udmmig_list_matches
        -session_id=<sessionId>

  Description:
    Lists the matching metrics per user-defined metric in a migration session
  Options:
    -session_id=<id of the session>
      Specify the id that was returned at time of session created,
      or from the output of udmmig_summary


  emcli udmmig_request_udmdelete
        -session_id=<sessionId>
```

```
          -input_file=metric_tasks:<complete path to file>

    Description:
      Delete the user-defined metrics that have been replaced by Metric Extenions

    Options:
      -session_id=<id of the session>
        Specify the id that was returned at time of session created,
        or from the output of udmmig_summary
      -input_file=metric_tasks:<complete file path>
        This takes a file name that contains a target, user-defined metric,
        one per line in the following format:
        <targetType>,<targetName>,<collection name>


    emcli udmmig_retry_deploys
          -session_id=<sessionId>
          -input_file=metric_tasks:<complete path to file>

    Description:
      Retry the deployment of metric extensions to a target

    Options:
      -session_id=<id of the session>
        Specify the id that was returned at time of session created,
        or from the output of udmmig_summary
      -input_file=metric_tasks:<complete file path>
        This takes a file name that contains a target, user-defined metric,
        one per line in the following format:
        <targetType>,<targetName>,<collection name>


    emcli udmmig_submit_metricpicks
          -session_id=<sessionId>
          -input_file=metric_picks:<complete path to file>

    Description:
      Supply the metric picks to use to replace user-defined metrics per target in a
  session

    Options:
      -session_id=<id of the session>
        Specify the id that was returned at time of session created,
        or from the output of udmmig_summary
      -input_file=metric_picks:<complete file path>
        This takes a file name that contains a target, user-defined metric, metric
  pick,
        one per line in the following format:
        <targetType>,<targetName>,<collection name>,[N/E],<metric>,<column>
         using N if a new metric should be created or E if an existing
         metric is referenced.


    emcli udmmig_summary
        [-showAll]

    Description:
      Gets the summary details of all migration sessions in progress

    Options:
```

```
  -showAll
    This prints out all sessions including those that are complete.
    By default, only in-progress sessions are listed.


emcli udmmig_update_incrules
      -session_id=<sessionId>
      -input_file=udm_inc_rules:<complete path to file>

Description:
  Update Incident Rules that reference user-defined metrics with a reference to
  replacing metric extension.

Options:
  -session_id=<id of the session>
    Specify the id that was returned at time of session created,
    or from the output of udmmig_summary
  -input_file=udm_inc_rules:<complete file path>
    This takes a file name that contains rule, user-defined metric, metric,
    one per line in the following format:
    <ruleset id>,<rule id>,<udm name>,<metric name>
```

10

Advanced Threshold Management

There are monitoring situations in which different workloads for a target occur at regular (expected) intervals. Under these conditions, a static alert threshold would prove to be inaccurate. For example, the accurate alert thresholds for a database performing Online Transaction Process (OLTP) during the day and batch processing at night would be different. Similarly, database workloads can change based purely on different time periods, such as weekday versus weekend. In both these situations, fixed, static values for thresholds might result in false alert reporting.

Advanced Thresholds allow you to define and manage alert thresholds that are either adaptive (self-adjusting) or time-based (static).

- *Adaptive Thresholds* are thresholds based on statistical calculations from the target's observed behavior (metrics).
- *Time-based Thresholds* are user-defined threshold values to be used at different times of the day/week to account for changing target workloads.

This chapter covers the following topics:

- Accessing the Advanced Threshold Management Page
- Adaptive Thresholds
- Time-based Static Thresholds
- Determining What is a Valid Metric Threshold

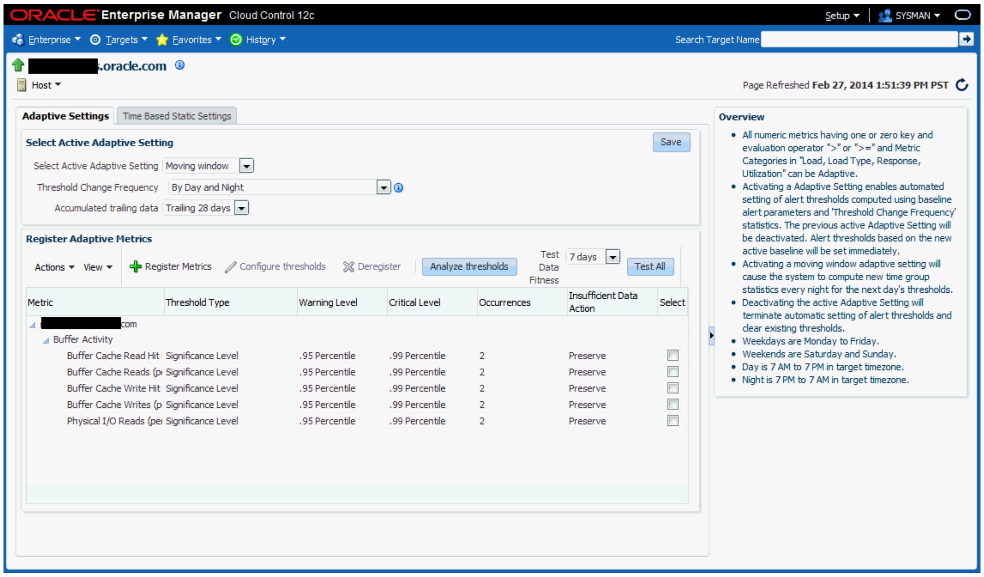
10.1 Accessing the Advanced Threshold Management Page

You manage advanced thresholds from the Enterprise Manager console. The Advanced Threshold Management page allows you to create time-based static thresholds and adaptive thresholds. To access this page:

1. From a target home page (host, for example), navigate to the **Metric Collection and Settings** page.
2. From the Related Links region, click **Advanced Threshold Management**.

   The Advanced Threshold Management page displays as shown in the following graphic.

Figure 10–1 Advanced Threshold Management Page



[redacted].oracle.com

Page Refreshed **Feb 27, 2014 1:51:39 PM PST**

Select Active Adaptive Setting

Select Active Adaptive Setting: Moving window

Threshold Change Frequency: By Day and Night

Accumulated trailing data: Trailing 28 days

Register Adaptive Metrics

Test Data Fitness: 7 days

Metric	Threshold Type	Warning Level	Critical Level	Occurrences	Insufficient Data Action	Select
[redacted]com						
Buffer Activity						
Buffer Cache Read Hit	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Buffer Cache Reads (p	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Buffer Cache Write Hit	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Buffer Cache Writes (p	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Physical I/O Reads (pe	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□

Overview

- All numeric metrics having one or zero key and evaluation operator ">" or ">=" and Metric Categories in "Load, Load Type, Response, Utilization" can be Adaptive.
- Activating a Adaptive Setting enables automated setting of alert thresholds computed using baseline alert parameters and 'Threshold Change Frequency' statistics. The previous active Adaptive Setting will be deactivated. Alert thresholds based on the new active baseline will be set immediately.
- Activating a moving window adaptive setting will cause the system to compute new time group statistics every night for the next day's thresholds.
- Deactivating the active Adaptive Setting will terminate automatic setting of alert thresholds and clear existing thresholds.
- Weekdays are Monday to Friday.
- Weekends are Saturday and Sunday.
- Day is 7 AM to 7 PM in target timezone.
- Night is 7 PM to 7 AM in target timezone.

10.2 Adaptive Thresholds

Adaptive thresholds are statistically computed thresholds that adapt to target workload conditions. Adaptive thresholds apply to all targets (both Agent and repository-monitored).

Important Concepts

Creating an adaptive threshold is based on the following key concepts:

- **Baseline periods**

  For the purpose of performance evaluation, a baseline period is a period of time used to characterize the typical behavior of the system. You compare system behavior over the baseline period to that observed at some other time.

  There are two types of baseline periods:

- **Moving window baseline periods**: Moving window baselines are defined as some number of days prior to the current date. This "window" of days forms a rolling interval that moves with the current time. The number of days that can be used to define moving window baseline in Enterprise Manager are:

  – 7 days

  – 14 days

  – 21 days

  – 30 days

  Example: Suppose you have specified trailing 7 days as a time period while creating moving window baseline. In this situation, the most recent 7-day period becomes the baseline period for all metric observations and comparisons today. Tomorrow, this reference period drops the oldest day and picks up today.

  Moving window baselines allow you to compare current metric values with recently observed history, thus allowing the baseline to incorporate changes to the system over time. Moving window baselines are suitable for systems with predictable workload cycles.

Note: Enterprise Manager computes moving window statistics every day rather than sampling.

10.2.1 Registering Adaptive Threshold Metrics

Adaptive threshold metrics are not immediately available by default; they must be defined and added to the system (registered) in order for them to become available for use by Enterprise Manager. Not all metrics can have adaptive thresholds: Adaptive Threshold metrics must fall into one of the following categories:

- Load
- LoadType
- Utilization
- Response

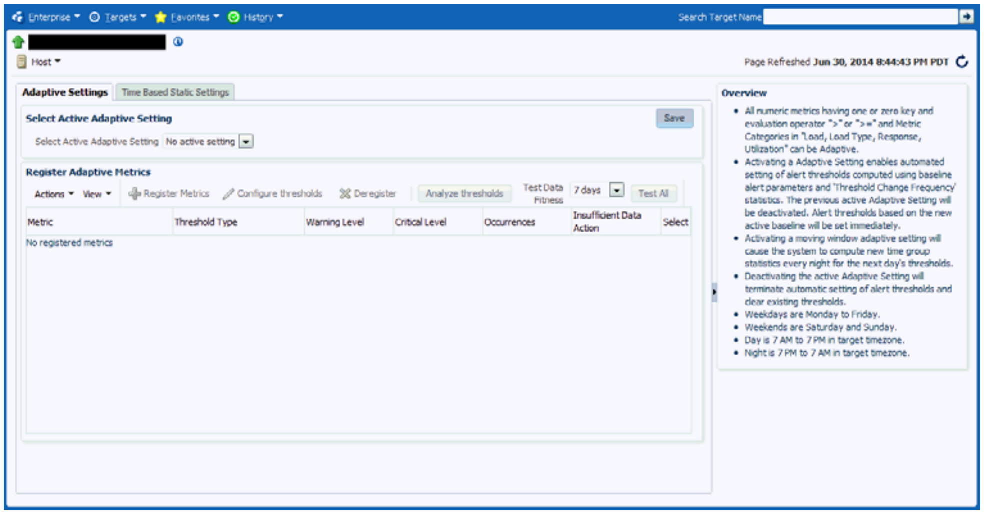
There are two methods for registering adaptive metric:

- Standard Registration Method
- Quick Configuration Method

10.2.1.1 Standard Registration Method

You can manually register adaptive threshold metrics from the Advanced Threshold Management page.

1. From a target menu (Host is used in this example), select **Monitoring** and then **Metric and Collection Settings**.
2. In the Related Links area, click **Advanced Threshold Management**.The Advanced Threshold Management page displays.



[redacted]

Page Refreshed **Jun 30, 2014 8:44:43 PM PDT**

Select Active Adaptive Setting

Select Active Adaptive Setting: No active setting

Register Adaptive Metrics

Test Data Fitness: 7 days

Metric	Threshold Type	Warning Level	Critical Level	Occurrences	Insufficient Data Action	Select
No registered metrics						

Overview

- All numeric metrics having one or zero key and evaluation operator ">" or ">=" and Metric Categories in "Load, Load Type, Response, Utlization" can be Adaptive.
- Activating a Adaptive Setting enables automated setting of alert thresholds computed using baseline alert parameters and 'Threshold Change Frequency' statistics. The previous active Adaptive Setting will be deactivated. Alert thresholds based on the new active baseline will be set immediately.
- Activating a moving window adaptive setting will cause the system to compute new time group statistics every night for the next day's thresholds.
- Deactivating the active Adaptive Setting will terminate automatic setting of alert thresholds and clear existing thresholds.
- Weekdays are Monday to Friday.
- Weekends are Saturday and Sunday.
- Day is 7 AM to 7 PM in target timezone.
- Night is 7 PM to 7 AM in target timezone.

3. From the **Select Active Adaptive Setting** menu, select **Moving Window**, additional controls are displayed allowing you to define the moving window's *Threshold Change Frequency* and the *Accumulated Trailing Data* that will be used to compute the adaptive thresholds.

- *Threshold Change Frequency* (The target timezone is used.)
  - **None**: One set of thresholds will be calculated using past data. This set of thresholds will be valid for the entire week.

    None should be used when there is no usage pattern between daytime versus nighttime or within hours of a day.
  - **By Day and Night**: Two sets of thresholds (day and night) will be calculated using past data. Day thresholds will be calculated using previous day's daytime data, Night thresholds will be calculated using previous day's nighttime data. Thresholds will be changed every day and night.

    By Day and Night should be used when there are distinct performance and usage variations between day hours and night hours.
  - **By Weekdays and Weekend**: Two sets of thresholds (weekdays and weekend) will be calculated using past data. Weekdays thresholds will be calculated using the previous weekdays data. Weekend thresholds will be calculated using the previous weekend data. Thresholds will be changed at start of the weekdays and start of the weekend.
  - **By Day and Night, over Weekdays and Weekend**: Four sets of thresholds will be calculated using past data. *Weekdays Day* thresholds will be calculated using the previous weekday's daytime data, *Weekdays Night* thresholds will be calculated using the previous weekday's nighttime data. *Weekends Day* thresholds will be calculated using previous weekend's daytime data, *Weekends Night* thresholds will be calculated using previous weekend's nighttime data. Thresholds will be changed each day and night.

    Weekday day hours (7a.m. to 7p.m)

    Weekend day hours (7am to 7pm)

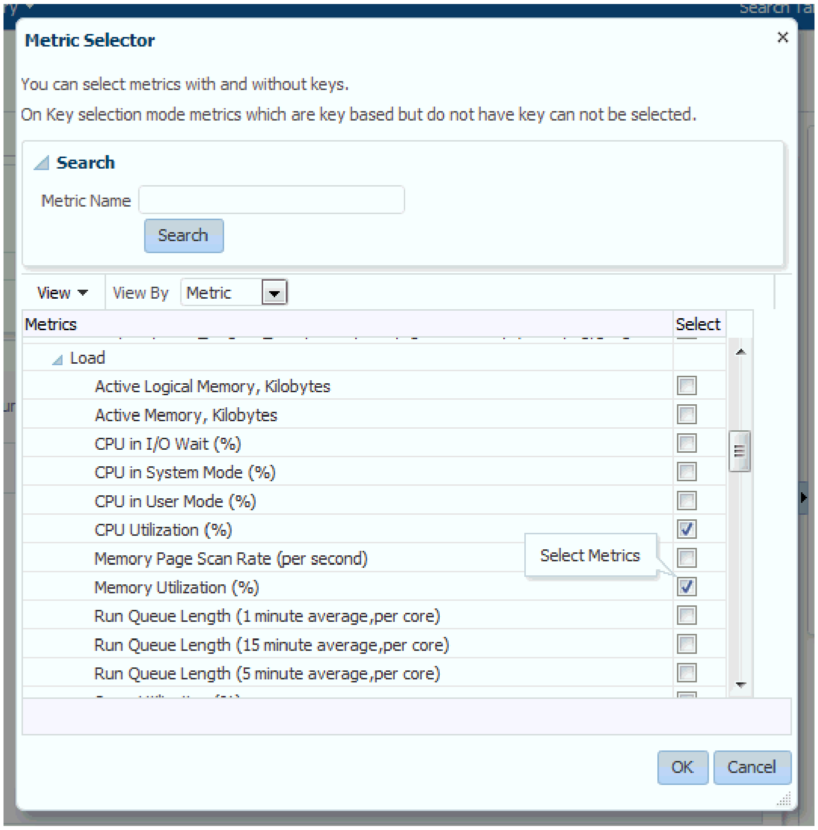
    Weekday night hours (7pm to 7am)

    Weekend night hours (7pm to 7am)
  - **By Day of Week**: Seven sets of thresholds will be calculated, one for each day of the week. Thresholds will be calculated using the previous week's same-day data. Thresholds will be changed every day.

    By Day of Week should be used when there is significant daily variation in usage for each day of week.
  - **By Day and Night, per Day of Week**: Fourteen sets of thresholds will be calculated, one for each day of the week and one for each night of the week. *Day* thresholds will be calculated using previous weeks same-day daytime data, *Night* thresholds will be calculated using the previous week's same-day nighttime data. Thresholds will be changed every day and night each day of the week.
- *Accumulated Trailing Data*

  Total time period for which metric data will be collected. Options are 7, 14, 21, and 28 days. In general, you should select the larger value as the additional data helps in computing more accurate thresholds.

4. The **Register Metrics** button becomes active in the Register Adaptive Metrics region. Click R**egister Metrics.** The Metric Selector dialog displays.



Metric Selector

You can select metrics with and without keys.

On Key selection mode metrics which are key based but do not have key can not be selected.

Search

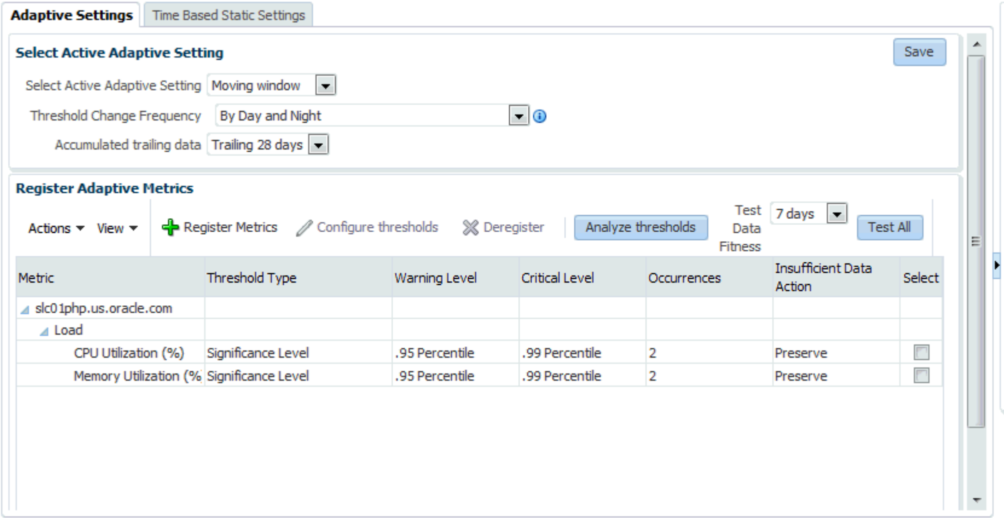
Metric Name

Search

View ▾ View By Metric

Metrics	Select
Load	
Active Logical Memory, Kilobytes	□
Active Memory, Kilobytes	□
CPU in I/O Wait (%)	□
CPU in System Mode (%)	□
CPU in User Mode (%)	□
CPU Utilization (%)	☑
Memory Page Scan Rate (per second)	□
Memory Utilization (%)	☑
Run Queue Length (1 minute average,per core)	□
Run Queue Length (15 minute average,per core)	□
Run Queue Length (5 minute average,per core)	□

5. Select the desired metric(s) and then click **OK**. A confirmation dialog displays stating that the selected metric(s) will be added to this target's Adaptive Setting. Click **Yes** to confirm the action. The selected metrics appear in the Register Adaptive Metrics region.



Select Active Adaptive Setting

Select Active Adaptive Setting: Moving window

Threshold Change Frequency: By Day and Night

Accumulated trailing data: Trailing 28 days

Register Adaptive Metrics

Metric	Threshold Type	Warning Level	Critical Level	Occurrences	Insufficient Data Action	Select
slc01php.us.oracle.com						
Load						
CPU Utilization (%)	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□
Memory Utilization (%	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□

6. Once registered as adaptive metrics, you can then select individual metrics to configure thresholds. When metrics are first registered, by default, Enterprise Manager enables *Significance Level* and sets the warning and critical thresholds at 95 and 99 percentile respectively.

10.2.1.2 Quick Configuration Method

If you have a large number of metrics to configure for many different target types, using the standard registration method can be cumbersome. The *Quick Configuration* method is typically used by integrators to specify predefined settings for specific usage patterns, such as a database running in batch processing mode versus a database running in an online transaction processing (OLTP) mode.

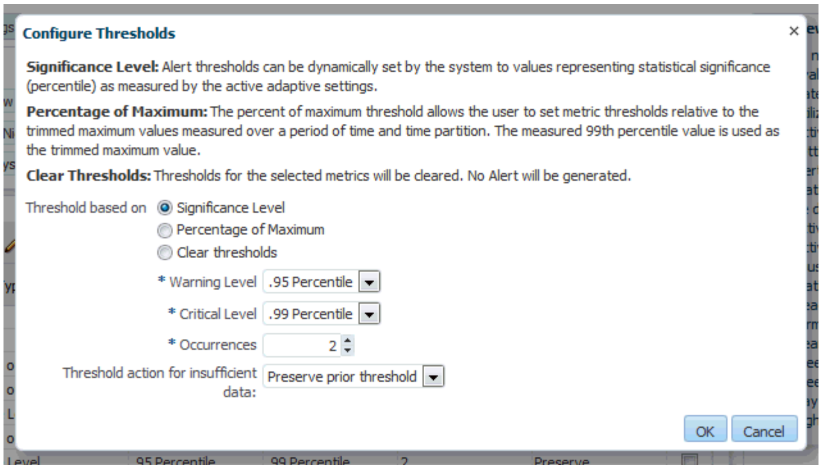
The *Quick Configuration* method of registering adaptive threshold metrics involves updating the target metadata using Enterprise Manager's Metric Registration Service (MRS). The MRS allows you to upload one or more updated target XML metadata files to the Oracle Management Service and have it registered with the Enterprise Manager framework. For more information about the MRS and the Quick Configuration method, see the Oracle® Enterprise Manager Cloud Control Extensibility Programmer's Reference.

10.2.2 Configuring Adaptive Thresholds

Once you have registered the adaptive metrics, you now have the option of configuring the thresholds if the predefined thresholds do not meet your monitoring requirements.

To configure adaptive thresholds:

1. From the Register Adaptive Metrics region, select the metric(s) you wish to configure and click **Configure Thresholds**. The Configure Thresholds dialog displays.



Configure Thresholds

Significance Level: Alert thresholds can be dynamically set by the system to values representing statistical significance (percentile) as measured by the active adaptive settings.

Percentage of Maximum: The percent of maximum threshold allows the user to set metric thresholds relative to the trimmed maximum values measured over a period of time and time partition. The measured 99th percentile value is used as the trimmed maximum value.

Clear Thresholds: Thresholds for the selected metrics will be cleared. No Alert will be generated.

Threshold based on ● Significance Level
○ Percentage of Maximum
○ Clear thresholds

* Warning Level: .95 Percentile

* Critical Level: .99 Percentile

* Occurrences: 2

Threshold action for insufficient data: Preserve prior threshold

2. Choose whether you want your threshold to be based on:

   Significance Level: Thresholds based on significance level use statistical relevance to determine which current values are statistical outliers. The primary reason to use Significance Level for alerting is that you are trying to detect statistical outliers in metric values as opposed to simply setting a threshold value. Hence, thresholds are percentile based. For example, if the significance level is set to .95 for a warning threshold, the metric threshold is set where 5% of the collected metric values fall outside this value and any current values that exceed this value trigger an alert. A higher significance level of .98 or .99 will cause fewer alerts to be triggered.

   Percentage of Maximum: These types of thresholds compute the threshold values based on specified percentages of the maximum observed over the period of time you selected. Percentage-of-maximum-based alerts are generated if the current value is at or above the percentage of maximum you specify. For example, if a maximum value of 1000 is encountered during a time group, and if 105 is specified as the Warning level, then values above 1050 (105% of 1000 = 1050) will raise an alert.

For both types of alerts you can set the **Occurrences** parameter, which is the number of times the metric crosses a threshold value before an alert is generated.

Clear Threshold: Thresholds for the selected metrics will be cleared. No Alert will be generated. Use this option when you do not want any thresholds set for the metrics but you do not want to remove historical data. **Important**: Deregistering metrics will remove the historical data.

Occurrences: Consecutive number of occurrences before raising an alert.

Depending on the option selected, the Warning, Critical, and Occurrence setting options will change.

The **Threshold action for insufficient data** menu allows you set the appropriate action for Enterprise Manager to take if there is not enough data to calculate a valid metric threshold. There are two actions available: *Preserve the prior threshold* and *Suppress Alerts*.

3. Click **OK** to set the changes.

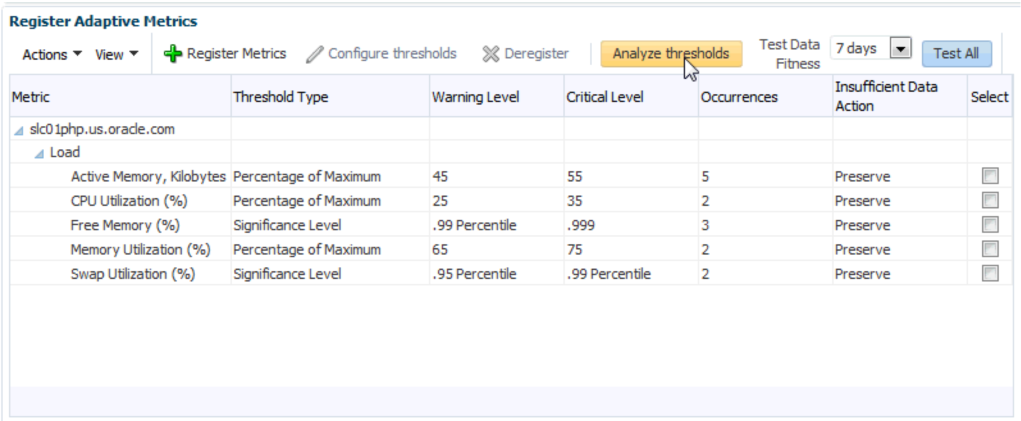
10.2.3 Determining whether Adaptive Thresholds are Correct

Even though Enterprise Manager will use the adaptive threshold settings to determine an accurate target workload-metric threshold match, it is still be necessary to match the metric sampling schedule with the actual target workload. For example, your moving window baseline period (see *Moving Window Baseline Periods* on page 10-2) should match the target workloads. In some situations, you may not know the actual target workloads, in which case setting adaptive thresholds may be problematic.

To help you determine the validity of your adaptive thresholds, Enterprise Manager allows you to analyze threshold using various adaptive settings to determine whether the settings are correct.

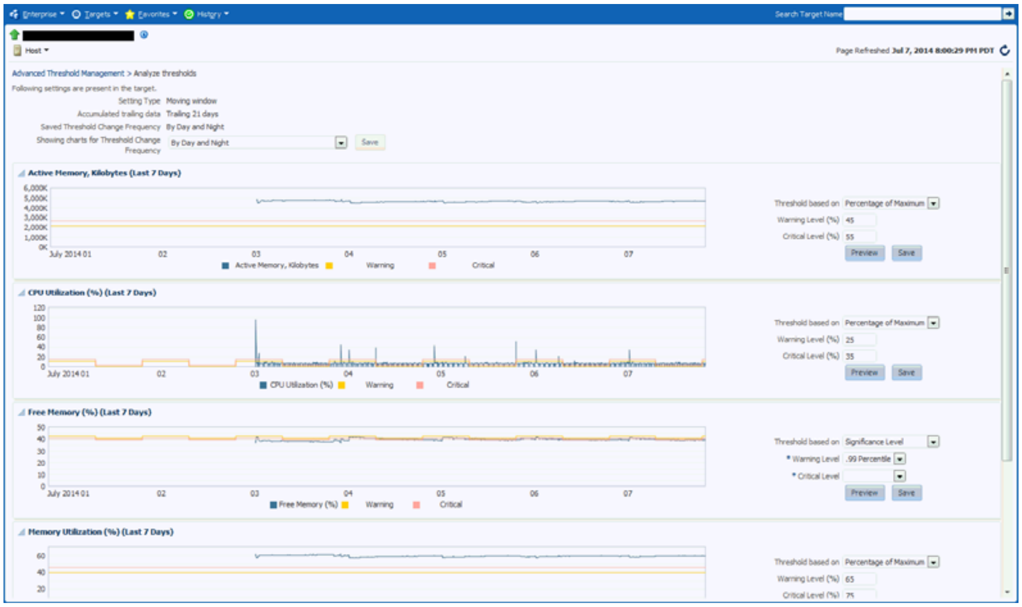
To analyze existing adaptive thresholds:

1. From the Register Adaptive Metrics region, click **Analyze Thresholds**.



Metric	Threshold Type	Warning Level	Critical Level	Occurrences	Insufficient Data Action	Select
slc01php.us.oracle.com						
Load						
Active Memory, Kilobytes	Percentage of Maximum	45	55	5	Preserve	□
CPU Utilization (%)	Percentage of Maximum	25	35	2	Preserve	□
Free Memory (%)	Significance Level	.99 Percentile	.999	3	Preserve	□
Memory Utilization (%)	Percentage of Maximum	65	75	2	Preserve	□
Swap Utilization (%)	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	□

The Analyze Threshold page displays containing historical metric data charts (one for each metric).



[redacted]

Host ▾

Advanced Threshold Management > Analyze thresholds

Following settings are present in the target.

Setting Type: Moving window
Accumulated trailing data: Trailing 21 days
Saved Threshold Change Frequency: By Day and Night
Showing charts for Threshold Change Frequency: By Day and Night

Active Memory, Kilobytes (Last 7 Days) — Threshold based on: Percentage of Maximum; Warning Level (%): 45; Critical Level (%): 55

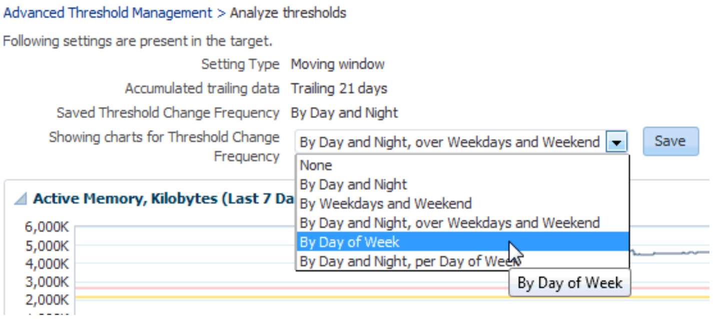
CPU Utilization (%) (Last 7 Days) — Threshold based on: Percentage of Maximum; Warning Level (%): 25; Critical Level (%): 35

Free Memory (%) (Last 7 Days) — Threshold based on: Significance Level; * Warning Level: .99 Percentile; * Critical Level:

Memory Utilization (%) (Last 7 Days) — Threshold based on: Percentage of Maximum; Warning Level (%): 65; Critical Level (%): 75

2. Modify the adaptive threshold parameters to closely match metric threshold settings with the target workload. You can experiment with the following adaptive metric parameters:

Threshold Change Frequency

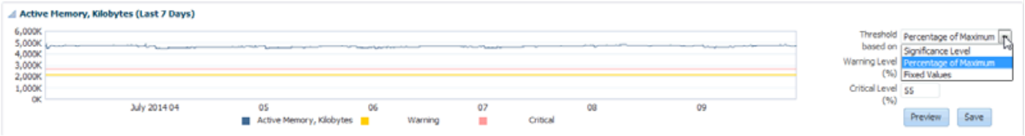

Save
None
By Day and Night
By Weekdays and Weekend
By Day and Night, over Weekdays and Weekend
By Day of Week
By Day and Night, per Day of Week
By Day of Week
Active Memory, Kilobytes (Last 7 Da
6,000K
5,000K
4,000K
3,000K
2,000K

Advanced Threshold Management > Analyze thresholds

Following settings are present in the target.

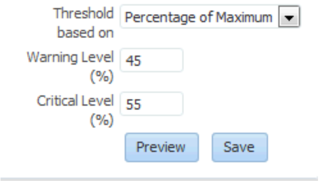
Setting Type: Moving window
Accumulated trailing data: Trailing 21 days
Saved Threshold Change Frequency: By Day and Night
Showing charts for Threshold Change Frequency: By Day and Night, over Weekdays and Weekend

Threshold Based On



Threshold based on: Percentage of Maximum
Warning Level (%):
Critical Level (%): 55

Metric Warning and Critical Thresholds



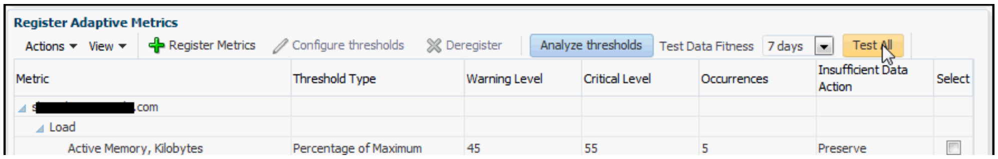
Threshold based on: Percentage of Maximum
Warning Level (%): 45
Critical Level (%): 55

3. Once you are satisfied with the modifications for the Threshold Change Frequency or any of the individual metrics, click **Save** to set the new parameters.

10.2.4 Testing Adaptive Metric Thresholds

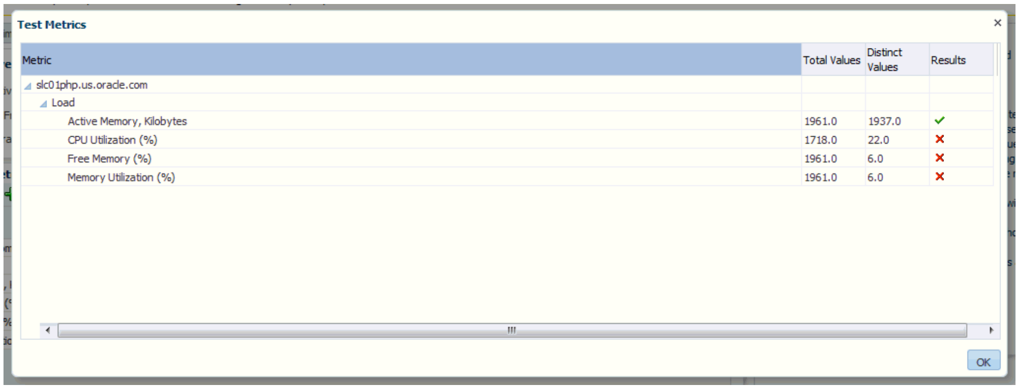
Because adaptive metric thresholds utilize statistical sampling of data over time, the accuracy of the thresholds will rely on the quantity and quality of the data collected. Hence, a sufficient amount of metric data needs to have been collected in order for the thresholds to be valid. To verify whether enough data has been collected for metrics registered with adaptive thresholds, use the **Test All** function.

1. From the Registered Adaptive Metrics regions, click **Test All**.



Metric	Threshold Type	Warning Level	Critical Level	Occurrences	Insufficient Data Action	Select
s[redacted].com						
Load						
Active Memory, Kilobytes	Percentage of Maximum	45	55	5	Preserve	□

Enterprise Manager evaluates the adaptive threshold metrics and then displays the results in the Test Metrics window.



Metric	Total Values	Distinct Values	Results
slc01php.us.oracle.com			
Load			
Active Memory, Kilobytes	1961.0	1937.0	✓
CPU Utilization (%)	1718.0	22.0	✗
Free Memory (%)	1961.0	6.0	✗
Memory Utilization (%)	1961.0	6.0	✗

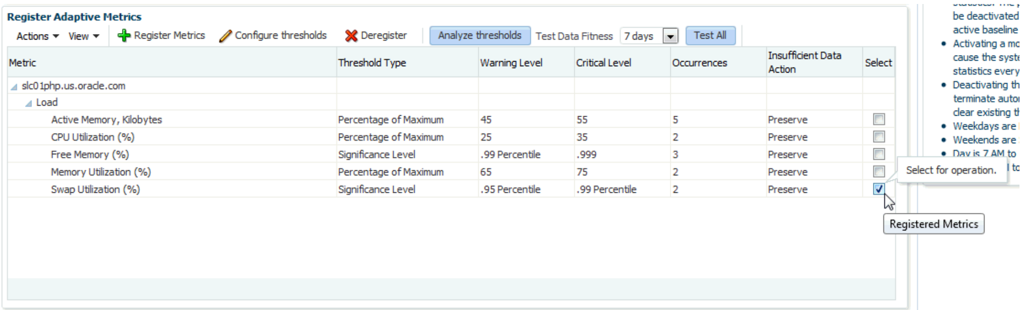
If there is sufficient data collected to compute the adaptive threshold, a green check appears in the results column. A red 'x' appears in the results column if there is insufficient data collected. To resolve this situation, you can use a longer accumulating trailing data window. Additionally, you can have metric data collected more frequently.

2. Click **OK** once you are finished viewing the results.

10.2.5 Deregistering Adaptive Threshold Metrics

If you no longer want specific metrics to be adaptive, you can deregister them at any time. To deregister an adaptive threshold metric:

1. From the Register Adaptive Metrics regions, select the metric(s) you wish to deregister.



Metric	Threshold Type	Warning Level	Critical Level	Occurrences	Insufficient Data Action	Select
slc01php.us.oracle.com						
Load						
Active Memory, Kilobytes	Percentage of Maximum	45	55	5	Preserve	□
CPU Utilization (%)	Percentage of Maximum	25	35	2	Preserve	□
Free Memory (%)	Significance Level	.99 Percentile	.999	3	Preserve	□
Memory Utilization (%)	Percentage of Maximum	65	75	2	Preserve	□
Swap Utilization (%)	Significance Level	.95 Percentile	.99 Percentile	2	Preserve	☑

2. Click **Deregister**. A confirmation displays asking if you want the metric removed from the target’s adaptive setting.
3. Click **Yes**.

10.2.6 Setting Adaptive Thresholds using Monitoring Templates

You can use monitoring templates to apply adaptive thresholds broadly across targets within your environment. For example, using a monitoring template, you can apply adaptive threshold setting for the CPU Utilization metric for all Host targets.

To apply adaptive thresholds using monitoring templates:

1. Create a template out of a target that already has adaptive threshold settings enabled.

   From the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates**.The Monitoring Templates page displays.
2. Click **Create**. The **Create Monitoring Template: Copy Monitoring Settings** page displays.
3. Choose a target on which adaptive thresholds have already been set and click **Continue**.
4. Enter a template **Name** and a brief **Description**. Click **OK**.

Once the monitoring template has been created, you can view or edit the template as you would any other template. To modify, add, or delete adaptive metrics in the template:

1. From the **Enterprise** menu, select **Monitoring** and then **Monitoring Templates**.The **Monitoring Templates** page displays.
2. On the **Monitoring Templates** page, select the monitoring template from the list.
3. From the **Actions** menu, select **Edit Advanced Monitoring Settings**. The **Edit Advanced Monitoring Settings** page displays with the **Adaptive Settings** tab selected.
4. Modify the adaptive metrics as required.

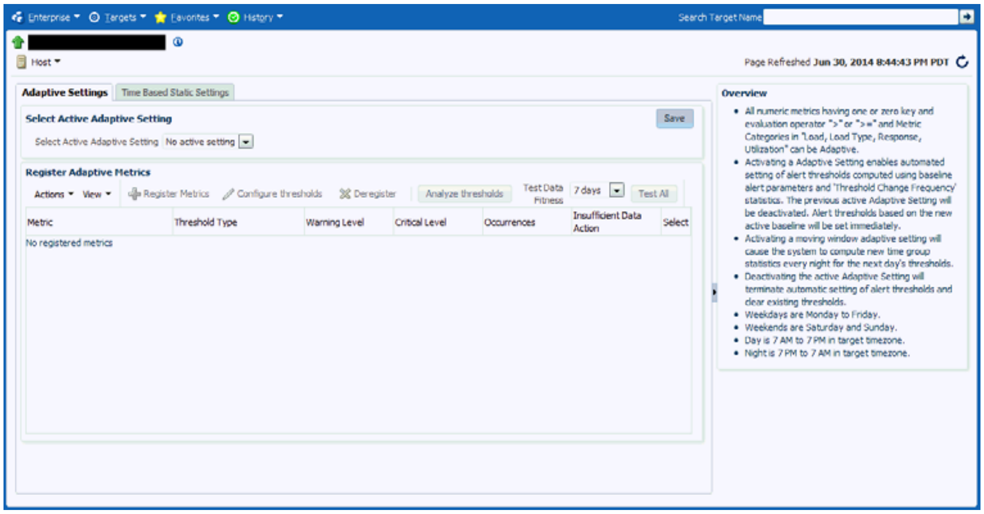
10.3 Time-based Static Thresholds

Time-based static thresholds allow you to define specific threshold values to be used at different times to account for changing workloads over time. Using time-based static thresholds can be used whenever the workload schedule for a specific target is well known or if you know what thresholds you want to specify.

10.3.1 Registering Time-based Static Thresholds

To register metrics with time-based static thresholds:

1. From the target menu (Host is used in this example), select **Monitoring** and then **Metric and Collection Settings**.
2. In the Related Links area, click **Advanced Threshold Management**.The Advanced Threshold Management page displays.



Enterprise ▾ Targets ▾ Favorites ▾ History ▾ Search Target Name

[redacted]

Host ▾

Page Refreshed **Jun 30, 2014 8:44:43 PM PDT**

Adaptive Settings | Time Based Static Settings

Select Active Adaptive Setting Save

Select Active Adaptive Setting: No active setting

Register Adaptive Metrics

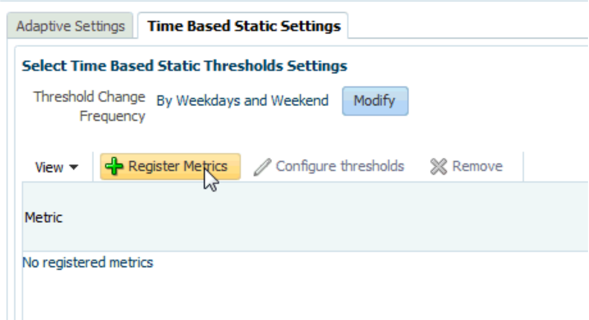
Actions ▾ View ▾ Register Metrics Configure thresholds Deregister Analyze thresholds Test Data Fitness 7 days Test All

Metric	Threshold Type	Warning Level	Critical Level	Occurrences	Insufficient Data Action	Select
No registered metrics						

Overview

- All numeric metrics having one or zero key and evaluation operator ">" or ">=" and Metric Categories in "Load, Load Type, Response, Utilization" can be Adaptive.
- Activating a Adaptive Setting enables automated setting of alert thresholds computed using baseline alert parameters and 'Threshold Change Frequency' statistics. The previous active Adaptive Setting will be deactivated. Alert thresholds based on the new active baseline will be set immediately.
- Activating a moving window adaptive setting will cause the system to compute new time group statistics every night for the next day's thresholds.
- Deactivating the active Adaptive Setting will terminate automatic setting of alert thresholds and clear existing thresholds.
- Weekdays are Monday to Friday.
- Weekends are Saturday and Sunday.
- Day is 7 AM to 7 PM in target timezone.
- Night is 7 PM to 7 AM in target timezone.

3. Click on the **Time Based Static Settings** tab.
4. Select the **Threshold Change Frequency**.
5. Click **Register Metrics**.



Adaptive Settings | **Time Based Static Settings**

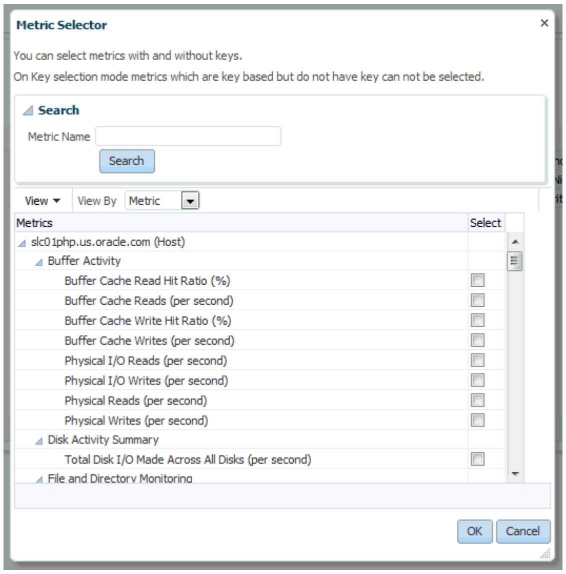
Select Time Based Static Thresholds Settings

Threshold Change Frequency: By Weekdays and Weekend Modify

View ▾ Register Metrics Configure thresholds Remove

Metric
No registered metrics

The Metric Selector dialog displays.



Metric Selector

You can select metrics with and without keys.

On Key selection mode metrics which are key based but do not have key can not be selected.

Search

Metric Name

Search

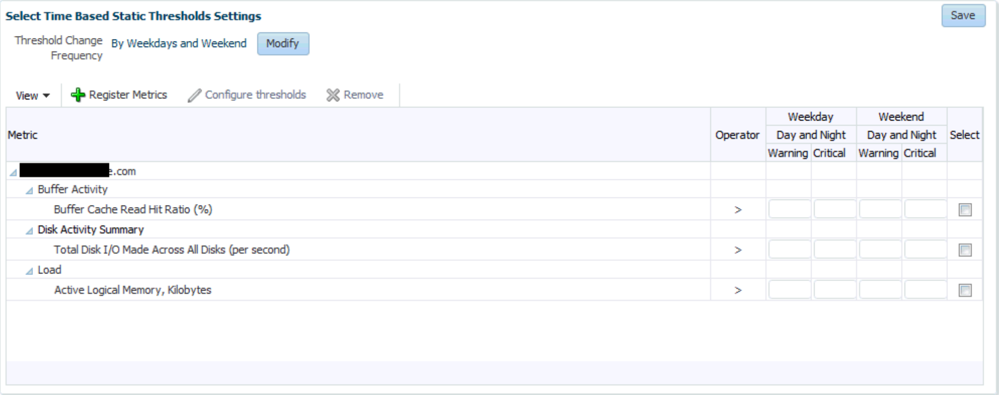
View ▾ View By Metric

Metrics	Select
slc01php.us.oracle.com (Host)	
Buffer Activity	
Buffer Cache Read Hit Ratio (%)	□
Buffer Cache Reads (per second)	□
Buffer Cache Write Hit Ratio (%)	□
Buffer Cache Writes (per second)	□
Physical I/O Reads (per second)	□
Physical I/O Writes (per second)	□
Physical Reads (per second)	□
Physical Writes (per second)	□
Disk Activity Summary	
Total Disk I/O Made Across All Disks (per second)	□
File and Directory Monitoring	

OK Cancel

6. Select the desired metric(s) and click **OK**.

The selected metrics appear in the Registered Metrics table.



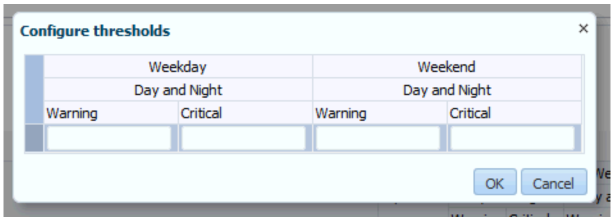
Select Time Based Static Thresholds Settings

Threshold Change Frequency: By Weekdays and Weekend

Metric	Operator	Weekday		Weekend		Select
		Day and Night		Day and Night		
		Warning	Critical	Warning	Critical	
[redacted].com						
Buffer Activity						
Buffer Cache Read Hit Ratio (%)	>					□
Disk Activity Summary						
Total Disk I/O Made Across All Disks (per second)	>					□
Load						
Active Logical Memory, Kilobytes	>					□

7. Enter the desired metric thresholds and click **Save** once you are done.

   If you want to set the thresholds for multiple metrics simultaneously, check the *Select* box for the metrics you want to update and click **Configure Thresholds**. The Configure Thresholds dialog displays.

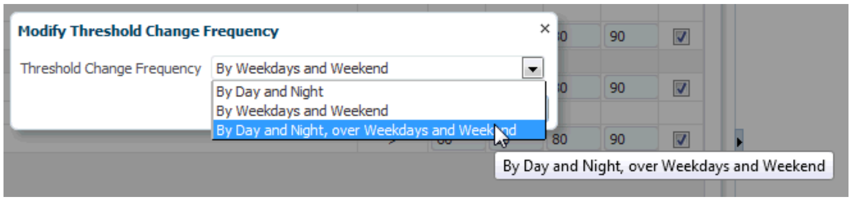


Configure thresholds

Weekday		Weekend	
Day and Night		Day and Night	
Warning	Critical	Warning	Critical

   Enter the revised Warning and Critical threshold values and click **OK**. A confirmation dialog displays stating that existing metric threshold values will be overwritten. Click **Yes**.

8. Optionally, you can change the Threshold Change Frequency. To do so, from the Time Based Static Thresholds Settings page, click **Modify**. The Modify Threshold Change Frequency dialog displays allowing you to select a new change frequency. Select a new frequency and click **OK**.



Modify Threshold Change Frequency

Threshold Change Frequency: By Weekdays and Weekend

×
By Day and Night
By Weekdays and Weekend
By Day and Night, over Weekdays and Weekend
By Day and Night, over Weekdays and Weekend
80
90
90
90

   A confirmation dialog displays stating that changing Threshold Change Frequency will affect all the registered metrics and whether you want to continue. Click **Yes** to proceed.

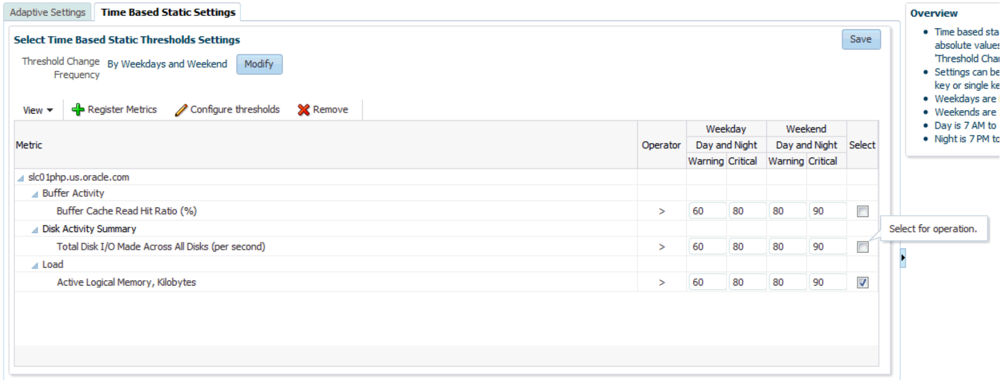
9. Click **Save** to ensure all changes have been saved to the Enterprise Manager repository.

10.3.2 Deregistering Time-based Static Thresholds

If you no longer require time-based static threshold metrics, you can deregister them from the target.

To deregister time-based static metric thresholds:

1. From the Time Based Static Thresholds tab, select the metric(s) you want to deregister.



Select Time Based Static Thresholds Settings

Threshold Change Frequency By Weekdays and Weekend

Metric	Operator	Weekday		Weekend		Select
		Day and Night		Day and Night		
		Warning	Critical	Warning	Critical	
slc01php.us.oracle.com						
Buffer Activity						
Buffer Cache Read Hit Ratio (%)	>	60	80	80	90	☐
Disk Activity Summary						
Total Disk I/O Made Across All Disks (per second)	>	60	80	80	90	☐
Load						
Active Logical Memory, Kilobytes	>	60	80	80	90	☑

Overview

- Time based sta absolute values 'Threshold Cha
- Settings can be key or single ke
- Weekdays are
- Weekends are
- Day is 7 AM to
- Night is 7 PM to

2. Click **Remove**. The metric entry is removed from list of

3. Click **Save** to save the changes to the Enterprise Manager repository.

10.4 Determining What is a Valid Metric Threshold

As previously discussed, static thresholds do not account for expected performance variation due to increased/decreased workloads encountered by the target, such as the workload encountered by a warehouse database target against which OLTP transactions are performed. Workloads can also change based on different time periods, such as weekday versus weekend, or day versus night. These types of workload variations present conditions where fixed static metric threshold values may cause monitoring issues, such as the generation of false and/or excessive metric alerts. Ultimately, your monitoring needs dictate how to best go about obtaining accurate metric thresholds.

11

Utilizing the Job System and Corrective Actions

The Enterprise Manager Cloud Control Job System can automate routine administrative tasks and synchronize components in your environment so you can manage them more efficiently.

This chapter facilitates your usage of the Job System by presenting instructional information in the following sections:

11.1 Job System Purpose and Overview

The Enterprise Manager Job System serves these purposes:

- Automates many administrative tasks; for example: backup, cloning, and patching
- Enables you to create your own jobs using your own custom OS and SQL scripts
- Enables you to create your own multi-task jobs comprised of multiple tasks
- Centralizes environment job scheduling into one robust tool

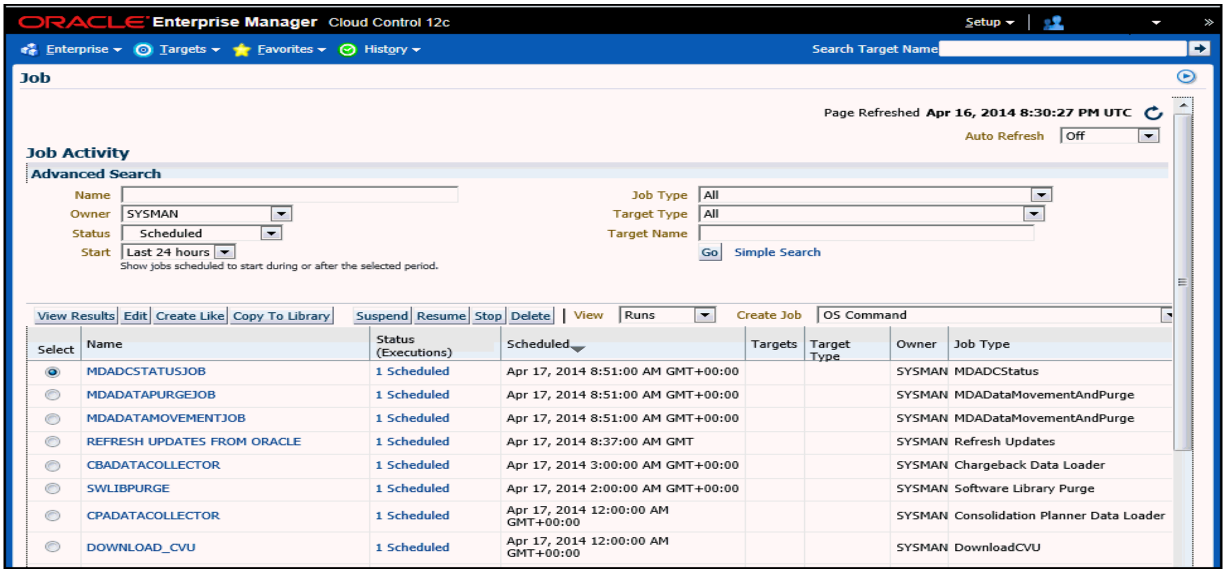
A job is a unit of work that you define to automate commonly-run tasks. Scheduling flexibility is one of the advantages of jobs. You can schedule a job to start immediately or start at a later date and time. You can also run the job once or at a specific interval, such as three times every month.

The Job Activity page (Figure 11–1) is the hub of the Job System. From this page, you can:

- Search for existing job runs and job executions filtered by name, owner, status, scheduled start, job type, target type, and target name
- Create a job

- View or edit the job definition
- Create like, copy to library, suspend, resume, stop, and delete a job
- View results, edit, create like, suspend, resume, retry, stop, and delete a job run or execution

Figure 11–1 Job Activity Page


ORACLE Enterprise Manager Cloud Control 12c
Setup
Enterprise
Targets
Favorites
History
Search Target Name
Job

Page Refreshed **Apr 16, 2014 8:30:27 PM UTC**

Auto Refresh: Off

Job Activity

Advanced Search

Name		Job Type	All
Owner	SYSMAN	Target Type	All
Status	Scheduled	Target Name	
Start	Last 24 hours Show jobs scheduled to start during or after the selected period.	Go	Simple Search

View Results | Edit | Create Like | Copy To Library | Suspend | Resume | Stop | Delete

View: Runs

Create Job: OS Command

Select	Name	Status (Executions)	Scheduled	Targets	Target Type	Owner	Job Type
●	MDADCSTATUSJOB	1 Scheduled	Apr 17, 2014 8:51:00 AM GMT+00:00			SYSMAN	MDADCStatus
○	MDADATAPURGEJOB	1 Scheduled	Apr 17, 2014 8:51:00 AM GMT+00:00			SYSMAN	MDADataMovementAndPurge
○	MDADATAMOVEMENTJOB	1 Scheduled	Apr 17, 2014 8:51:00 AM GMT+00:00			SYSMAN	MDADataMovementAndPurge
○	REFRESH UPDATES FROM ORACLE	1 Scheduled	Apr 17, 2014 8:37:00 AM GMT			SYSMAN	Refresh Updates
○	CBADATACOLLECTOR	1 Scheduled	Apr 17, 2014 3:00:00 AM GMT+00:00			SYSMAN	Chargeback Data Loader
○	SWLIBPURGE	1 Scheduled	Apr 17, 2014 2:00:00 AM GMT+00:00			SYSMAN	Software Library Purge
○	CPADATACOLLECTOR	1 Scheduled	Apr 17, 2014 12:00:00 AM GMT+00:00			SYSMAN	Consolidation Planner Data Loader
○	DOWNLOAD_CVU	1 Scheduled	Apr 17, 2014 12:00:00 AM GMT+00:00			SYSMAN	DownloadCVU

Besides accessing the Job Activity page from the Enterprise menu, you can also access this page from any target-specific menu for all target types by selecting Job Activity from the target type’s menu. When you access this page from these alternate locations, rather than showing the entire list of jobs, the Job Activity page shows a subset of the jobs associated with the particular target.

11.1.1 What Are Job Executions and Job Runs?

The following sections explain the characteristics of each of these.

11.1.1.1 Job Executions

Job executions are usually associated with one target, such as a patch job on a particular database. However, job executions are not always a one-to-one mapping to a target. Some executions have multiple targets, such as comparing hosts. When a job is run against multiple targets, it either runs with all targets in a single execution or with each target in a separate execution.

Job executions are usually associated with one target, such as a patch job on a particular database. These are called single-target jobs because each execution has only one target. However, job executions are not always a one-to-one mapping to a target. Some executions have multiple targets, such as comparing hosts. These jobs are called single-execution jobs, since there is only one execution for all the targets. When a job is run against multiple targets, it runs in one or many executions depending on whether it is a single-execution or single-target job. A few jobs have no target. These jobs are called targetless jobs and run in one execution.

When you submit a job to many targets, it would be tedious to examine the status of each execution of the job against each target. For example, suppose you run a backup job against several databases. A typical question would be: Were all the backup jobs successful, and if not, which jobs failed? If this backup job runs every week, you would want to know which backups were successful and those that failed each week.

11.1.1.2 Job Runs

With the Job System, you can easily get these answers by viewing the *job run*. A job run is the summary of all job executions of a job that ran on a particular scheduled date. For example, if you have a job scheduled for March 5th, you will have a March 5 job run. The job table that shows the job run provides a roll-up of the status of the executions, such as Succeeded, Failed, or Error.

11.1.2 Operations on Job Executions and Job Runs

Besides supporting the standard job operations of create, edit, create like, and delete, the Job System enables you to:

- **Suspend jobs —**

  You can suspend individual executions or entire jobs. For example, you may need to suspend a job if a needed resource was unavailable, or the job needs to be postponed.

  If a job is scheduled to repeat but is suspended past the scheduled repeat time, or a maximum of one day, the execution of this job would be marked "Skipped." A job is also skipped when the scheduled time plus the grace period has passed.

- **Resume jobs —**

  After you suspend a job, any scheduled executions do not occur until you decide to resume the job.

- **Retry all failed executions in a job run —**

  When analyzing individual executions or entire jobs, it is useful to retry a failed execution after you determine the cause of the problem. This alleviates the need to create a new job for that failed execution. When you use the Retry operation in the Job System, Enterprise Manager provides links from the failed execution to the retried execution and vice versa, should it become useful to retroactively examine the causes of the failed executions. Only the most recent retry is shown in the Job Run page.

With regard to job runs, the Job System enables you to:

- **Delete old job runs**
- **Stop job runs**
- **Retry all failed executions in a job run**. Successful executions are never retried.

> **See Also:** For more information on job executions and runs, refer to Enterprise Manager Cloud Control online help.

11.2 Preliminary Considerations

Before proceeding to the procedural information presented in Section 11.3, "Creating Jobs" on page 11-5, it is suggested that you read the topics presented in the sections below:

- Administrator Roles
- Creating Scripts

- Sharing Job Responsibilities
- Submitting Jobs for Groups

11.2.1 Administrator Roles

Enterprise Manager provides the following administrator types:

- **Administrator —** Most jobs and other activities should be initiated using this "normal" user type
- **Super Administrator —** There may be limited use cases for a super administrator to run jobs, create blackouts, or own targets, but generally, this should be avoided.
- **Repository owner (SYSMAN) —** The special repository owner user SYSMAN should almost never own or do any of the tasks listed for the other two types above. This user should only be reserved for top-level actions, such as setting up the site and so forth.

11.2.2 Creating Scripts

Besides predefined job tasks, you can define your own job tasks by writing code to be included in OS and SQL scripts. The advantages of using these scripts include:

- When defining these jobs, you can use target properties.
- When defining these jobs, you can use the job library, which enables you to share the job and make updates as issues arise. However, you need to resubmit modified library jobs for them to take effect.
- You can submit the jobs against multiple targets.
- You can submit the jobs against a group. The job automatically keeps up with changes to group membership.
- For host command jobs, you can submit to a cluster.
- For SQL jobs, you can submit to a Real Application Cluster.

11.2.3 Sharing Job Responsibilities

To allow you to share job responsibilities, the Job System provides job privileges. These job privileges allow you to share the job with other administrators. Using privileges, you can:

- Grant access to the administrators who need to see the results of the job.
- Grant Full access to the administrators who may need to edit the job definition or control the job execution (suspend, resume, stop).

You can grant these privileges on an as-needed basis.

11.2.4 Submitting Jobs for Groups

Rather than listing a large number of targets individually, you can use a group as the target of a job. All member targets in the group that match the selected target type of the job are selected as actual targets of the job when it runs. If the membership of the group changes, the actual target list of the job changes with it. If the job repeats, each iteration (or "run") of the job executes on the matching targets in the group at the time of the run.

Overriding the Target Type Selection

To override the target type selection for a group, set targetType=<override_target_type> in the input file for the create_job verb. For example, the default target type for OSCommand jobs is "host". To submit a job against a group of databases, specify:

```
target_list=my_db_group:composite
targetType=oracle_database
```

Note that any targets in the group that do not match the target type selected are ignored.

See Also: Chapter 6, "Managing Groups"

11.3 Creating Jobs

Your first task in creating a job from the Job Activity page is to choose a job type, which the next section, Selecting a Job Type, explains. The most typical job types are OS command jobs, script jobs, and multi-task jobs, which are explained in these subsequent sections:

- Creating an OS Command Job
- Creating a SQL Script Job
- Creating a Multi-task Job

11.3.1 Selecting a Job Type

Using the Job System, you can create a job by selecting one of the job types from the Create Job drop-down in the Job Activity page. The most commonly used types are as follows:

- **OS Command** — Runs an operating system command or script.
- **SQL Script** — Runs a user-defined SQL or PL/SQL script.
- **Multi-Task** — Use to specify primary characteristics for multi-task jobs or corrective actions. Multi-task jobs enable you to create composite jobs by defining tasks, with each task functioning as an independent job. You edit and define tasks similarly to a regular job.

11.3.2 Creating an OS Command Job

Use this type of job to run an operating system command or script. Tasks and their dependent steps for creating an OS command are discussed below.

Task 1 Initiate Job Creation

1. From the Enterprise menu, select **Jobs**, then **Job Activity.**
2. Select **OS Command** from the Create Job drop-down, then click **Go**. The **General property page** of the Create OS Command Job page appears.

Task 2 Specify General Job Information

Perform these steps on the General property page:

1. Provide a required Name for the job, then select a Target Type from the drop-down.

   After you have selected a target of a particular type for the job, only targets of that same type can be added to the job. If you change target types, the targets you have populated in the Targets table disappear, as well as parameters and credentials for the job.

If you specify a composite as the target for this job, the job executes only against targets in the composite that are of the selected target type. For example, if you specify a target type of host and a group as the target, the job only executes against the hosts in the group, even if there are other non-host targets in the group. You can also include clusters in the target list if they are of the same base target type. For example, a host cluster would be selected if the target type is "host" and a RAC database would be selected if the target type is database.

2. Click **Add**, then select one or more targets from the Search and Select: Targets pop-up window. The targets now appear in the Targets table.
3. Click the **Parameters** property page link.

Task 3 Specify Parameters

Perform these steps on the Parameters property page:

1. Select either **Single Operation** or **Script** from the Command Type drop-down.

   The command or script you specify executes against each target specified in the target list for the job. The Management Agent executes it for each of these targets.

   Depending on your objectives, you can choose one of the following options:

   - Single Operation to run a specific command
   - Script to run an OS script and optionally provide an interpreter, which processes the script; for example, %perlbin%/perl or /bin/sh .

   Sometimes, a single command line is insufficient to specify the commands to run, and you may not want to install and update a script on all hosts. In this case, you can use the Script option to specify the script text as part of the job.

2. Based on your objectives, follow the instructions in Section 11.3.2.1, "Specifying a Single Operation" or Section 11.3.2.2, "Specifying a Script".
3. Click the **Credentials** property page link.

> **Note:** The OS Command relies on the target host's shell to execute the command/interpreter specified. On *nix systems, it is /bin/sh -c and on Windows systems, it is cmd /c. The command line specified is interpreted by the corresponding shell.

Task 4 Specify Credentials - (optional)

You do not need to provide input on this page if you want to use the system default of using preferred credentials.

On the Credentials property page, you can specify the credentials that you want the Oracle Management Service to use when it runs the OS Command job against target hosts. The job can use either the job submitter's preferred host-based credentials for the selected targets, or you can specify other credentials to override the preferred credentials.

You do not need to provide input on this page if you have already set preferred credentials.

Tip: preferred credentials are useful when a job is submitted on multiple targets and each target needs to use different credentials for authentication.

- **To use preferred credentials:**

  1. Select the **Preferred Credential** radio button, which is the default selection.

     If the target for the OS Command job is a host or host group, the preferred host credentials are used. You specify these for the host target on the Preferred Credentials page, and they are different from the host credentials for the host on which the database resides.

  2. Select either **Normal Host Credentials** or **Privileged Host Credentials** from the Host Credentials drop-down.

     You specify these separately on the Preferred Credentials page, which you can access by selecting **Security** from the **Setup** menu, then **Preferred Credentials**. The Preferred Credentials page appears, where you can click the Manage Preferred Credentials button to set credentials.

- **To use named credentials:**

  1. Select the **Named Credential** radio button to override database or host preferred credentials.

     The drop-down list is a pre-populated credential set with values saved with names. These are not linked to targets, and you can use them to provide credential and authentication information to tasks.

- **To use other credentials:**

  1. Select the **New Credential** radio button to override previously defined preferred credentials.

     Note that override credentials apply to all targets. This applies even for named credentials.

  2. Optionally select Sudo or PowerBroker as the run privilege.

     Sudo enables you to authorize certain users (or groups of users) to run some (or all) commands as root while logging all commands and arguments. PowerBroker provides access control, manageability, and auditing of all types of privileged accounts.

     If you provide Sudo or PowerBroker details, they must be applicable to all targets. It is assumed that Sudo or PowerBroker settings are already applied on all the hosts on which this job is to run.

     See your Super Administrator about setting up these features if they are not currently enabled.

Tip: For information on using Sudo, see the Sudo Manual at:

`http://www.sudo.ws/sudo/man/1.7.4p6/sudo.man.html`

For information on using PowerBroker, see the PowerBroker Desktops User Guide at:

`http://www.ubm-global.com/docs/powerbroker/PBWD_User_Guide_V5%200.pdf`

Task 5 Schedule the Job - (optional)

You do not need to provide input on this page if you want to proceed with the system default of running the job immediately after you submit it.

1. Select the type of schedule:

   - **One Time (Immediately)**

     If you do not set a schedule before submitting a job, Enterprise Manager executes the job immediately with an indefinite grace period. You may want to run the job immediately, but specify a definite grace period in case the job is unable to start for various reasons, such as a blackout, for instance.

     A grace period is a period of time that defines the maximum permissible delay when attempting to start a scheduled job. The job system sets the job status to Skipped, if it cannot start the execution between the scheduled time and the time equal to the scheduled time plus the grace period, or within the grace period from the scheduled time.

   - **One Time (Later)**

     – Setting up a custom schedule:

     You can set up a custom schedule to execute the job at a designated time in the future. When you set the Time Zone for your schedule, the job runs simultaneously on all targets when this time zone reaches the start time you specify. If you select each target's time zone, the job runs at the scheduled time using the time zone of the managed targets. The time zone you select is used consistently when displaying date and time information about the job, such as on the Job Activity page, Job Run page, and Job Execution page.

     For example, if you have targets in the Western United States (US Pacific Time) and Eastern United States (US Eastern Time), and you specify a schedule where Time Zone = US Pacific Time and Start Time = 5:00 p.m., the job runs simultaneously at 5:00 p.m. against the targets in the Western United States and at 8:00 p.m. against the targets in the Eastern United States. If you specify 5:00 p.m. in the Agent time zone, the executions do not run concurrently. The EST target would run 3 hours earlier.

     – Specifying the Grace Period:

     The grace period controls the latest start time for the job in case the job is delayed. A job might not start for many reasons, but the most common reasons are that the Agent was down or there was a blackout. By default, jobs are scheduled with indefinite grace periods.

     A job can start any time before the grace period expires. For example, a job scheduled for 1 p.m. with a grace period of 1 hour can start any time before 2 p.m., but if it has not started by 2 p.m., it is designated as skipped.

   - **Repeating**

     – Defining the repeat interval:

     Specify the Frequency Type (time unit) and Repeat Every (repeat interval) parameters to define your job's repeat interval. The Repeat Until options are as follows:

     Note that both the end date and time determine the last execution. For example, for a job that runs daily at 6 p.m., where...

Start Time is June 1, 2010 at 6 p.m.
End Time is June 30, 2010 at 4 a.m.

... the last execution runs on June 29, not June 30, since the June 30 end time occurs before the daily time of the job.

- eart:

  See the description above for Grace Period under the One Time schedule type.

2. Click the **Access** property page link.

Task 6 Specify Who Can Access the Job - (optional)

You do not need to provide input on this page if you want to proceed with the system default of not sharing the job. The table shows the access that administrators and roles have to the job. Only the job owner (or Super Administrator) can make changes on the Job Access page.

1. Change access levels for administrators and roles, or remove administrators and roles. Your ability to make changes depends on your function.

   If you are a job owner, you can:

   - Change the access of an administrator or role by choosing the Full or View access privilege in the Access Level column in the table.
   - Remove all access to the job for an administrator or role by clicking the icon in the Remove column for the administrator or role. All administrators with Super Administrator privileges have the View access privilege to a job. If you choose to provide access privileges to a role, you can only provide the View access privilege to the role, not the Full access privilege. For private roles, it is possible to grant Full access privileges.

   If you are a Super Administrator, you can:

   - Grant View access to other Enterprise Manager administrators or roles.
   - Revoke all administrator access privileges.

   > **Note:** Neither the owner nor a super user can revoke View access from a super user. All super users have View access.

   For more information on access levels, see Section 11.3.2.3, "Access Level Rules".

2. Click **Add** to add administrators and roles. The Create Job Add Administrators and Roles page appears.

   a. Specify a **Name** and **Type** in the Search section and click **Go**. If you just click Go without specifying a Name or Type, all administrators and roles in the Management Repository appear in the table.

   The value you specify in the Name field is not case-sensitive. You can specify either * or % as a wildcard character at any location in a string (the wildcard character is implicitly added to the end of any string). For example, if you specify %na in the Name field, names such as ANA, ANA2, and CHRISTINA may be returned as search results in the Results section.

   b. Select one or more administrators or roles in the Results section, then click **Select** to grant them access to the job. Enterprise Manager returns to the

Create Job Access page or the Edit Job Access page, where you can modify the access of administrators and roles.

3. Define a notification rule.

   You can use the Notification system (rule creation) to easily associate specific jobs with a notification rule. The Cloud Control Notification system enables you to define a notification rule that sends e-mail to the job owner when a job enters one of these chosen states:

   - Scheduled
   - Running
   - Suspended
   - Succeeded
   - Problems
   - Action Required

   Note: Before you can specify notifications, you need to set up your email account and notification preferences. See Chapter 4, "Using Notifications" for this information.

Task 7 Conclude Job Creation

At this point, you can either submit the job for execution or save it to the job library.

- **Submitting the job —**

  Click **Submit** to send the active job to the job system for execution, and then view the job's execution status on the main Job Activity page. If you are creating a library job, Submit saves the job to the library and returns you to the main Job Library page where you can edit or create other library jobs.

  If you submit a job that has problems, such as missing parameters or credentials, an error appears and you will need to correct these issues before submitting an active job. For library jobs, incomplete specifications are allowed, so no error occurs.

  Note: If you click Submit without changing the access, only Super Administrators can view your job.

- **Saving the job to the library —**

  Click **Save to Library** to the job to the Job Library as a repository for frequently used jobs. Other administrators can then share and reuse your library job if you provide them with access privileges. Analogous to active jobs, you can grant View or Full access to specific administrators. Additionally, you can use the job library to store:

  – Basic definitions of jobs, then add targets and other custom settings before submitting the job.

  – Jobs for your own reuse or to share with others. You can share jobs using views or giving Full access to the jobs.

  – Critical jobs for resubmitting later, or revised versions of these jobs as issues arise.

11.3.2.1 Specifying a Single Operation

Note: The following information applies to step 2 in Task 3, "Specify Parameters" on page 11-6.

Enter the full command in the **Command** field. For example:

```
/bin/df -k /private
```

Note the following points about specifying a single operation:

- You can use shell commands as part of your command. The default shell for the platform is used, which is /bin/sh for Linux and cmd/c for Windows.

  ```
  ls -la /tmp > /tmp/foobar.out
  ```

- If you need to execute two consecutive shell commands, you must invoke the shell in the Command field and the commands themselves in the OS Script field. You would specify this as follows in the Command field:

  ```
  sleep 3; ls
  ```

- The job status depends on the exit code returned by the command. If the command execution returns 0, the job returns a status of Succeeded. If it returns any other value, it returns a job status of Failed.

11.3.2.2 Specifying a Script

Note: The following information applies to step 2 in Task 3, "Specify Parameters" on page 11-6.

The value you specify in the OS Script field is used as stdin for the command interpreter, which defaults to /bin/sh on Linux and cmd/c on Windows. You can override this with another interpreter; for example: %perlbin%/perl. The shell scripts size is limited to 2 GB.

To control the maximum output size, set the mgmt_job_output_size_limit parameter in MGMT_PARAMETERS to the required limit. Values less than 10 KB and greater than 2 GB are ignored. The default output size is 10 MB.

The job status depends on the exit code returned by the last command in the script. If the last command execution returns 0, the job returns a status of Succeeded. If it returns any other value, it returns a job status of Failed. You should implement proper exception handling in the script and return non-zero exit codes when appropriate. This will avoid situations in which the script failed, but the job reports the status as Succeeded.

You can run a script in several ways:

- **OS Scripts** — Specify the path name to the script in the OS Script field. For example:

  OS Script field: /path/to/mycommand
  Interpreter field:

- **List of OS Commands** — You do not need to enter anything in the Interpreter field for the following example of standard shell commands for Linux or Unix systems. The OS's default shell of /bin/sh or cmd/c will be used.

  ```
  /usr/local/bin/myProg arg1 arg2
  mkdir /home/$USER/mydir
  cp /dir/to/cp/from/file.txt /home/$USER/mydir
  /usr/local/bin/myProg2 /home/$USER/mydir/file.txt
  ```

  When submitting shell-based jobs, be aware of the syntax you use and the targets you choose. This script does not succeed on NT hosts, for example.

- **Scripts Requiring an Interpreter** — Although the OS shell is invoked by default, you can bypass the shell by specifying an alternate interpreter. For example, you can run a Perl script by specifying the Perl script in the OS Script field and the location of the Perl executable in the Interpreter field:

  OS Script field: <Enter-Perl-script-commands-here>
  Interpreter field: %perlbin%/perl

  The following example shows how to run a list of commands that rely on a certain shell syntax:

  ```
  setenv VAR1 value1
  setenv VAR2 value2
  /user/local/bin/myProg $VAR1 $VAR2
  ```

  You would need to specify csh as the interpreter. Depending on your system configuration, you may need to specify the following string in the Interpreter field:

  ```
  /bin/csh
  ```

  You have the option of running a script for a list of Windows shell commands, as shown in the following example. The default shell of cmd/c is used for Windows systems.

  ```
  C:\programs\MyApp arg1 arg2
  md C:\MyDir
  copy C:\dir1x\copy\from\file.txt \home\$USER\mydir
  ```

11.3.2.3 Access Level Rules

> **Note:** The following rules apply to Task 6, "Specify Who Can Access the Job - (optional)" on page 11-9.

- Super Administrators always have View access on any job.
- The Enterprise Manager administrator who owns the job can make any access changes to the job, except revoking View from Super Administrators.
- Super Administrators with a View or Full access level on a job can grant View (but not Full) to any new user. Super Administrators can also revoke Full and View from normal users, and Full from Super Administrators.
- Normal Enterprise Manager administrators with Full access levels cannot make any access changes on the job.
- If the job owner performs a Create Like operation on a job, all access privileges for the new job are identical to the original job. If the job owner grants other administrators View or Full job access to other administrators, and any of these

administrators perform a Create Like operation on the job, ALL administrators will, by default, have View access on the newly created job.

11.3.3 Creating a SQL Script Job

The basic process for creating a SQL script job is the same as described in Section 11.3.2, "Creating an OS Command Job." The following sections provide supplemental information specific to script jobs:

- Specifying Targets
- Specifying Options for the Parameters Page
- Specifying Host and Database Credentials
- Returning Error Codes from SQL Script Jobs

11.3.3.1 Specifying Targets

You can run a SQL Script job against database and cluster database target types. You select the targets to run the job against by doing the following:

1. Click **Add** in the Targets section.
2. Select the database target(s) from the pop-up.

Your selection(s) now appears in the Target table.

> **Note:** For a cluster host or RAC database, a job runs only once for the target, regardless of the number of database instances. Consequently, a job cannot run on all nodes of a RAC cluster.

11.3.3.2 Specifying Options for the Parameters Page

In a SQL Script job, you can specify any of the following in the SQL Script field of the Parameters property page:

- Any directives supported by SQL*Plus
- Contents of the SQL script itself
- Fully-qualified SQL script file; for example:

  ```
  @/private/oracle/scripts/myscript.sql
  ```

  Make sure that the script file is installed in the appropriate location on all targets.
- PL/SQL script using syntax supported by SQL*Plus; for example, one of the following:

  ```
  EXEC plsql_block;
  ```

  or

  ```
  DECLARE
     local_date DATE;
  BEGIN
     SELECT SYSDATE INTO local_date FROM dual;
  END;
  /
  ```

You can use target properties in the SQL Script field, a list of which appears in the Target Properties table. Target properties are case-sensitive. You can enter optional parameters to SQL*Plus in the Parameters field.

11.3.3.3 Specifying Host and Database Credentials

In the Credentials property page, you specify the host credentials and database credentials. The Management Agent uses the host credentials to launch the SQL*Plus executable, and uses database credentials to connect to the target database and run the SQL script. The job can use either the preferred credentials for hosts and databases, or you can specify other credentials that override the preferred credentials.

- **Use Preferred Credentials —**

  Select this choice if you want to use the preferred credentials for the targets for your SQL Script job. The credentials used for both host and database are those you specify in the drop-down. If you choose Normal Database Credentials, your normal database preferred credentials are used. If you choose SYSDBA Database Credentials, the SYSDBA preferred credentials are used. For both cases, the host credentials associated with the database target are used. Each time the job executes, it picks up the current values of your preferred credentials.

- **Named Credentials —**

  Select this choice if you want to override the preferred credentials for all targets, then enter the named credentials you want the job to use on all targets.

  Many IT organizations require that passwords be changed on regular intervals. You can change the password of any preferred credentials using this option. Jobs and corrective actions that use preferred credentials automatically pick up these new changes, because during execution, Enterprise Manager uses the current value of the credentials (both user name and password). Named credentials are also centrally managed. A change to a named credential is propagated to all jobs or corrective actions that use it.

  For corrective actions, if you specify preferred credentials, Enterprise Manager uses the preferred credentials of the last Enterprise Manager user who edited the corrective action. For this reason, if a user attempts to edit the corrective action that a first user initially specified, Enterprise Manager requires this second user to specify the credentials to be used for that corrective action.

11.3.3.4 Returning Error Codes from SQL Script Jobs

The SQL Script job internally uses SQL*Plus to run a user's SQL or PL/SQL script. If SQL*Plus returns 0, the job returns a status of Succeeded. If it returns any other value, it returns a job status of Failed. By default, if a SQL script runs and encounters an error, it may still result in a job status of Succeeded, because SQL*Plus still returned a value of 0. To make such jobs return a Failed status, you can use SQL*Plus EXIT to return a non-zero value.

The following examples show how you can return values from your PL/SQL or SQL scripts. These, in turn, will be used as the return value of SQL*Plus, thereby providing a way to return the appropriate job status (Succeeded or Failed). Refer to the *SQL*Plus User's Guide and Reference* for more information about returning EXIT codes.

Example 1

```
WHENEVER SQLERROR EXIT SQL.SQLCODE
select column_does_not_exist from dual;
```

Example 2

```
-- SQL*Plus will NOT return an error for the next SELECT statement
SELECT COLUMN_DOES_NOT_EXIST FROM DUAL;

WHENEVER SQLERROR EXIT SQL.SQLCODE;
BEGIN
  -- SQL*Plus will return an error at this point
  SELECT COLUMN_DOES_NOT_EXIST FROM DUAL;
END;
/
WHENEVER SQLERROR CONTINUE;
```

Example 3

```
variable exit_code number;

BEGIN
 DECLARE
 local_empno number(5);
 BEGIN
  -- do some work which will raise exception: no_data_found
  SELECT 123 INTO local_empno FROM sys.dual WHERE 1=2;
 EXCEPTION
  WHEN no_data_found THEN
    :exit_code := 10;
  WHEN others THEN
    :exit_code := 2;
  END;
 END;
/
exit :exit_code;
```

11.3.4 Creating a Multi-task Job

The basic process for creating a multi-task job is the same as described in Section 11.3.2, "Creating an OS Command Job." The following sections provide supplemental information specific to multi-task jobs:

- Job Capabilities
- Specifying Targets for a Multi-task Job
- Adding Tasks to the Job

11.3.4.1 Job Capabilities

Multi-task jobs enable you to create complex jobs consisting of one or more distinct tasks. Because multi-task jobs can run against targets of the same or different type, they can perform ad hoc operations on one or more targets of the same or different type.

The Job System's multi-task functionality makes it easy to create extremely complex operations. You can create multi-task jobs in which all tasks run on a single target. You can also create a multi-task job consisting of several tasks, each of which has a different job type, and with each task operating on separate (and different) target types. For example:

- Task 1 (OS Command job type) performs an operation on Host 1.
- If Task 1 is successful, run Task2 (SQL Script job type) against Database 1 and Database 2.

11.3.4.2 Specifying Targets for a Multi-task Job

You can run a multi-task job against any targets for which jobs are defined that can be used as tasks. Not all job types can be used as tasks.

The Target drop-down in the General page enables you to choose between running the job against the same targets for all tasks, or different targets for different tasks. Because each task of a multi-task job can be considered a complete job, when choosing the **Same targets for all tasks** option, you add all targets against which the job is to run from the General page. If you choose the **Different targets for different tasks** option, you specify the targets (and required credentials) the tasks will run against as you define each task.

After making your choice from the Target drop-down, you then select the targets to run the job against by clicking Add in the Targets section.

11.3.4.3 Adding Tasks to the Job

You can use the Tasks page to:

- Add, delete, or edit tasks of various job types
- Set task condition and dependency logic
- Add task error handling

You must define at least two tasks in order to set Condition and Depends On options. Task conditions define states in which the task will be executed. Condition options include:

- **Always** — Task is executed each time the job is run.
- **On Success** — Task execution **Depends On** the successful execution of another task.
- **On Failure** — Task execution **Depends On** the execution failure of another task.

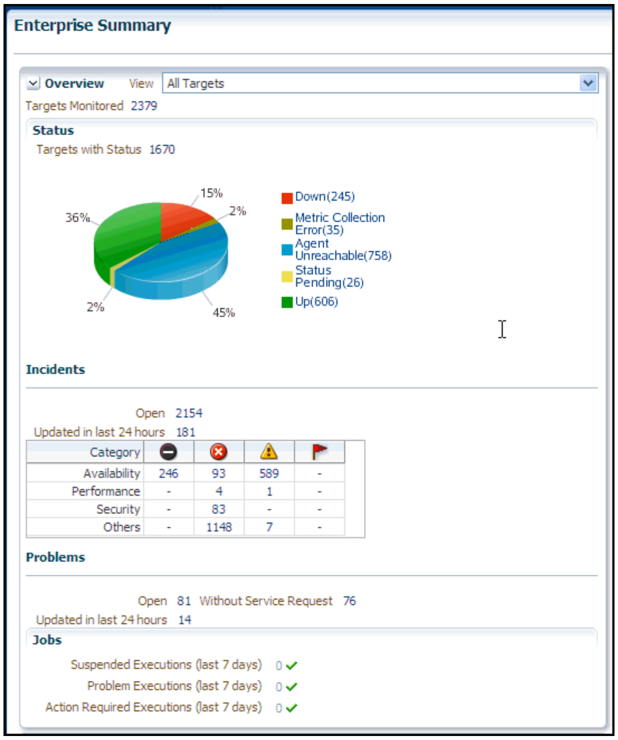
The Error Handler Task is often a "clean-up" step that can undo the partial state of the job. The Error Handler Task executes if any task of the multi-task job has an error. Errors are a more severe form of failure, usually meaning that the job system could not run the task. Failures normally indicate that the task ran, but failed. The Error Handler Task does not affect the job execution status. Use the Select Task Type page to specify the job type of the task to be used for error handling.

11.4 Viewing and Analyzing Job Status

Viewing the Aggregate Status of All Jobs

After you submit jobs, the status of all job executions across all targets is automatically rolled up and available for review on the Enterprise Summary page. Figure 11–2 shows the Jobs section at the bottom of the Enterprise Summary page.

Figure 11–2 Summary of Target Jobs on the Enterprise Summary Page



Enterprise Summary

Overview View All Targets

Targets Monitored 2379

Status

Targets with Status 1670

Incidents

Open 2154

Updated in last 24 hours 181

Category	⊖	⊗	⚠	🚩
Availability	246	93	589	-
Performance	-	4	1	-
Security	-	83	-	-
Others	-	1148	7	-

Problems

Open 81 Without Service Request 76

Updated in last 24 hours 14

Jobs

Suspended Executions (last 7 days) 0 ✓

Problem Executions (last 7 days) 0 ✓

Action Required Executions (last 7 days) 0 ✓

This information is particularly important when you are examining jobs that execute against hundreds or thousands of systems. You can determine the job executions that have failed. By clicking the number associated with a particular execution, you can drill down to study the details of the failed jobs.

Viewing the General Status of a Particular Job

To find out general status information for a particular job or jobs you have submitted, search for them in the Job Activity page, shown in Figure 11–1.

Viewing the Status of Job Executions

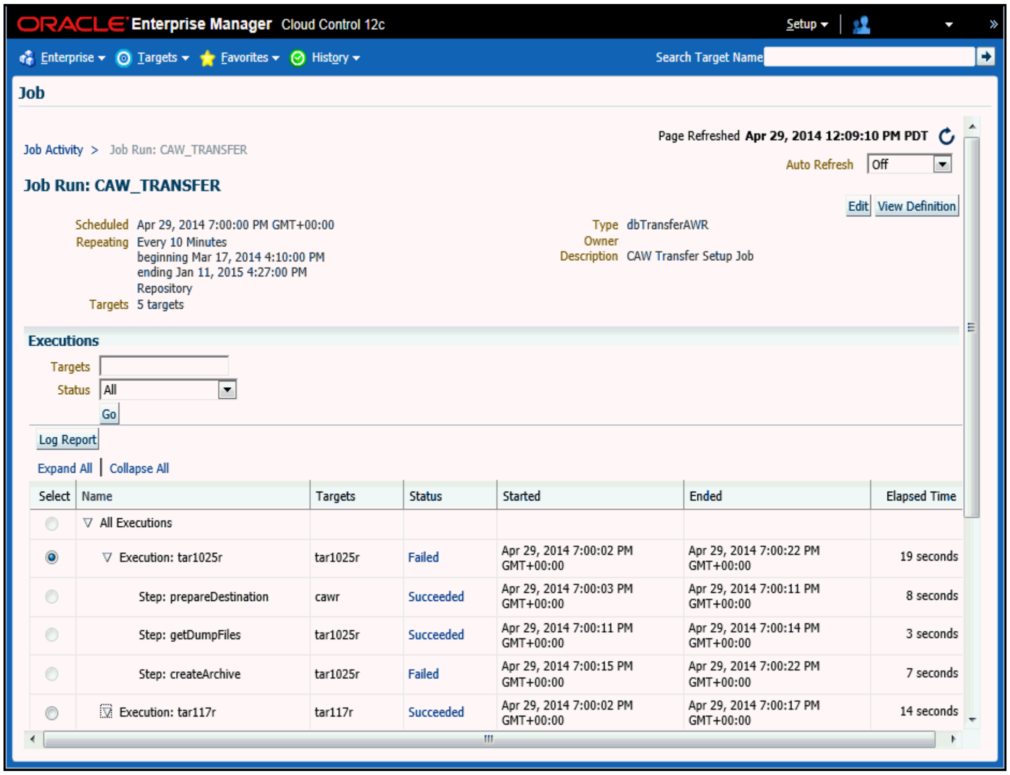
You can view detailed information about a single execution or multiple executions. A single execution can have a single step or multiple steps.

To view the status of executions:

1. From the Job Activity page, click the **Name** link or **Status** link for the job of interest.

   The Job Run page appears, as shown in Figure 11–3.

Figure 11–3 Job Run Page



Job Activity > Job Run: CAW_TRANSFER

Page Refreshed **Apr 29, 2014 12:09:10 PM PDT**

Auto Refresh Off

Job Run: CAW_TRANSFER

Edit | View Definition

Scheduled Apr 29, 2014 7:00:00 PM GMT+00:00
Repeating Every 10 Minutes
beginning Mar 17, 2014 4:10:00 PM
ending Jan 11, 2015 4:27:00 PM
Repository
Targets 5 targets

Type dbTransferAWR
Owner
Description CAW Transfer Setup Job

Executions

Targets
Status All
Go

Log Report

Expand All | Collapse All

Select	Name	Targets	Status	Started	Ended	Elapsed Time
○	▽ All Executions					
●	▽ Execution: tar1025r	tar1025r	Failed	Apr 29, 2014 7:00:02 PM GMT+00:00	Apr 29, 2014 7:00:22 PM GMT+00:00	19 seconds
○	Step: prepareDestination	cawr	Succeeded	Apr 29, 2014 7:00:03 PM GMT+00:00	Apr 29, 2014 7:00:11 PM GMT+00:00	8 seconds
○	Step: getDumpFiles	tar1025r	Succeeded	Apr 29, 2014 7:00:11 PM GMT+00:00	Apr 29, 2014 7:00:14 PM GMT+00:00	3 seconds
○	Step: createArchive	tar1025r	Failed	Apr 29, 2014 7:00:15 PM GMT+00:00	Apr 29, 2014 7:00:22 PM GMT+00:00	7 seconds
○	▽ Execution: tar117r	tar117r	Succeeded	Apr 29, 2014 7:00:02 PM GMT+00:00	Apr 29, 2014 7:00:17 PM GMT+00:00	14 seconds

2. Click on the Status link of a particular execution or step for further information.

Switching to Enhanced View

Beginning with Cloud Control version 12.1.0.4, you can optionally invoke a view of job runs that combines the views of several drill-downs on one page. To enable the enhanced view, execute the following command:

```
emctl set property -name oracle.sysman.core.jobs.ui.useAdfExecutionUi -value true
```

To revert to the standard view, execute the following command:

```
emctl set property -name oracle.sysman.core.jobs.ui.useAdfExecutionUi -value false
```

> **Note:** These commands do not require you to restart the OMS.

Viewing the Enhanced Status of a Job Run with a Single Execution

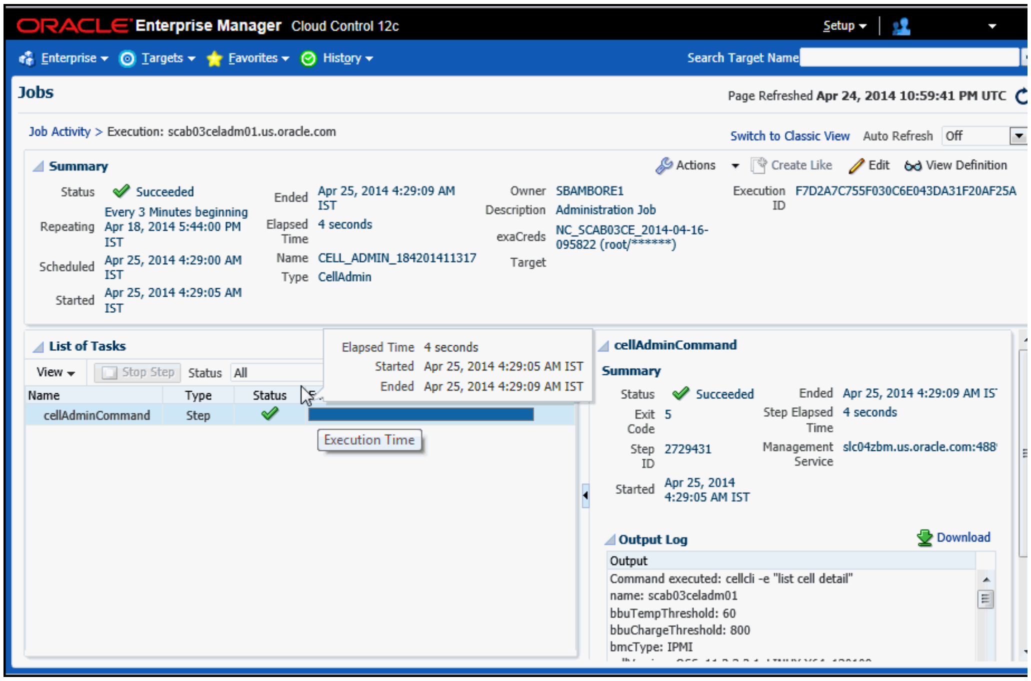
A single execution can have a single step or multiple steps. To view the status of a single execution:

1. From the Job Activity page, click the **Name** link or **Status** link for a job containing a single execution.

2. Click on the task or step in the List of Tasks table.

   The details for the particular execution appears on the right side of the page, as shown in Figure 11–4.

Figure 11–4 Enhanced Execution Summary in Jobs Page



Page Refreshed Apr 24, 2014 10:59:41 PM UTC

Auto Refresh Off

Summary

Status Succeeded
Repeating Every 3 Minutes beginning Apr 18, 2014 5:44:00 PM IST
Scheduled Apr 25, 2014 4:29:00 AM IST
Started Apr 25, 2014 4:29:05 AM IST
Ended Apr 25, 2014 4:29:09 AM IST
Elapsed Time 4 seconds
Name CELL_ADMIN_184201411317
Type CellAdmin
Owner SBAMBORE1
Description Administration Job
exaCreds NC_SCAB03CE_2014-04-16-095822 (root/******)
Target
Execution ID F7D2A7C755F030C6E043DA31F20AF25A

List of Tasks

Status All

Name	Type	Status
cellAdminCommand	Step	✓

Elapsed Time 4 seconds
Started Apr 25, 2014 4:29:05 AM IST
Ended Apr 25, 2014 4:29:09 AM IST

cellAdminCommand

Summary

Status Succeeded
Exit Code 5
Step ID 2729431
Started Apr 25, 2014 4:29:05 AM IST
Ended Apr 25, 2014 4:29:09 AM IS
Step Elapsed Time 4 seconds
Management Service slc04zbm.us.oracle.com:488

Output Log

```
Output
Command executed: cellcli -e "list cell detail"
name: scab03celadm01
bbuTempThreshold: 60
bbuChargeThreshold: 800
bmcType: IPMI
```

Viewing the Enhanced Status of a Job Run with Multiple Executions

To view the status of multiple executions:

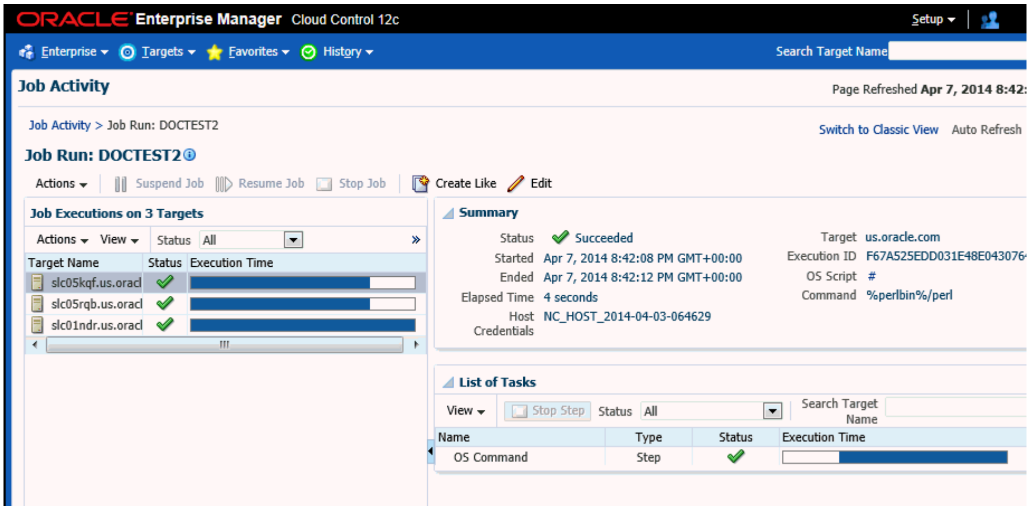
1. From the Job Activity page, click the **Name** link or **Status** link for a job containing multiple executions.

   The Job Run page appears.

2. Click on an execution of interest in the left table.

   The details for the particular execution appears on the right side of the page, as shown in Figure 11–5.

Figure 11–5 Execution Summary in Job Run Page



Page Refreshed Apr 7, 2014 8:42:

Job Run: DOCTEST2

Job Executions on 3 Targets

Status All

Target Name	Status	Execution Time
slc05kqf.us.oracl	✓	
slc05rqb.us.oracl	✓	
slc01ndr.us.oracl	✓	

Summary

Status Succeeded
Started Apr 7, 2014 8:42:08 PM GMT+00:00
Ended Apr 7, 2014 8:42:12 PM GMT+00:00
Elapsed Time 4 seconds
Host Credentials NC_HOST_2014-04-03-064629
Target us.oracle.com
Execution ID F67A525EDD031E48E043076
OS Script #
Command %perlbin%/perl

List of Tasks

Status All

Name	Type	Status	Execution Time
OS Command	Step	✓	

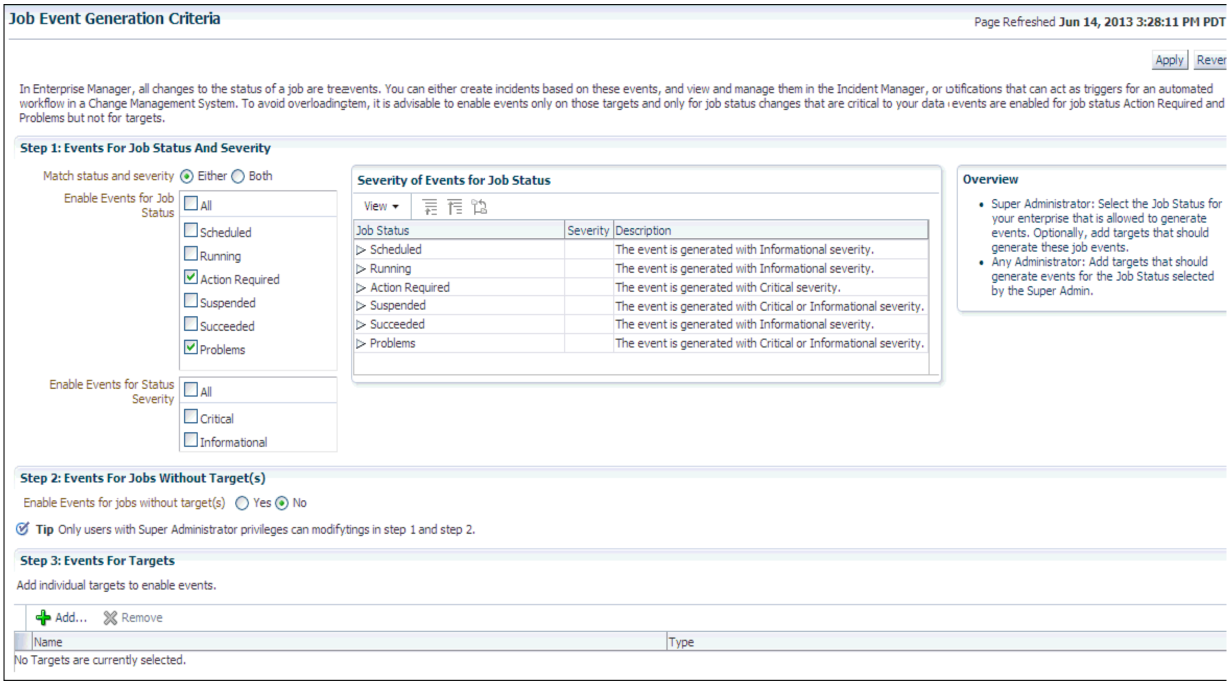
11.5 Generating Job Event Criteria

The job system publishes status change events when a job changes its execution status, and these events have different severities based on the execution status.

Use the Job Event Generation Criteria page (Figure 11–6) to set up targets for job event notifications. This page enables you to decide about the jobs or targets or statuses for which you want to raise events or notifications. This ensures that users raise only useful events. Any settings you make on this page do not change the job behavior whatsoever. You can set up notifications on job events through incident rule sets.

To access this page, from the Setup menu, select **Incidents**, then **Job Events**.

Figure 11–6 Job Event Generation Criteria Page



Job Event Generation Criteria

Page Refreshed **Jun 14, 2013 3:28:11 PM PDT**

In Enterprise Manager, all changes to the status of a job are treᴞevents. You can either create incidents based on these events, and view and manage them in the Incident Manager, or ᴝtifications that can act as triggers for an automated workflow in a Change Management System. To avoid overloadingtem, it is advisable to enable events only on those targets and only for job status changes that are critical to your data ᵢevents are enabled for job status Action Required and Problems but not for targets.

Step 1: Events For Job Status And Severity

Match status and severity ● Either ○ Both

Enable Events for Job Status
□ All
□ Scheduled
□ Running
☑ Action Required
□ Suspended
□ Succeeded
☑ Problems

Enable Events for Status Severity
□ All
□ Critical
□ Informational

Severity of Events for Job Status

Job Status	Severity	Description
▷ Scheduled		The event is generated with Informational severity.
▷ Running		The event is generated with Informational severity.
▷ Action Required		The event is generated with Critical severity.
▷ Suspended		The event is generated with Critical or Informational severity.
▷ Succeeded		The event is generated with Informational severity.
▷ Problems		The event is generated with Critical or Informational severity.

Overview

- Super Administrator: Select the Job Status for your enterprise that is allowed to generate events. Optionally, add targets that should generate these job events.
- Any Administrator: Add targets that should generate events for the Job Status selected by the Super Admin.

Step 2: Events For Jobs Without Target(s)

Enable Events for jobs without target(s) ○ Yes ● No

Tip Only users with Super Administrator privileges can modifytings in step 1 and step 2.

Step 3: Events For Targets

Add individual targets to enable events.

Name	Type

No Targets are currently selected.

11.5.1 Enabling Events For Job Status, Status Severity, and Targetless Jobs

To enable events for job status and targetless jobs, do the following:

1. Ensure that you have Super Administrator privileges to select the job status for which you want to generate events.
2. Ensure that you are an administrator with View Target privileges to add targets for which you want to generate events for the job status set by the Super Administrator.
3. Log into Cloud Control as a Super Administrator.
4. From the **Setup** menu, select **Incidents** and then select **Job Events**. The Job Event Generation Criteria Page is displayed.
5. In the Job Event Generation Criteria page, do the following:
   a. In the "Enable Events for Job Status"region, select the statuses for which you want to publish events.

   b. In the "Enable Events for Status Severity" region, select whether you want to enable events for a critical status, informational status, for both.

   c. In the **"Enable Events for Jobs Without Target(s)"** section, select **Yes** if you want to create events for jobs that are not associated with any target.

   d. In the "Events for Targets" section, click **Add** to add targets for which you want the job events to be enabled.

6. Click **Apply**.

11.5.2 Adding Targets To Generate Events For Job Status

After a Super Administrator selects events for which job status will be published, administrators can add targets to generate events. To add targets to generate events for job status, do the following:

1. Ensure that you are an administrator with View Target privileges to add targets for which you want to generate events for the job status set by a Super Administrator.
2. Log into Cloud Control as an administrator.
3. From the **Setup** menu, select **Incidents** and then select **Job Events**. The Job Event Generation Criteria Page is displayed.
4. In the Job Event Generation Criteria page, do the following:
   a. In the Events For Job Status And Targetless Jobs section, you can view the status for which events can be published. You can also see if events have been enabled for targetless job filters.
   b. In the Events For Targets section, click **Add** to add targets for which you want the job events to be enabled. You can also remove targets for which you do not want the job events to be enabled by clicking **Remove**.

   Note: Your selected settings in the Events for Targets section are global. Adding or removing targets for events also affect other Enterprise Manager users.

5. Click **Apply**.

11.6 Creating Event Rules For Job Status Change

Enterprise Manager enables you to create and apply rules to events, incidents, and problems. A rule is applied when a newly created or updated event, incident, or problem matches the conditions defined in the rule. The following sections explain how to create event rules for job status change events:

- Creating Job Status Change Event Rules For Jobs
- Creating Job Status Change Event Rules For Targets

11.6.1 Creating Job Status Change Event Rules For Jobs

To create job status change event rules for jobs, do the following:

1. Ensure that the relevant job status is enabled and required targets have been added to job event generation criteria.

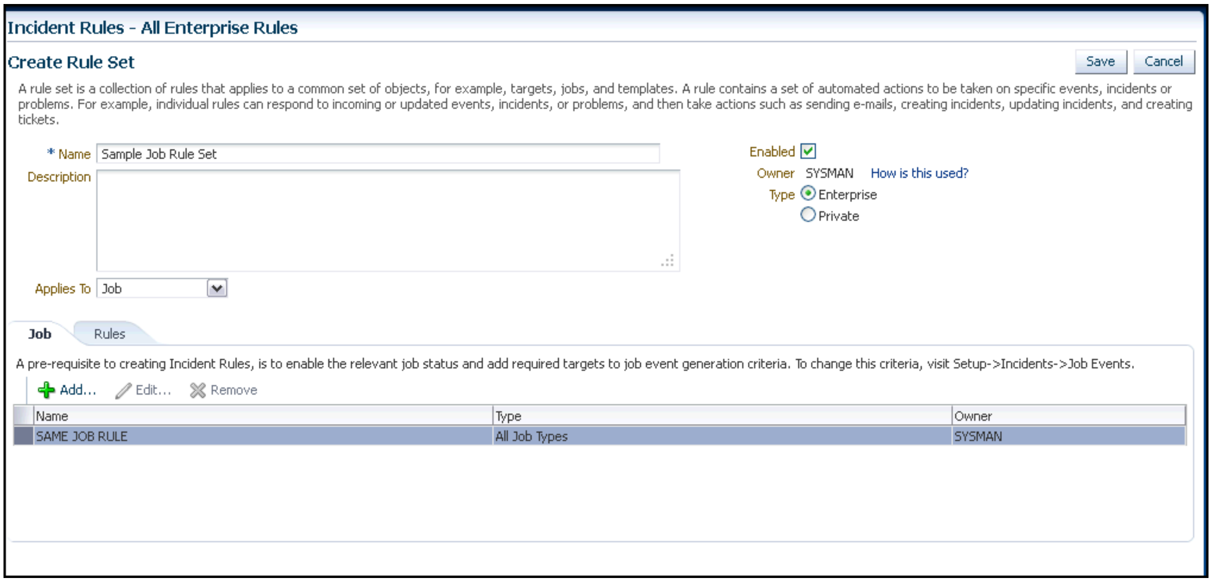
2. Ensure that you have administrator privileges to create event rules for job status change events.

3. Log into Cloud Control as an administrator.

4. From the **Setup** menu, select **Incidents** and then **Incident Rules**. The Incident Rules Page appears.

5. In the Incident Rules page, click **Create Rule Set** to create rule sets for incidents.

6. Specify the **Name**, **Description**, and select **Enabled** to enable the rule set. Select Type as **Enterprise** if you want to set the rule for all Enterprise Manager users or Private if you want to set the rule for a specific user only. Select **Applies to Job**.



Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name: Sample Job Rule Set

Description:

Applies To: Job

Enabled ☑

Owner: SYSMAN How is this used?

Type: ● Enterprise ○ Private

A pre-requisite to creating Incident Rules, is to enable the relevant job status and add required targets to job event generation criteria. To change this criteria, visit Setup->Incidents->Job Events.

Name	Type	Owner
SAME JOB RULE	All Job Types	SYSMAN

In the Job tab, click **Add** to add jobs for which you want to create event rules.

7. In the Add Jobs dialog box, if you select the job **By Pattern**, provide **Job name like** and select the **Job Type**. Specify **Job owner like**. For the **Specific jobs** choice, select the job. Click **OK**.

8. In the **Rules** tab, click **Create**.

   In the Select Type of Rule to Create dialog box that appears, you can select from the following choices according to the rule set you want to create:

   - **Incoming events and updates to events** to receive notification or create incidents for job rules. If you are operating on events (for example, if you want to create incidents for incoming events, such as job failed, or notify someone), choose this option.

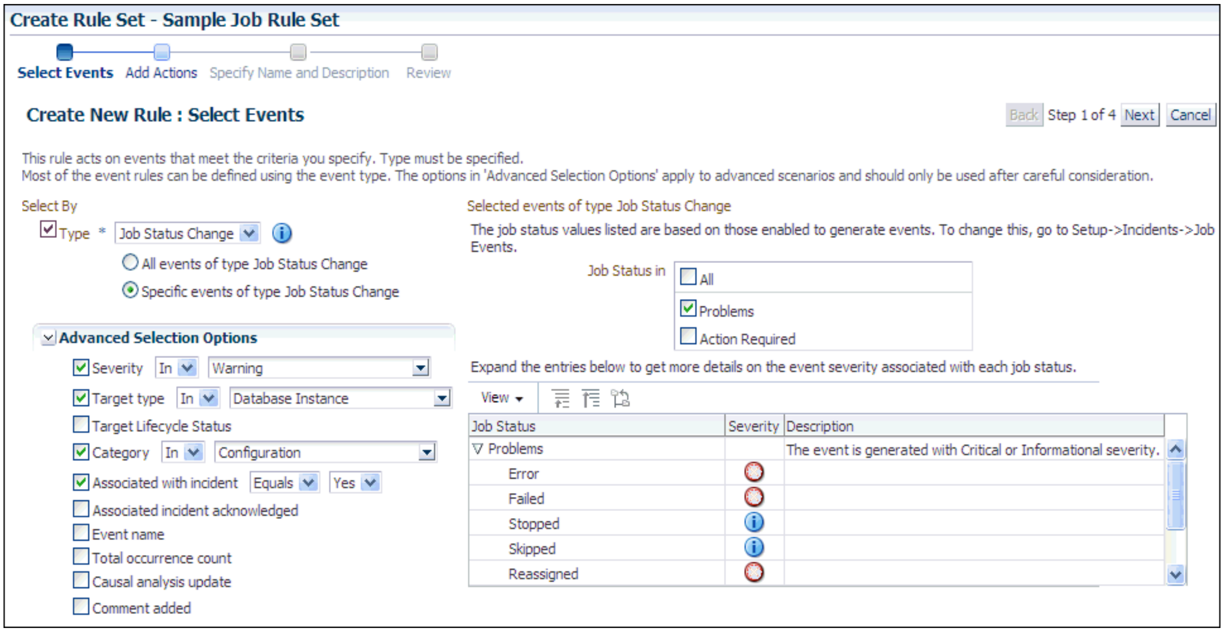
   - **Newly created incidents or updates to incidents** receive notifications or create rules for incidents even though the events for which incidents are generated do not have associated rules. If you are operating on incidents already created or newly created (for example, you want to direct all incidents related to a group, say foo, to a particular user or escalate all incidents open for more than 3 days), choose this option.

   - **Newly created problems or updates to problems** to receive notifications or create rules for problems even though the incidents for which problems are generated do not have associated rules. This option does not apply for jobs.

9. Select **Incoming events and updates to events**, and in the Create New Rule: Select Events page, do the following:

   a. **Select By Type** to **Job Status Change**. Select **All events of type Job Status Change** if you want to take an action for all job state change events for the selected jobs. Select **Specific events of type Job Status Change** if you only want to act on specific job states. If you have selected Specific events of type Job Status Change, select Job Status for events for which you want to create the rule.

   b. Set the other criteria for which you want to set the rule as displayed in the graphic below.



Create Rule Set - Sample Job Rule Set

Create New Rule : Select Events

This rule acts on events that meet the criteria you specify. Type must be specified.
Most of the event rules can be defined using the event type. The options in 'Advanced Selection Options' apply to advanced scenarios and should only be used after careful consideration.

Select By

☑ Type * Job Status Change

○ All events of type Job Status Change

● Specific events of type Job Status Change

Advanced Selection Options

☑ Severity In Warning

☑ Target type In Database Instance

☐ Target Lifecycle Status

☑ Category In Configuration

☑ Associated with incident Equals Yes

☐ Associated incident acknowledged

☐ Event name

☐ Total occurrence count

☐ Causal analysis update

☐ Comment added

Selected events of type Job Status Change

The job status values listed are based on those enabled to generate events. To change this, go to Setup->Incidents->Job Events.

Job Status in ☐ All

☑ Problems

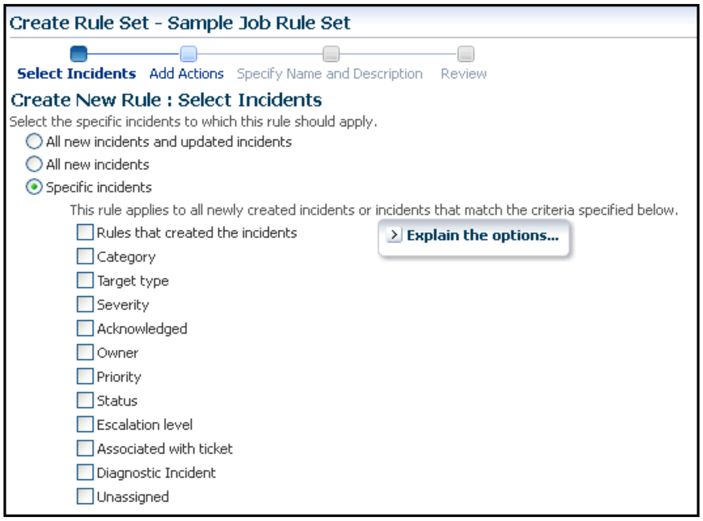
☐ Action Required

Expand the entries below to get more details on the event severity associated with each job status.

Job Status	Severity	Description
▽ Problems		The event is generated with Critical or Informational severity.
Error	○	
Failed	○	
Stopped	ⓘ	
Skipped	ⓘ	
Reassigned	○	

10. Select **Newly created incidents or updates to incidents** if you want to create rules for an incident, though the event associated with the incident does not have notification rules. In the Create New Rule: Select Incidents page, select any of the following:

    - **All new incidents and updated incidents** to apply the rule to all new and updated incidents
    - **All new incidents** to apply the rule to all new incidents
    - **Specific incidents** and then select the criteria for the incidents



Create Rule Set - Sample Job Rule Set

Create New Rule : Select Incidents

Select the specific incidents to which this rule should apply.

○ All new incidents and updated incidents
○ All new incidents
● Specific incidents

This rule applies to all newly created incidents or incidents that match the criteria specified below.

□ Rules that created the incidents
□ Category
□ Target type
□ Severity
□ Acknowledged
□ Owner
□ Priority
□ Status
□ Escalation level
□ Associated with ticket
□ Diagnostic Incident
□ Unassigned

11. In the Create New Rule: Add Actions page, click **Add** to add actions to the rule.

12. In the Add Conditional Actions page, specify actions to be performed when the event matches the rule.

    In the Conditions for actions section, select:

    - **Always execute the actions** to execute actions regardless of event.
    - **Only execute the actions if specified conditions match** to execute actions to match specific criteria.

    When adding actions to events, specify the following:

    - Select **Create Incident** to create an incident for the event to manage and track its resolution.
    - In the Notifications section, specify recipients for notifications in the **E-mail To**, **E-mail Cc**, and **Page** fields who will receive e-mail when the event for which a condition is set occurs. If Advanced and Repeat Notifications options have been set, specify them.
    - In the Clear events section, select **Clear permanently** if you want to clear an event after the issue that generated the event is resolved.
    - If you have configured event connections, in the Forward to Event Connectors section, you can send the events to third-party event management systems.

    When adding actions to incidents, specify the following:

    - In the Notifications section, specify recipients for notifications in the **E-mail To**, **E-mail Cc**, and **Page** fields who will receive e-mail when the event for which a condition is set occurs. If Advanced and Repeat Notifications options have been set, specify them.
    - In the Update Incident section, specify the details to triage incidents when they occur. Specify **Assign to**, **Set priority to**, **Set status to**, and **Escalate to** details.
    - In the Create Ticket section, if a ticket device has been configured, specify details to create the ticket.

    Click **Continue**.

13. In the Specify Name and Description page, specify a **Name** and **Description** for the event rule. Click **Next**.

14. In the Review page, verify the details you have selected for the event rule and click **Continue** to add this rule in the rule set.

15. On the Create Rule Set page, click **Save** to save the rule set.

11.6.2 Creating Job Status Change Event Rules For Targets

To create job status change event rules for targets, do the following:

1. Ensure that the relevant job status is enabled and required targets have been added to job event generation criteria.

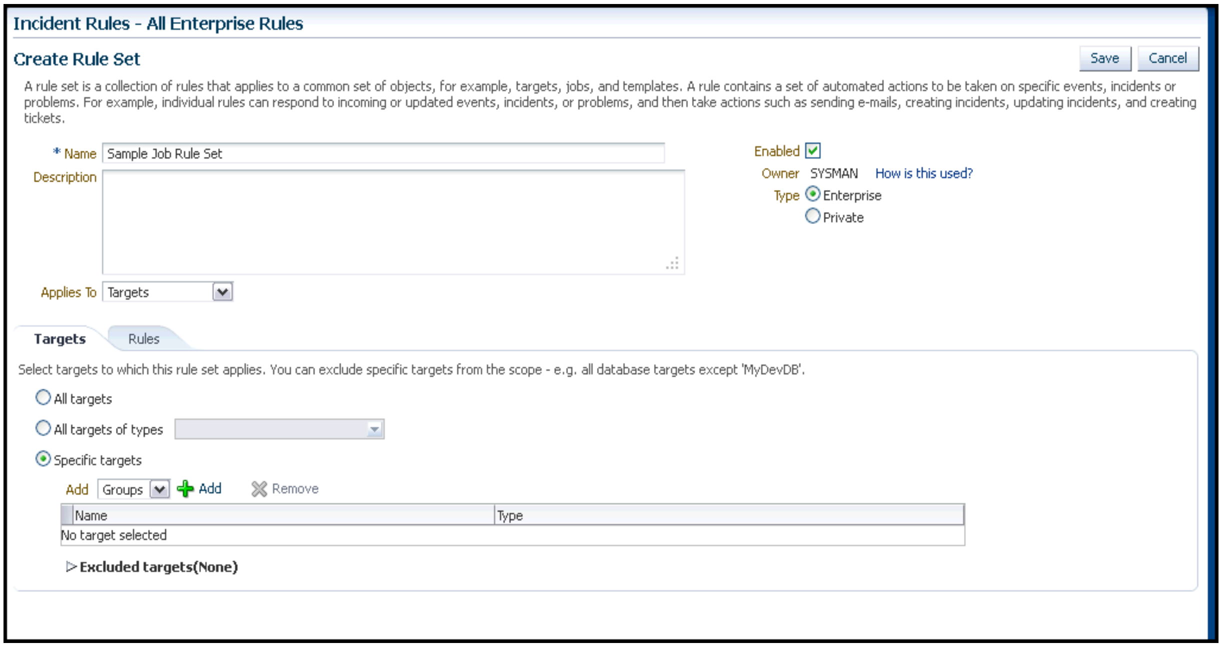
2. Ensure that you have administrator privileges to create event rules for job status change events.

3. Log into Cloud Control as an administrator.

4. From the **Setup** menu, select **Incidents**, then **Incident Rules**. The Incident Rules Page is displayed.

5. In the Incident Rules page, click **Create Rule Set** to create rule sets for incidents.

6. Specify the **Name**, **Description**, and select **Enabled** to enable the rule set. Select Type as **Enterprise** if you want to set the rule for all Enterprise Manager users, or Private if you want to set the rule for a only specific user. Select **Applies to Targets**.



Incident Rules - All Enterprise Rules

Create Rule Set

A rule set is a collection of rules that applies to a common set of objects, for example, targets, jobs, and templates. A rule contains a set of automated actions to be taken on specific events, incidents or problems. For example, individual rules can respond to incoming or updated events, incidents, or problems, and then take actions such as sending e-mails, creating incidents, updating incidents, and creating tickets.

* Name: Sample Job Rule Set

Description:

Applies To: Targets

Enabled ☑

Owner SYSMAN

Type ● Enterprise ○ Private

Select targets to which this rule set applies. You can exclude specific targets from the scope - e.g. all database targets except 'MyDevDB'.

○ All targets

○ All targets of types

● Specific targets

Add: Groups

Name	Type
No target selected	

▷ Excluded targets(None)

In the **Targets** tab, select one of the following:

- **All targets** to apply to all targets. In the Excluded Targets section, click **Add** to search and select the target that you want to exclude from the rule set. Click **Select**.

- **All targets of types** to select the types of targets to which you want to apply the rule set.

- **Specific targets** to individually specify the targets. Select to Add **Groups** or **Targets** to add groups or targets and click **Add** to search and select the targets to which you want to apply the rule set. Click **Select**. In the Excluded Targets section, click **Add** to search and select the target that you want to exclude from the rule set. Click **Select**.

7. In the **Rules** tab, click **Create**.

8. In the Select Type of Rule to Create dialog box, select from the following choices according to the rule set you want to create:

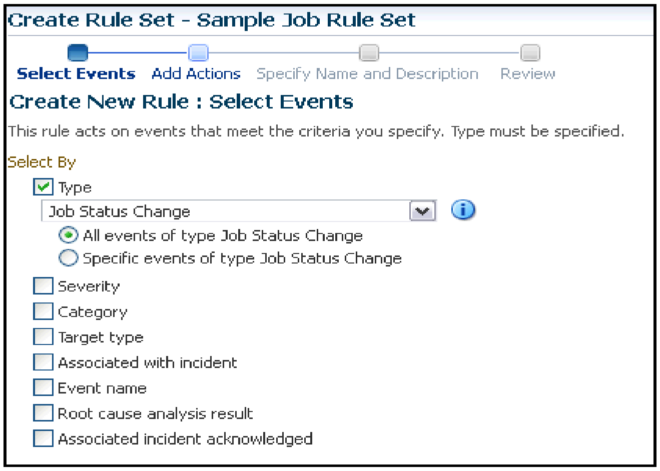
   - **Incoming events and updates to events** to receive notifications or create incidents for job rules. If you are operating on events (for example, if you want to create incidents for incoming events, such as job failed, or notify someone), choose this option.

   - **Newly created incidents or updates to incidents** receive notifications or create rules for incidents even though the events for which incidents are generated do not have associated rules. If you are operating on incidents already created or newly created (for example, you want to direct all incidents related to a group, say foo, to a particular user or escalate all incidents open for more than 3 days), choose this option.

   - **Newly created problems or updates to problems** to receive notifications or create rules for problems even though the incidents for which problems are generated do not have associated rules. This option does not apply for jobs.

9. Select **Incoming events and updates to events**, and in the Create New Rule: Select Events page, do the following:

   - **Select By Type** to **Job Status Change**. Select **All events of type Job Status Change** if you want to take an action for all job state change events for the selected jobs. Select **Specific events of type Job Status Change** if you only want to act on specific job states. If you have selected Specific events of type Job Status Change, select Job Status for events for which you want to create the rule.



Create Rule Set - Sample Job Rule Set

Create New Rule : Select Events

This rule acts on events that meet the criteria you specify. Type must be specified.

Select By

☑ Type

Job Status Change

● All events of type Job Status Change

○ Specific events of type Job Status Change

□ Severity

□ Category

□ Target type

□ Associated with incident

□ Event name

□ Root cause analysis result

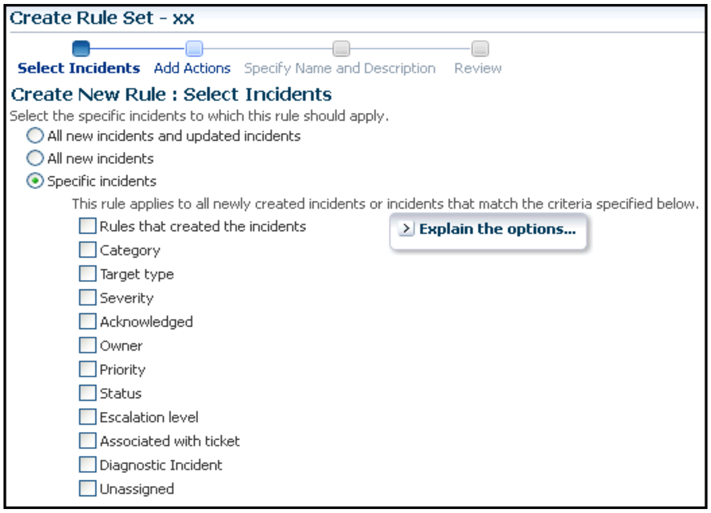
□ Associated incident acknowledged

   - Set the other criteria for which you want to set the rule as displayed in the above graphic.

10. Select **Newly created incidents or updates to incidents** if you want to create rules for an incident, though the event associated with the incident does not have

notification rules. In the Create New Rule: Select Incidents page, select any of the following:

- **All new incidents and updated incidents** to apply the rule to all new and updated incidents.
- **All new incidents** to apply the rule to all new incidents.
- **Specific incidents** and then select the criteria for the incidents.



Create New Rule : Select Incidents

Select the specific incidents to which this rule should apply.

○ All new incidents and updated incidents
○ All new incidents
● Specific incidents

This rule applies to all newly created incidents or incidents that match the criteria specified below.

□ Rules that created the incidents
□ Category
□ Target type
□ Severity
□ Acknowledged
□ Owner
□ Priority
□ Status
□ Escalation level
□ Associated with ticket
□ Diagnostic Incident
□ Unassigned

11. In the Create New Rule: Add Actions page, click **Add** to add actions to the rule.
12. In the Add Conditional Actions page, specify actions to be performed when the event matches the rule.

    In the Conditions for actions section, select:

    - **Always execute the actions** to execute actions regardless of event.
    - **Only execute the actions if specified conditions match** to execute actions to match specific criteria.

    When adding actions to events, specify the following:

    - Select **Create Incident** to create an incident for the event to manage and track its resolution.
    - In the Notifications section, specify recipients for notifications in the **E-mail To**, **E-mail Cc**, and **Page** fields who will receive e-mail when the event for which a condition is set occurs. If Advanced and Repeat Notifications options have been set, specify them.
    - In the Clear events section, select **Clear permanently** if you want to clear an event after the issue that generated the event is resolved.
    - If you have configured event connections, in the Forward to Event Connectors section, you can send the events to third-party event management systems.

    When adding actions to incidents, specify the following:

    - In the Notifications section, specify recipients for notifications in the **E-mail To**, **E-mail Cc**, and **Page** fields who will receive e-mail when the event for which a condition is set occurs. If Advanced and Repeat Notifications options have been set, specify them.

- In the Update Incident section, specify the details to triage incidents when they occur. Specify **Assign to**, **Set priority to**, **Set status to**, and **Escalate to** details.
- In the Create Ticket section, if a ticket device has been configured, specify the details to create the ticket.

Click **Continue**.

13. In the Specify Name and Description page, specify a **Name** and **Description** for the event rule. Click **Next**.
14. In the Review page, verify the details you have selected for the event rule and click **Continue** to add this rule in the rule set.
15. On the Create Rule Set page, click **Save** to save the rule set.

11.7 Using Diagnostic Tools

The following sections provided procedures for these diagnostic topics:

- Enabling Job Logging
- Viewing Job Logging
- Debugging a Failed Job
- Checking for Incidents Related to a Failed Job
- Packaging an Incident Generated by a Job Step
- Viewing Remote Log Files
- Diagnosing Problems with Cloud Control Management Tools

11.7.1 Enabling Job Logging

You can enable and disable object logging for purposes.

To enable job logging for a scheduled job:

1. From the Enterprise menu of the Cloud Control console, select **Job**, then **Activity**.
2. In the Top Activity table, click the link for the job you want to log.
3. In the Job Run table, click the **Scheduled** link for the job.
4. In the Execution page that appears, click **Debug**.

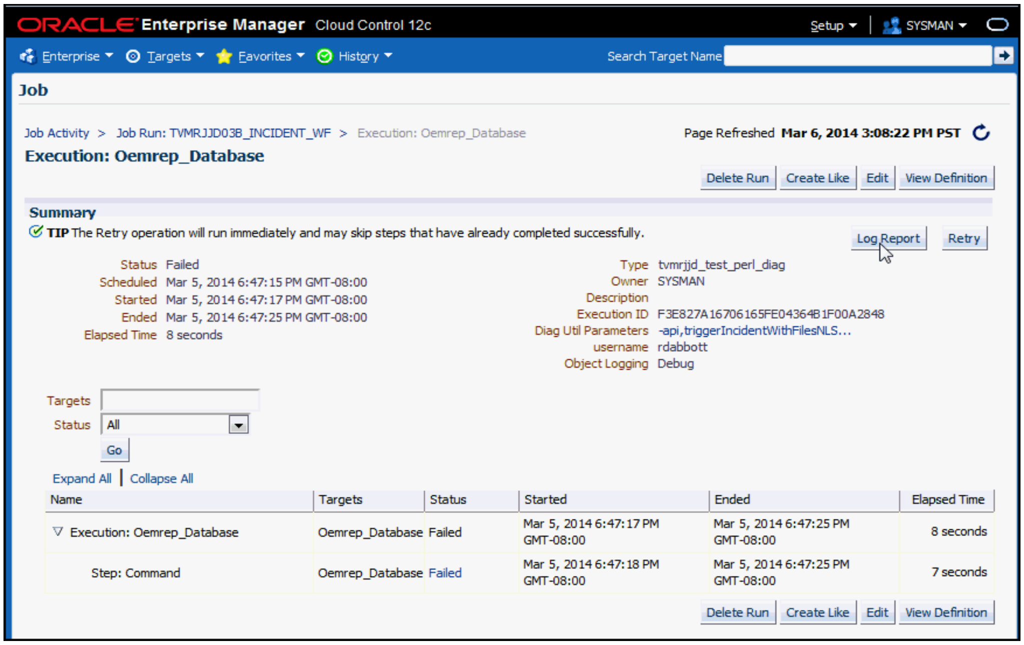
   A confirmation message appears that states "Successfully enabled logging at DEBUG level."

11.7.2 Viewing Job Logging

If there is user-visible logging for a particular job, you can view the job execution log by doing the following:

1. In the Top Activity page, click the link of the job for which you want to view the log.
2. In the Job Run table, click **Log Report**.

You can also access job logging from the Execution page by clicking the link that appears in the Status column of the Job Run page, then clicking **Log Report** on the Execution page as shown below.



Job Activity > Job Run: TVMRJJD03B_INCIDENT_WF > Execution: Oemrep_Database

Page Refreshed **Mar 6, 2014 3:08:22 PM PST**

Execution: Oemrep_Database

Summary

TIP The Retry operation will run immediately and may skip steps that have already completed successfully.

Status	Failed	Type	tvmrjjd_test_perl_diag
Scheduled	Mar 5, 2014 6:47:15 PM GMT-08:00	Owner	SYSMAN
Started	Mar 5, 2014 6:47:17 PM GMT-08:00	Description	
Ended	Mar 5, 2014 6:47:25 PM GMT-08:00	Execution ID	F3E827A16706165FE04364B1F00A2848
Elapsed Time	8 seconds	Diag Util Parameters	-api,triggerIncidentWithFilesNLS...
		username	rdabbott
		Object Logging	Debug

Targets

Status All

Name	Targets	Status	Started	Ended	Elapsed Time
▽ Execution: Oemrep_Database	Oemrep_Database	Failed	Mar 5, 2014 6:47:17 PM GMT-08:00	Mar 5, 2014 6:47:25 PM GMT-08:00	8 seconds
Step: Command	Oemrep_Database	Failed	Mar 5, 2014 6:47:18 PM GMT-08:00	Mar 5, 2014 6:47:25 PM GMT-08:00	7 seconds

To view the log for a job step, do the following:

1. In the Top Activity page, click the link of the job for which you want to view the log.
2. In the Job Run table, click the link that appears in the Status column for the step you want to examine.

   The Output Log appears for the step.

11.7.3 Debugging a Failed Job

If an execution fails and you had not previously set debug as the logging level, you can choose to set the debug level when you retry the execution. For new job executions, you can set logging at the debug level in advance by clicking the Debug button. The Object Logging field indicates whether logging is enabled at the debug level.

Perform the following procedure if you encounter a job that fails.

1. View the job steps that failed.
2. Check the output for the failed step(s). Aggregated job output is displayed for all steps, and also for specific steps.
3. If the output does not contain the reason for the failure, view the logging output. You may also want to check for any incidents that have occurred while the job was running.
4. Determine the cause of the failure and fix the problem.
5. Enable debug mode, then resubmit the job.

   Note that the checkbox for Debug mode only appears on the confirmation page if the earlier execution was not in Debug mode. If the earlier execution was already in Debug mode, the retried execution is automatically in Debug mode.

11.7.4 Checking for Incidents Related to a Failed Job

It is possible for a job to fail because of an internal code error, a severe scaling issue, or other Enterprise Manager issue for which you may be able to investigate an incident or event trail. For example, if the OMS bounced because all Job Workers were stuck, this would cause many jobs to fail. If the loader were failing, that could also cause some jobs to fail.

1. Check for incidents or alerts in the time-frame of the job.

   - To check for incidents, select **Summary** from the Enterprise menu of the Cloud Control console, then view the Incidents section of the Enterprise Summary page.

     For more detailed information, select **Monitoring** from the Enterprise menu, then select **Support Workbench**.

   - To check for alerts,

2. Submit a service request with the related incident(s) or event data.

   All step output, error output, logging, remote log files, and incident dump files for a given job are captured for an incident.

   - To submit a service request, select **My Oracle Support** from the Enterprise menu of the console, then select **Service Requests**.

   - To create a technical SR, click **Create SR** on the Service Requests Home page. To create a contact us SR, click **Create "Contact Us" SR** at the top of the Contact Us Service Requests region, or click **Contact Us** at the top of any My Oracle Support page. If you are creating a technical service request, depending on the Support IDs registered in your profile, you can create hardware or software SRs, or both.

     The Create Service Request wizard guides you through the process of specifying product information and attaching configuration information to the SR when it is filed with Oracle Support. To ensure that Oracle Support has the most accurate target information, select the Configuration tab in the What is the Problem? section of Step 1: Problem, then select a target.

3. Apply a patch that support provides.

   - Select **Provisioning and Patching** from the Enterprise menu of the console, then select **Patches & Updates**.

   - Provide login credentials, then click **Go**.

   - Access the online help for assistance with this page.

4. Try to submit the job again after applying the patch.

To package an incident or manually trigger an incident:

1. Access Support Workbench.

2. Gather all job-related dumps and log files, as well as other data from the same time, and package it for Support.

3. Review the incident-related data in Support Workbench, searching for relevant errors.

4. If you determine the root cause without support intervention, fix the job and resubmit it.

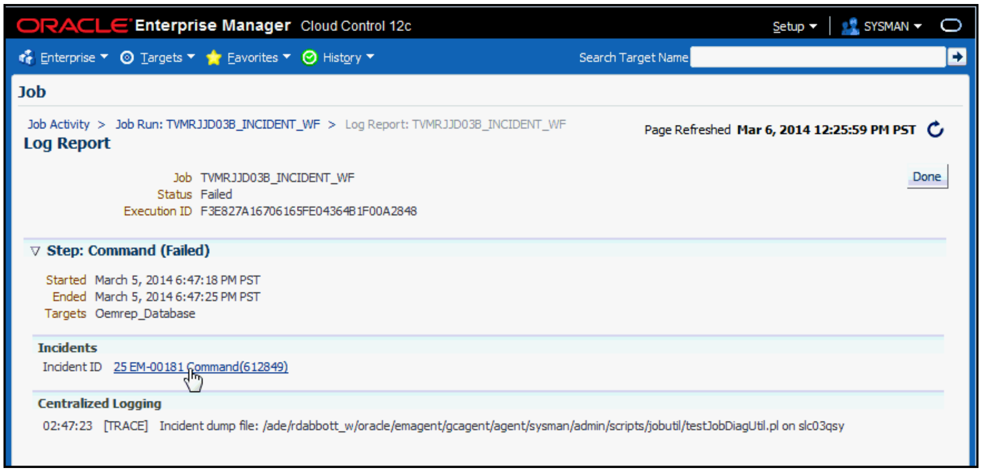
11.7.5 Packaging an Incident Generated by a Job Step

Incidents (and the problems that contain them) are not packaged by default. You will need to package the problems of interest or concern in Support Workbench. You can choose whether to package all problems or only a portion thereof.

> **Note:** If a job with remote log files is involved in an incident, the remote files are automatically included in the incident as part of packaging. For more information on remote log files, see Section 11.7.6, "Viewing Remote Log Files."

To package an incident generated by a job step:

1. On the Log Report page, click the **Incident ID** link as shown below.



Job

Job Activity > Job Run: TVMRJJD03B_INCIDENT_WF > Log Report: TVMRJJD03B_INCIDENT_WF

Log Report

Page Refreshed **Mar 6, 2014 12:25:59 PM PST**

Job TVMRJJD03B_INCIDENT_WF
Status Failed
Execution ID F3E827A16706165FE04364B1F00A2848

Step: Command (Failed)

Started March 5, 2014 6:47:18 PM PST
Ended March 5, 2014 6:47:25 PM PST
Targets Oemrep_Database

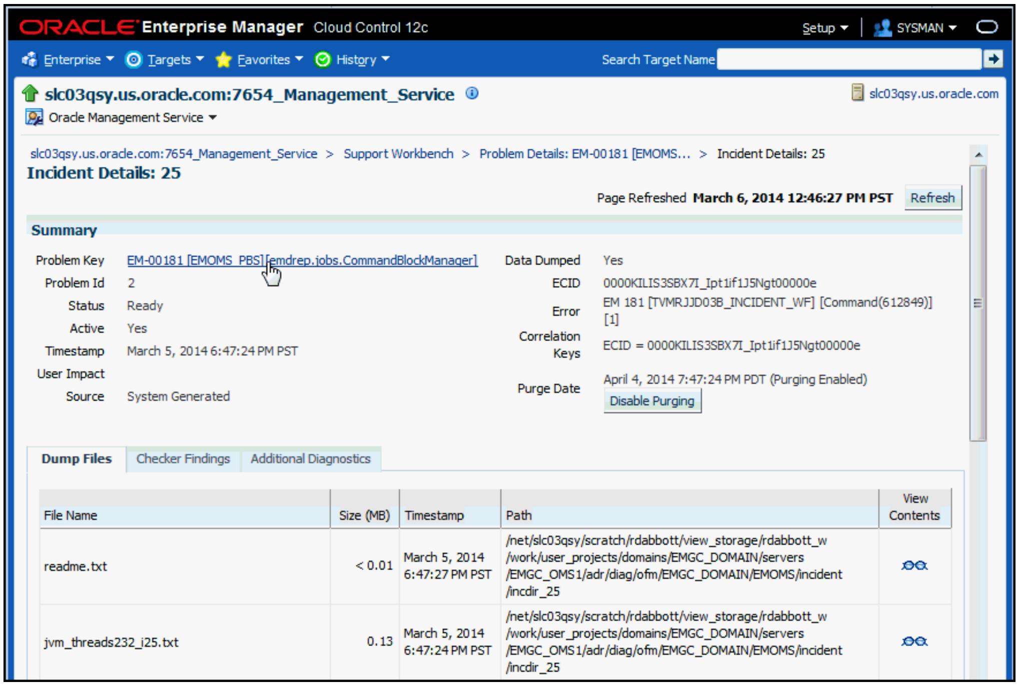
Incidents

Incident ID 25 EM-00181 Command(612849)

Centralized Logging

```
02:47:23  [TRACE]  Incident dump file: /ade/rdabbott_w/oracle/emagent/gcagent/agent/sysman/admin/scripts/jobutil/testJobDiagUtil.pl on slc03qsy
```

2. Click the **Problem Key** link on the Support Workbench Incident Details page as shown below.



slc03qsy.us.oracle.com:7654_Management_Service

slc03qsy.us.oracle.com:7654_Management_Service > Support Workbench > Problem Details: EM-00181 [EMOMS... > Incident Details: 25

Incident Details: 25

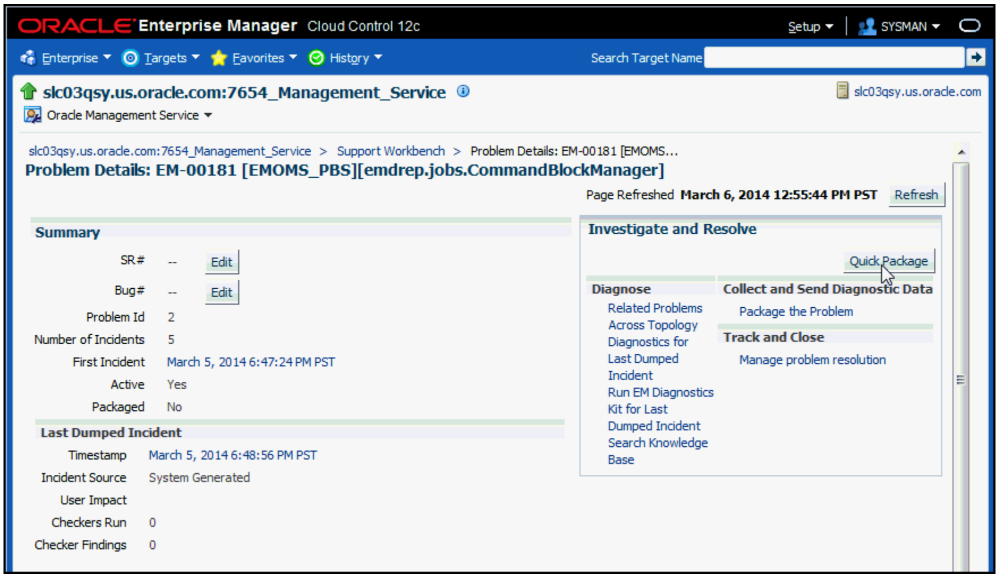
Page Refreshed **March 6, 2014 12:46:27 PM PST**

Summary

Problem Key	EM-00181 [EMOMS_PBS][emdrep.jobs.CommandBlockManager]	Data Dumped	Yes
Problem Id	2	ECID	0000KILIS3SBX7I_Ipt1if1J5Ngt00000e
Status	Ready	Error	EM 181 [TVMRJJD03B_INCIDENT_WF] [Command(612849)] [1]
Active	Yes	Correlation Keys	ECID = 0000KILIS3SBX7I_Ipt1if1J5Ngt00000e
Timestamp	March 5, 2014 6:47:24 PM PST	Purge Date	April 4, 2014 7:47:24 PM PDT (Purging Enabled)
User Impact			
Source	System Generated		

File Name	Size (MB)	Timestamp	Path	View Contents
readme.txt	< 0.01	March 5, 2014 6:47:27 PM PST	/net/slc03qsy/scratch/rdabbott/view_storage/rdabbott_w/work/user_projects/domains/EMGC_DOMAIN/servers/EMGC_OMS1/adr/diag/ofm/EMGC_DOMAIN/EMOMS/incident/incdir_25	👓
jvm_threads232_i25.txt	0.13	March 5, 2014 6:47:24 PM PST	/net/slc03qsy/scratch/rdabbott/view_storage/rdabbott_w/work/user_projects/domains/EMGC_DOMAIN/servers/EMGC_OMS1/adr/diag/ofm/EMGC_DOMAIN/EMOMS/incident/incdir_25	👓

3. In the Support Workbench Problem Details page, either click the **Package the Problem** link or the **Quick Package** button as shown below, then follow the instructions in the Quick Packaging wizard and online help.



slc03qsy.us.oracle.com:7654_Management_Service

Oracle Management Service

slc03qsy.us.oracle.com

slc03qsy.us.oracle.com:7654_Management_Service > Support Workbench > Problem Details: EM-00181 [EMOMS...

Problem Details: EM-00181 [EMOMS_PBS][emdrep.jobs.CommandBlockManager]

Page Refreshed **March 6, 2014 12:55:44 PM PST** Refresh

Summary

SR#	--	Edit
Bug#	--	Edit
Problem Id	2	
Number of Incidents	5	
First Incident	March 5, 2014 6:47:24 PM PST	
Active	Yes	
Packaged	No	

Last Dumped Incident

Timestamp	March 5, 2014 6:48:56 PM PST
Incident Source	System Generated
User Impact	
Checkers Run	0
Checker Findings	0

Investigate and Resolve

Quick Package

Diagnose

Related Problems Across Topology
Diagnostics for Last Dumped Incident
Run EM Diagnostics Kit for Last Dumped Incident
Search Knowledge Base

Collect and Send Diagnostic Data

Package the Problem

Track and Close

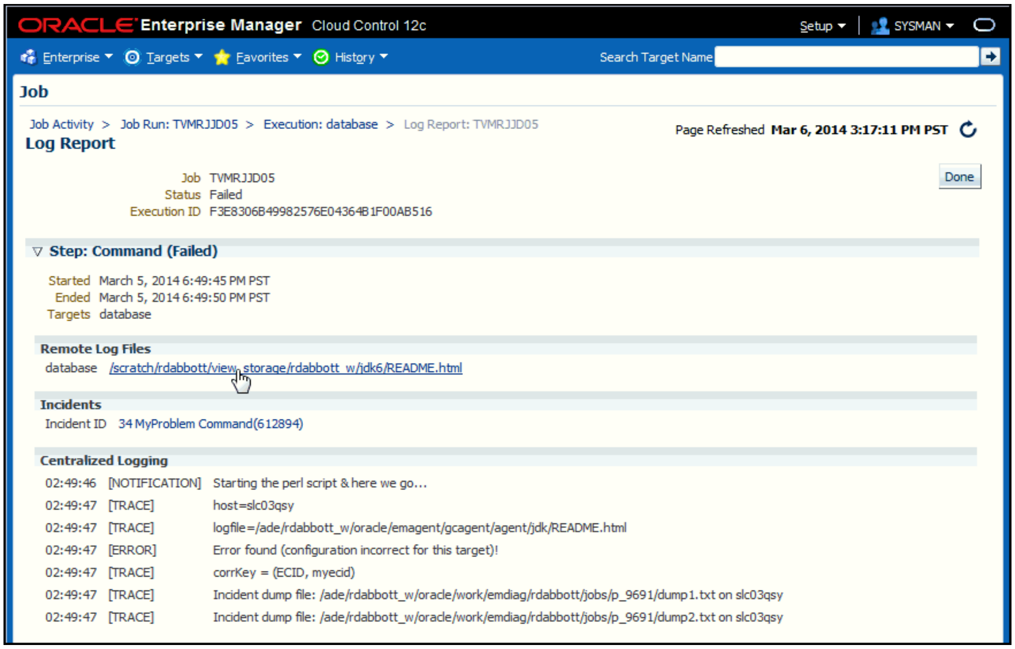
Manage problem resolution

11.7.6 Viewing Remote Log Files

Some jobs or Provisioning Adviser Framework (PAF) procedures run external commands, such as DBCA or the installer. These commands generate their own log files local to the system and Oracle home where they ran.

To view remote log files:

1. In the Top Activity page, click the link of the job for which you want to view the log.
2. In the Job Run table, click **Log Report**.
3. In the Log Report page, click the **Remote Log Files** link as shown below.


ORACLE Enterprise Manager Cloud Control 12c
Setup
SYSMAN
Enterprise
Targets
Favorites
History
Search Target Name
Job
Job Activity > Job Run: TVMRJJD05 > Execution: database > Log Report: TVMRJJD05
Done

Log Report

Page Refreshed **Mar 6, 2014 3:17:11 PM PST**

Job TVMRJJD05
Status Failed
Execution ID F3E8306B49982576E04364B1F00AB516

Step: Command (Failed)

Started March 5, 2014 6:49:45 PM PST
Ended March 5, 2014 6:49:50 PM PST
Targets database

Remote Log Files

database /scratch/rdabbott/view_storage/rdabbott_w/jdk6/README.html

Incidents

Incident ID 34 MyProblem Command(612894)

Centralized Logging

```
02:49:46  [NOTIFICATION]  Starting the perl script & here we go...
02:49:47  [TRACE]         host=slc03qsy
02:49:47  [TRACE]         logfile=/ade/rdabbott_w/oracle/emagent/gcagent/agent/jdk/README.html
02:49:47  [ERROR]         Error found (configuration incorrect for this target)!
02:49:47  [TRACE]         corrKey = (ECID, myecid)
02:49:47  [TRACE]         Incident dump file: /ade/rdabbott_w/oracle/work/emdiag/rdabbott/jobs/p_9691/dump1.txt on slc03qsy
02:49:47  [TRACE]         Incident dump file: /ade/rdabbott_w/oracle/work/emdiag/rdabbott/jobs/p_9691/dump2.txt on slc03qsy
```

4. Specify host credentials, then click **OK**.

   The Remote File Viewer appears and displays the file contents.

11.7.7 Diagnosing Problems with Cloud Control Management Tools

The Cloud Control management portion of the console provides several tools that can assist you in assessing the current state of the job system and determining a proper course of action for optimum performance. All of these tools are accessible from the Setup menu of the Cloud Control console.

The following sections provide information on each of the available tools.

11.7.7.1 Health Overview

1. From the Setup menu of the Cloud Control console, select **Manage Cloud Control**.
2. Select the **Health Overview** sub-menu.

The Job System Status region of the Health Overview page displays the following information:

- **Step Scheduler Status**

  The job step scheduler processes the job steps that are ready to run. If the status indicates that job step scheduler is running in warning or error mode, the job system is not functioning normally. In this case, the job system may run in fail-over mode, where the job dispatcher process may also run the task performed by the job step scheduler periodically. However, the job system may be running below its potential capacity, so resolving this situation would be beneficial.

  Several possible messages can appear:

  – DBMS_SCHEDULER job for step-scheduler not found

    This message is very rare and usually indicates a potentially serious issue. The job was likely removed inadvertently or due to some special processing (patch installation, for example, that requires recycling all DBMS_SCHEDULER jobs). No automatic resolution is possible here, and this would need to be addressed on a case by case basis.

  - Failure in checking status

    This is a rare occurrence. The error message is usually shown. The error may disappear on its own as this error indicates that the status could not be calculated.

  - DBMS_SCHEDULER is disabled

    All of the DBMS_SCHEDULER jobs are disabled in the environment. This should not occur unless a type of installation is in progress. Resolve this by starting DBMS_SCHEDULER processes.

  - All job queue processes are in use

    The DBMS_SCHEDULER processes have been expended. Increase the parameter job_queue_processes in the repository RDBMS.

  - All slave processes are in use

    The cause is similar to the above case. In this situation, you need to increase MAX_JOB_SLAVE_PROCESSES of the DBMS_SCHEDULER.

  - All sessions are in use

    No RDBMS sessions were available for the DBMS_SCHEDULER. Increase the PROCESSES for the RDBMS.

  - Reason for delay could not be established

    This usually appears because none of the above criteria were met, and is the most common warning. The dispatcher may just be overloaded because there is more work than available workers. Check the backlog in this case. The situation should resolve automatically, but if it persists, the number of workers available for the job system may be insufficient for the load the site experiences.

- **Job Backlog**

  The job backlog indicates the number of job steps that have passed their scheduled time but have not executed yet. If this number is high and has not decreased for a long period, the job system is not functioning normally. This situation usually arises if job engine resources are unable to meet the inflow of jobs from system or user activity.

  A high backlog can also happen because of the abnormal processing of specific jobs because they are stuck for extended periods. For more information on stuck job worker threads, do the following:

  1. From the OMS and Repository menu of the Health Overview page, select **Monitoring**, then **Diagnostic Metrics**.

  If the jobs system has a backlog for long periods of time, or if you would like to process the backlog faster, set the following parameters with the emctl set property command. These settings assume that sufficient database resources are available to support more load. These parameters are likely to be needed in a Large configuration with 2 OMS nodes.

Table 11–1 Large Job System Backlog Settings

Parameter	Value
oracle.sysman.core.jobs.shortPoolSize	50
oracle.sysman.core.jobs.longPoolSize	24
oracle.sysman.core.jobs.longSystemPoolSize	20
oracle.sysman.core.jobs.systemPoolSize	50
oracle.sysman.core.conn.maxConnForJobWorkers	144 *

* This setting may require an increase of the processes setting in the database of 144 * number of OMS servers.

11.7.7.2 Repository Home Page

1. From the Setup menu of the Cloud Control console, select **Manage Cloud Control**.
2. Select the **Repository** sub-menu.

The Repository Scheduler Jobs Status table in the Management Services and Repository page displays the job system purge status and next run schedule.

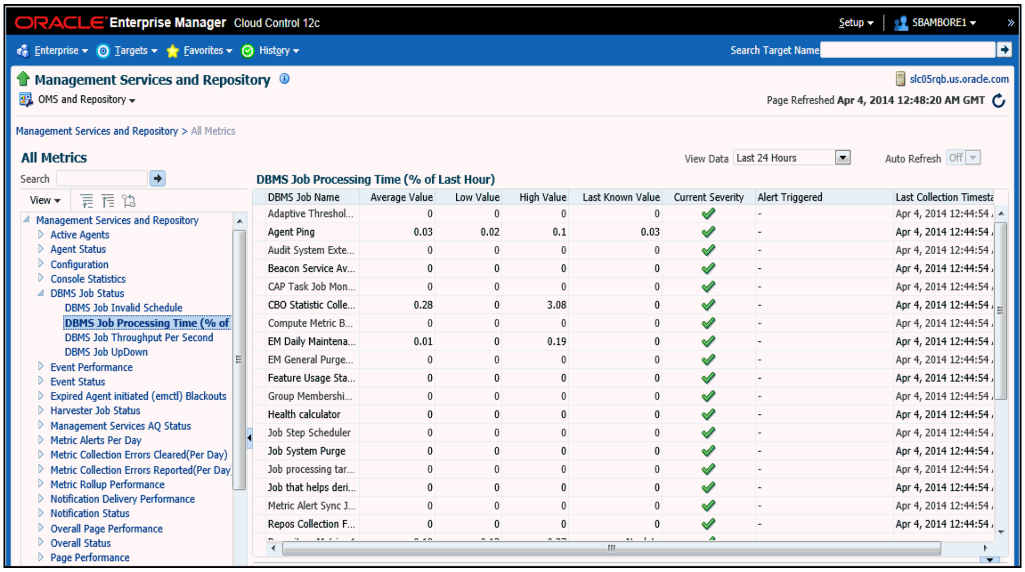
11.7.7.3 Management Services and Repository: All Metrics

There are two navigation paths for accessing the All Metrics page:

- From the Setup menu
- From the Targets menu

Setup Menu Navigation

1. From the Setup menu of the Cloud Control console, select **Manage Cloud Control**.
2. Select the **Health Overview** sub-menu.
3. From the Management Services and Repository page that appears, select **Monitoring** from the OMS and Repository menu, then select **All Metrics**.
4. Scroll down to DBMS Job Status in the left pane, then select a metric as shown below.


ORACLE Enterprise Manager Cloud Control 12c
Setup
SBAMBORE1
Enterprise
Targets
Favorites
History
Search Target Name
Management Services and Repository
OMS and Repository
slc05rqb.us.oracle.com
View
Management Services and Repository
Active Agents
Agent Status
Configuration
Console Statistics
DBMS Job Status
DBMS Job Invalid Schedule
DBMS Job Processing Time (% of
DBMS Job Throughput Per Second
DBMS Job UpDown
Event Performance
Event Status
Expired Agent initiated (emctl) Blackouts
Harvester Job Status
Management Services AQ Status
Metric Alerts Per Day
Metric Collection Errors Cleared(Per Day)
Metric Collection Errors Reported(Per Day
Metric Rollup Performance
Notification Delivery Performance
Notification Status
Overall Page Performance
Overall Status
Page Performance

Page Refreshed **Apr 4, 2014 12:48:20 AM GMT**

Management Services and Repository > All Metrics

All Metrics

Search

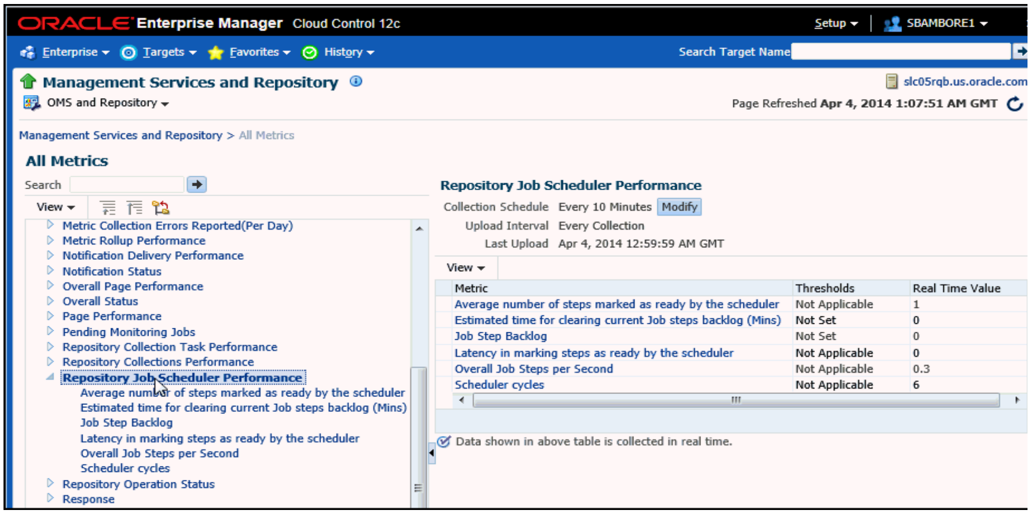
View Data Last 24 Hours

Auto Refresh Off

DBMS Job Processing Time (% of Last Hour)

DBMS Job Name	Average Value	Low Value	High Value	Last Known Value	Current Severity	Alert Triggered	Last Collection Timesta
Adaptive Threshol...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Agent Ping	0.03	0.02	0.1	0.03	✓	-	Apr 4, 2014 12:44:54
Audit System Exte...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Beacon Service Av...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
CAP Task Job Mon...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
CBO Statistic Colle...	0.28	0	3.08	0	✓	-	Apr 4, 2014 12:44:54
Compute Metric B...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
EM Daily Maintena...	0.01	0	0.19	0	✓	-	Apr 4, 2014 12:44:54
EM General Purge...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Feature Usage Sta...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Group Membershi...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Health calculator	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Job Step Scheduler	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Job System Purge	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Job processing tar...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Job that helps deri...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Metric Alert Sync J...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54
Repos Collection F...	0	0	0	0	✓	-	Apr 4, 2014 12:44:54

5. Scroll down further and expand Repository Job Scheduler Performance as shown below.


ORACLE Enterprise Manager Cloud Control 12c
Setup
SBAMBORE1
Enterprise
Targets
Favorites
History
Search Target Name
Management Services and Repository
OMS and Repository
slc05rqb.us.oracle.com
View
Metric Collection Errors Reported(Per Day)
Metric Rollup Performance
Notification Delivery Performance
Notification Status
Overall Page Performance
Overall Status
Page Performance
Pending Monitoring Jobs
Repository Collection Task Performance
Repository Collections Performance
Repository Job Scheduler Performance
Average number of steps marked as ready by the scheduler
Estimated time for clearing current Job steps backlog (Mins)
Job Step Backlog
Latency in marking steps as ready by the scheduler
Overall Job Steps per Second
Scheduler cycles
Repository Operation Status
Response
View
Modify

Page Refreshed **Apr 4, 2014 1:07:51 AM GMT**

Management Services and Repository > All Metrics

All Metrics

Search

Repository Job Scheduler Performance

Collection Schedule Every 10 Minutes

Upload Interval Every Collection

Last Upload Apr 4, 2014 12:59:59 AM GMT

Metric	Thresholds	Real Time Value
Average number of steps marked as ready by the scheduler	Not Applicable	1
Estimated time for clearing current Job steps backlog (Mins)	Not Set	0
Job Step Backlog	Not Set	0
Latency in marking steps as ready by the scheduler	Not Applicable	0
Overall Job Steps per Second	Not Applicable	0.3
Scheduler cycles	Not Applicable	6

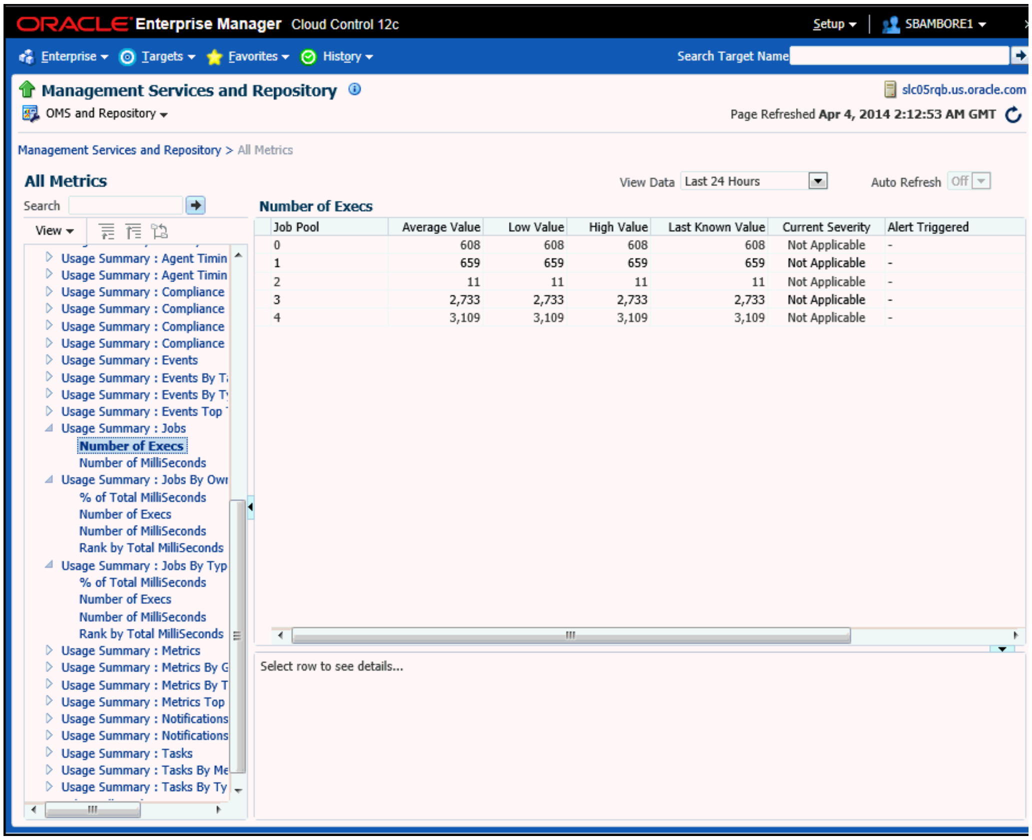
Data shown in above table is collected in real time.

Definitions for the available metrics are as follows:

- **Average number of steps marked as ready by the scheduler** — Average number of steps processed by the job step scheduler to mark the steps "ready" for execution. This number usually depends on the job system load over a time period.
- **Estimated time for clearing current Job steps backlog (Mins)** — Estimated time to clear the backlog assuming the current inflow rate of the job system.
- **Job step backlog** — Number of job steps that have passed their scheduled time but have not executed yet. If this number is high and has not decreased for a long period, the job system is not functioning normally. This situation usually arises if job engine resources are unable to meet the inflow of jobs from system or user activity.

- **Latency in marking steps as ready by the scheduler** — The job step scheduler moves scheduled steps to ready queue. This metric indicates the average latency in marking the steps to ready queue. High latency means abnormal functioning of the job step scheduler process.
- **Overall job steps per second** — Average number of steps the job system executes per second.
- **Scheduler cycles** — Frequency of dbms scheduler process. Executes a minimum of 5 cycles per min, and may increase depending on the job system load. A low number usually indicates a problem in the job step scheduler process.

6. Scroll down further and expand the Usage Summary entries for Jobs, then select the metric for which you are interested as shown below.


ORACLE Enterprise Manager Cloud Control 12c
Setup
SBAMBORE1
Enterprise
Targets
Favorites
History
Search Target Name
Management Services and Repository
OMS and Repository
slc05rqb.us.oracle.com
Management Services and Repository > All Metrics
All Metrics
Search
View
Usage Summary : Agent Timin
Usage Summary : Agent Timin
Usage Summary : Compliance
Usage Summary : Compliance
Usage Summary : Compliance
Usage Summary : Compliance
Usage Summary : Events
Usage Summary : Events By T
Usage Summary : Events By T
Usage Summary : Events Top
Usage Summary : Jobs
Number of Execs
Number of MilliSeconds
Usage Summary : Jobs By Ow
% of Total MilliSeconds
Number of Execs
Number of MilliSeconds
Rank by Total MilliSeconds
Usage Summary : Jobs By Typ
% of Total MilliSeconds
Number of Execs
Number of MilliSeconds
Rank by Total MilliSeconds
Usage Summary : Metrics
Usage Summary : Metrics By G
Usage Summary : Metrics By T
Usage Summary : Metrics Top
Usage Summary : Notifications
Usage Summary : Notifications
Usage Summary : Tasks
Usage Summary : Tasks By Me
Usage Summary : Tasks By Ty
View Data
Auto Refresh
Off

Page Refreshed **Apr 4, 2014 2:12:53 AM GMT**

View Data: Last 24 Hours

Number of Execs

Job Pool	Average Value	Low Value	High Value	Last Known Value	Current Severity	Alert Triggered
0	608	608	608	608	Not Applicable	-
1	659	659	659	659	Not Applicable	-
2	11	11	11	11	Not Applicable	-
3	2,733	2,733	2,733	2,733	Not Applicable	-
4	3,109	3,109	3,109	3,109	Not Applicable	-

Select row to see details...

Target Menu Navigation

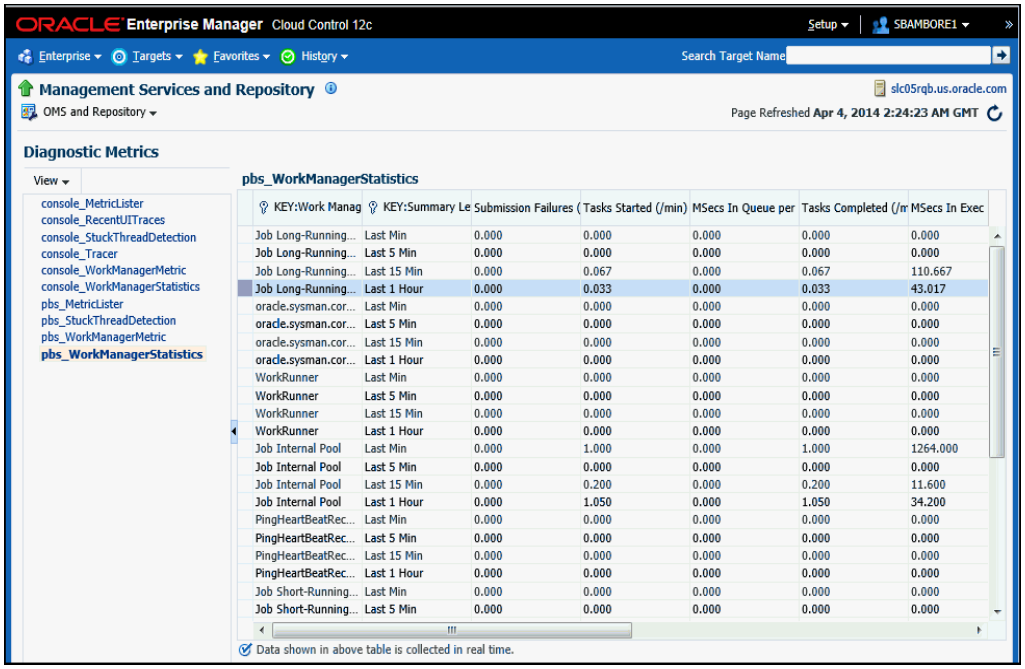
1. From the Targets menu of the Cloud Control console, select **All Targets**.
2. In the left pane of the All Targets page, scroll down and expand **Internal**, then select **OMS and Repository**.
3. Click on the **OMS and Repository** table entry in the page that follows.
4. From the OMS and Repository menu in the Health Overview page that appears, select **Monitoring**, then **All Metrics**.

11.7.7.4 OMS and Repository: Diagnostic Metrics

1. From the Setup menu of the Cloud Control console, select **Manage Cloud Control**.
2. Select the **Health Overview** sub-menu.

3. From the Management Services and Repository page that appears, select **Monitoring** from the OMS and Repository menu, then select **Diagnostic Metrics**.

pbs_* metrics are relevant for diagnosing issues in the job system. This information is useful if you are searching for more information on stuck job system threads, or job threads usage statistics to determine outliers preventing other jobs from running.



pbs_WorkManagerStatistics

KEY:Work Manag	KEY:Summary Le	Submission Failures (	Tasks Started (/min)	MSecs In Queue per	Tasks Completed (/m	MSecs In Exec
Job Long-Running...	Last Min	0.000	0.000	0.000	0.000	0.000
Job Long-Running...	Last 5 Min	0.000	0.000	0.000	0.000	0.000
Job Long-Running...	Last 15 Min	0.000	0.067	0.000	0.067	110.667
Job Long-Running...	Last 1 Hour	0.000	0.033	0.000	0.033	43.017
oracle.sysman.cor...	Last Min	0.000	0.000	0.000	0.000	0.000
oracle.sysman.cor...	Last 5 Min	0.000	0.000	0.000	0.000	0.000
oracle.sysman.cor...	Last 15 Min	0.000	0.000	0.000	0.000	0.000
oracle.sysman.cor...	Last 1 Hour	0.000	0.000	0.000	0.000	0.000
WorkRunner	Last Min	0.000	0.000	0.000	0.000	0.000
WorkRunner	Last 5 Min	0.000	0.000	0.000	0.000	0.000
WorkRunner	Last 15 Min	0.000	0.000	0.000	0.000	0.000
WorkRunner	Last 1 Hour	0.000	0.000	0.000	0.000	0.000
Job Internal Pool	Last Min	0.000	1.000	0.000	1.000	1264.000
Job Internal Pool	Last 5 Min	0.000	0.000	0.000	0.000	0.000
Job Internal Pool	Last 15 Min	0.000	0.200	0.000	0.200	11.600
Job Internal Pool	Last 1 Hour	0.000	1.050	0.000	1.050	34.200
PingHeartBeatRec...	Last Min	0.000	0.000	0.000	0.000	0.000
PingHeartBeatRec...	Last 5 Min	0.000	0.000	0.000	0.000	0.000
PingHeartBeatRec...	Last 15 Min	0.000	0.000	0.000	0.000	0.000
PingHeartBeatRec...	Last 1 Hour	0.000	0.000	0.000	0.000	0.000
Job Short-Running...	Last Min	0.000	0.000	0.000	0.000	0.000
Job Short-Running...	Last 5 Min	0.000	0.000	0.000	0.000	0.000

Data shown in above table is collected in real time.

11.7.7.5 OMS and Repository: Charts

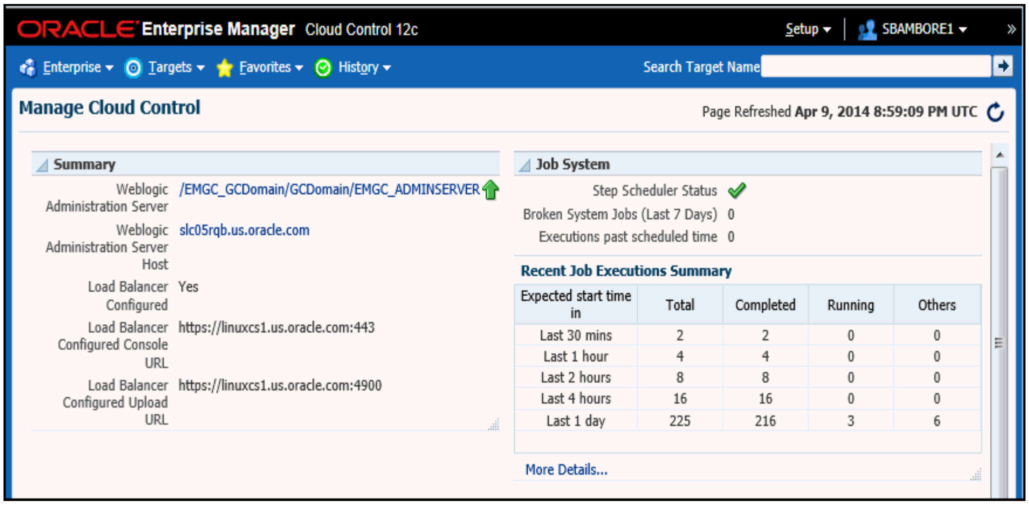
1. From the Setup menu of the Cloud Control console, select **Manage Cloud Control**.
2. Select the **Health Overview** sub-menu.
3. From the Management Services and Repository page that appears, select **Monitoring** from the OMS and Repository menu, then select **Charts**.

Assuming that the job had steps, this page shows historical charts for the overall upload backlog, job step backlog, and overall job steps per second.

11.7.7.6 Management Servers and Job Activity Details Pages

1. From the Targets menu of the Cloud Control console, select **All Targets**.
2. On the left pane under Groups, Systems, and Services, click **Management Servers**.
3. Click **Management Servers** in the Target Name table.

   The Job System region displays a snapshot of job system status and details of processed executions. The Recent Job Executions Summary table displays the total user job executions that are expected to run within a specific time period, the completed count, running count, and the count of executions that are neither completed nor running. This helps you to determine if various user jobs are running as expected in the system.



Manage Cloud Control

Page Refreshed **Apr 9, 2014 8:59:09 PM UTC**

Summary

Weblogic Administration Server	/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER
Weblogic Administration Server Host	slc05rqb.us.oracle.com
Load Balancer Configured	Yes
Load Balancer Configured Console URL	https://linuxcs1.us.oracle.com:443
Load Balancer Configured Upload URL	https://linuxcs1.us.oracle.com:4900

Job System

Step Scheduler Status	✓
Broken System Jobs (Last 7 Days)	0
Executions past scheduled time	0

Recent Job Executions Summary

Expected start time in	Total	Completed	Running	Others
Last 30 mins	2	2	0	0
Last 1 hour	4	4	0	0
Last 2 hours	8	8	0	0
Last 4 hours	16	16	0	0
Last 1 day	225	216	3	6

More Details...

4. Click the **More Details** link below the summary table.

5. Select the desired time frame in the drop-down for when executions are expected to start.

   Jobs and their status, if any, appear in the table.

6. Select the **Job Dispatchers** tab.

   If more than one management server is configured, the page displays the job dispatcher and thread pool utilization information for each management servers.

   - **Dispatcher Utilization (%)** — Measures how frequently the job dispatcher picks up the job steps. High utilization indicates a heavy job system load.
   - **Throughput (steps dispatched/min)** — Indicates the average number of steps other than internal steps processed by dispatcher every minute.
   - **Thread Pool Utilization** — Displays the total number of threads configured for each pool, the average steps selected by the thread pool per minute, and the average number of available threads.

11.7.7.7 Job System Reports

The job system provides both a diagnostic report and usage report.

Diagnostic Report

1. From the Setup Enterprise of the Cloud Control console, select **Reports**.
2. Select the **Information Publisher Reports** sub-menu.
3. Search for **job** in the Title field, then click **Go**.
4. Click the **Job System Diagnostic Report** link in the table.

This report provides an overview of the job system's health and displays diagnostic information about executing jobs or jobs that are possibly delayed beyond their scheduled time. This information is usually relevant for an Oracle Support engineer diagnosing problems in the job system.

Usage Report

Follow the steps above to access this report, except click the **Job Usage Report** link in step 4.

This report provides an overview of the job system usage information over the past 7 days.

11.8 Creating Corrective Actions

Corrective Actions enable you to specify automated responses to metric alerts. Corrective Actions ensure that routine responses to metric alerts are automatically executed, thereby saving you time and ensuring problems are dealt with before they noticeably impact end users.

Corrective actions share many features in common with the Job System. By default, a corrective action runs on the target on which the metric alert is triggered. Alternatively, you can specify a corrective action to contain multiple tasks, with each task running on a different target. You can also receive notifications for the success or failure of corrective actions.

You define corrective actions for individual metrics for monitored targets. The following sections provide instructions on setting up corrective actions and viewing the details of a corrective action execution:

- Providing Credentials
- Creating Corrective Actions for Metrics
- Creating a Library Corrective Action
- Specifying Access to Corrective Actions
- Setting Up Notifications for Corrective Actions
- Providing Agent-side Response Actions
- Viewing the Details of a Corrective Action Execution

11.8.1 Providing Credentials

Since corrective actions are associated with a target's metric thresholds, you can define corrective actions if you have been granted OPERATOR or greater privilege on the target. You can define separate corrective actions for both Warning and Critical thresholds. Corrective actions must run using the credentials of a specific user. For this reason, whenever a corrective action is created or modified, you must specify the credentials that the modified action runs with.

11.8.2 Creating Corrective Actions for Metrics

For any target, the Metric and Collection Settings page shows whether corrective actions have been set for various metrics. For each metric, the Corrective Actions column shows whether Critical and/or Warning severities of corrective actions have been set.

1. From any target’s home page menu, select **Monitoring**, then **Metric and Collection Settings**. The Metric and Collection Settings page appears.

   Tip: For instance, on the home page for a host named dadvmn0630.myco.com, you would select the Host menu, then Monitoring, then Metric and Collection Settings.

2. Click the pencil icon for a specific metric to access the Edit Advanced Settings page for the metric.

3. In the Corrective Actions section, click **Add** for the metric severity (Warning and/or Critical) for which you want to associate a corrective action.

4. Select the task type on the Add Corrective Actions page, then click **Continue**.

   - If you want to use a corrective action from the library, select **From Library** as the task type. Using a library corrective action copies the description, parameters, and credentials from the library corrective action. You must still define a name for the new corrective action. You can provide corrective action parameters if necessary.

   - If you want to create a corrective action to store in the library, see Section 11.8.3, "Creating a Library Corrective Action."

   - If you want to provide an Agent-side response action, select Agent Response Action as the task type. See Section 11.8.6, "Providing Agent-side Response Actions" for more information.

5. On the Corrective Action page, provide input for General, Parameters, and Credentials as you would similarly do when creating a job.

6. Click **Continue** to save the corrective action and return to the Edit Advanced Settings page, where your corrective action now appears.

7. *Optional*: To prevent multiple instances of a corrective action from operating simultaneously, enable the **Allow only one corrective action for this metric to run at any given time** checkbox.

   This option specifies that both Critical and Warning corrective actions will not run if a severity is reported to the Oracle Management Services when an execution of either corrective action is currently running. This can occur if a corrective action runs longer than the collection interval of the metric it corrects; the value of the metric may be oscillating back and forth across one of the thresholds (leading to multiple executions of the same corrective action), or may be rising or falling quickly past both thresholds (in which case an execution of the Warning corrective action may overlap an execution of the Critical corrective action).

   If you do not select this option, multiple corrective action executions are launched under the aforementioned circumstances. It is the administrator’s responsibility to ensure that the simultaneous corrective action executions do not conflict.

8. Click **Continue** when you have finished adding corrective actions to return to the Metric and Collection Settings page.

   The page shows the corrective action value you have provided for the metric in the Corrective Actions column. Possible values are:

   - **None** — No corrective actions have been set for this metric.

   - **Warning** — A corrective action has been set for Warning, but not Critical, alerts for this metric.

   - **Critical** — A corrective action has been set for Critical, but not Warning, alerts for this metric.

   - **Warning and Critical** — Corrective actions have been set for both Warning and Critical alerts for this metric. If an Agent-side response action is associated with the metric, the value is also Warning and Critical, since Agent-side response actions are always triggered on either Critical or Warning alert severities.

9. Continue the process from step 2 forward, then click **OK** on the Metric and Collection Settings page to save your corrective actions and return to the target page you started from in step 1.

11.8.3 Creating a Library Corrective Action

For corrective actions that you use repeatedly, you can define a library corrective action. After a corrective action is in the library, you can reuse the corrective action definition whenever you define a corrective action for a target metric or policy rule.

1. From the Enterprise menu, select **Monitoring**, then **Corrective Actions**. The Corrective Action Library page appears.
2. Select a job type from the **Create Library Corrective Action** drop-down, then click **Go**.
3. Define the corrective action as you would for creating a job in Section 11.3, "Creating Jobs" for General, Parameters, and Credentials. For Access, go to the following optional step.
4. *Optional*: Select **Access** to define or modify the access you want other users to have for this corrective action.

   For more information, see Section 11.8.4, "Specifying Access to Corrective Actions."
5. Click **Save to Library** when you have finished. The Corrective Action Library page reappears, and your corrective action appears in the list.

   You can now create another corrective action based on this one (Create Like button), edit, or delete this corrective action.

You can access this library entry whenever you define a corrective action for a metric severity by selecting From Library as the task type in the Add Corrective Actions page. See step 4 in Section 11.8.2, "Creating Corrective Actions for Metrics," for more information.

11.8.4 Specifying Access to Corrective Actions

As mentioned in the procedure above, you can determine the access to corrective actions by other users. You do not need to provide input for this page if you do not want to share the corrective action.

11.8.4.1 Defining or Modifying Access

The table on the Access page shows the access that administrators and roles have to the corrective action. Only the corrective action owner (or Super Administrator) can make changes on this page.

As the corrective action owner, you can do the following:

- Add other administrators and roles to the table by clicking **Add**, then selecting the appropriate type in the subsequent page that appears.
- Change the access of an administrator or role by choosing the **Full** or **View** access right in the Access Level column in the table.
- Remove all access to the corrective action for an administrator or role by clicking the icon in the **Remove** columns for this administrator or role. All administrators with Super Administrator privileges have the View access right to a corrective action.

If you choose to provide access rights to a role, you can only provide the View access right to the role, not the Full access right.

If you are a Super Administrator, you can:

- Grant View access to other Enterprise Manager administrators or roles.
- Revoke all administrator access privileges.

Note: If a new user is being created, the user should have the CREATE_JOB privilege to create Corrective Actions.

11.8.4.2 Access Level Rules

Access level rules are as follows:

- Super Administrators always have View access for any corrective action.
- The Enterprise Manager administrator who owns the corrective action can make any access changes to the corrective action (except revoking View from Super Administrators).
- Super Administrators with a View or Full access level for a corrective action can grant View (but not Full) access to any new user. Super Administrators can also revoke Full and View access from normal users, and Full access from Super Administrators.
- Normal Enterprise Manager administrators with Full access levels cannot make any access changes on the corrective action.
- If the corrective action owner performs a Create Like operation on a corrective action, all access privileges for the new corrective action become identical to the original corrective action. If the corrective action owner grants other administrators View or Full access to other administrators, and any of these administrators perform a Create Like operation on this corrective action, all administrators will, by default, have View access on the newly created corrective action.

11.8.5 Setting Up Notifications for Corrective Actions

Corrective actions are associated with metrics whose alerts trigger them. Any Enterprise Manager administrator with View or higher privileges on a target can receive notifications following the success or failure of a corrective action.

A single incident rule can contain any combination of alert and corrective action states. All metrics and targets selected by the incident rule are notified for the same alert and corrective action states. Therefore, if you want to be notified of corrective action success or failure for one metric, but only on failure for another, you need to use two incident rules. An incident rule can include corrective action states for metrics with which no corrective actions have been associated. In this case, no notifications are sent.

Note: Notifications cannot be sent for Agent-side response actions, regardless of the state of any incident rules applied to the target.

To create incident rules for notifications:

1. From the Setup menu, select **Incidents**, then **Incident Rules**.
2. Click **Create Rule Set**. The Create Rule Set wizard appears.

3. Provide the requisite information at the top of the Create Rule Set page, then select one of the target choices in the Targets sub-tab, supplying additional information as needed for the "All targets of types" and "Specific targets" choices.
4. Select the **Rules** sub-tab, then click **Create**.
5. In the pop-up that appears, select the default **Incoming events and update to events** choice, the click **Continue**.
6. On the Select Events page, enable the **Type** checkbox, then select **Metric Alert**.
7. Click the **Specific events of type Metric alert** radio button, then click **Add** in the table that appears.
8. In the pop-up that appears, select the Target Type, filter and select the metric, select a severity, then enable the desired corrective action status. Click **OK**.
9. From the Add Actions page, click **Add**.
10. Specify recipients in the Basic Notifications section of the Add Conditional Actions page.
11. Proceed through the final two pages of the wizard, then click **Continue**. Your new rule appears in the Create Rule Set page.
12. Click **Save** to save this rule.

After you have created one or more rule sets, you need to set up notification methods as follows:

1. From the Setup menu, select **Notifications**, then **Notification Methods**.
2. From the Notification Methods page, select **Help**, then **Enterprise Manager Help** for assistance on providing input for this page.

11.8.6 Providing Agent-side Response Actions

Agent-side response actions perform simple commands in response to an alert. When the metric triggers a warning or critical alert, the Management Agent automatically runs the specified command or script without requiring coordination with the Oracle Management Service (OMS). The Agent runs this command or script as the OS user who owns the Agent executable. Specific target properties can be used in the Agent response action script.

> **Note:** Use the Agent-side Response Action page to specify a single command-line action to be executed when a Warning or Critical severity is reached for a metric. For tasks that require alert context, contain more complex logic, or require that notifications be sent on success or failure, corrective actions should be used instead of an Agent-side response action.

To access this page, follow steps 1 through 4 in Section 11.8.2, "Creating Corrective Actions for Metrics."

11.8.6.1 Specifying Commands and Scripts

You can specify a single command or execute a script. You cannot specify special shell command characters (such as > and <) as part of the response action command. If you must include these types of special characters in your response action commands, you should use them in a script, then specify the script as the response action command.

If using a script, make sure the script is installed on the host machine that has the Agent. If using shell scripts, make sure the shell is specified either in the Response Action command line:

Script/Command: /bin/csh myScript

... or within the body of the script itself:

Script/Command: myScript

... where myScript contains the following:

```
!#/bin/csh<
<rest of script>
```

11.8.6.2 Using Target Properties in Commands

You can use target properties in a command. Click **Show Available Target Properties** to display target properties you can use in the Script/Command field. The list of available target properties changes according to the type of target the response action is to run against.

Use Target Properties as command-line arguments to the script or command, then have the script reference these command-line arguments. For example, to use the %OracleHome% and %SID% target properties, your command might appear as follows:

```
/bin/csh MyScript %OracleHome% %SID%
```

.... and your script, MyScript, can reference these properties as command-line arguments. For example:

```
IF $1 = 'u1/bin/OracleHome' THEN...
```

Target properties are case-sensitive. For example, if you want to access the Management Agent's Perl interpreter, you can specify %perlBin%/perl <my_perl_script> in the Script/Command field.

11.8.6.3 Using Advanced Capabilities

You can get other target properties from the target's XML file in the OracleHome/sysman/admin/metadata directory, where OracleHome is the Oracle home of the Management Agent that is monitoring the target. In the XML file, look for the PROP_LIST attribute of the DynamicProperties element to get a list of properties that are not listed in the targets.xml entry for the target.

The following example is an excerpt from the hosts.xml file:

```
<InstanceProperties>
 <DynamicProperties NAME="Config" FORMAT="ROW"
 PROP_LIST="OS;Version;OS_patchlevel;Platform;Boottime;IP_address">
   <ExecutionDescriptor>
   <GetTable NAME="_OSConfig"/>
   <GetView NAME="Config" FROM_TABLE="_OSConfig">
   <ComputeColumn NAME="osName" EXPR="Linux" IS_VALUE="TRUE"/>
   <Column NAME="osVersion"/>
   <Column NAME="osPatchLevel"/>
   <Column NAME="Platform"/>
   <Column NAME="Boottime"/>
   <Column NAME="IPAddress"/>
   </GetView>
   </ExecutionDescriptor>
   </DynamicProperties>
   <InstanceProperty NAME="Username" OPTIONAL="TRUE" CREDENTIAL="TRUE">
   <ValidIf>
   <CategoryProp NAME="OS" CHOICES="Linux"/>
   </ValidIf>
   <Display>
   <Label NLSID="host_username_iprop">Username</Label>
   </Display>
   </InstanceProperty>
   <InstanceProperty NAME="Password" OPTIONAL="TRUE" CREDENTIAL="TRUE">
   <ValidIf>
   <CategoryProp NAME="OS" CHOICES="Linux"/>
   </ValidIf>
   <Display>
   <Label NLSID="host_password_iprop">Password</Label>
   </Display>
   </InstanceProperty>
</InstanceProperties>
```

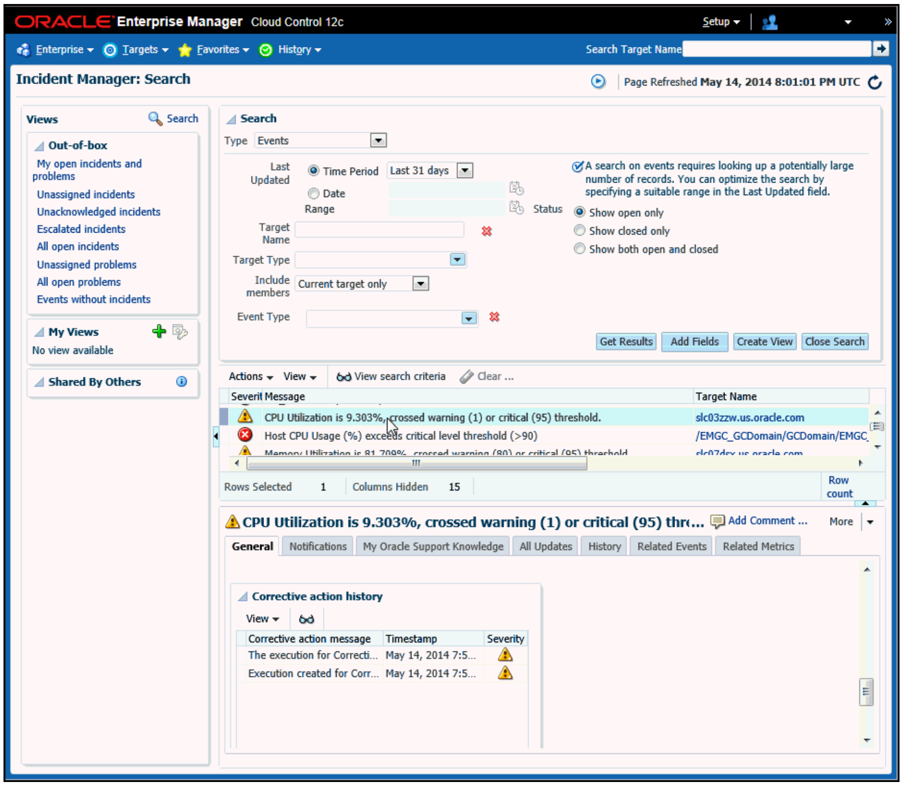
11.8.7 Viewing the Details of a Corrective Action Execution

There are two methods of displaying the outcome of a corrective action execution.

- Incident Manager method

  1. From the Enterprise Manager Cloud Control console Enterprise menu, select **Monitoring**, then **Incident Manager**.
  2. Click the **Search** icon, select **Events** from the Type drop-down, then click **Get Results**.
  3. Double-click the message of interest in the search results table.

     The Corrective Action History table now appears at the bottom of the page, as shown below.



Incident Manager: Search

Page Refreshed May 14, 2014 8:01:01 PM UTC

Search

Type: Events

Last Updated: ● Time Period Last 31 days ○ Date Range

Target Name:

Target Type:

Include members: Current target only

Event Type:

A search on events requires looking up a potentially large number of records. You can optimize the search by specifying a suitable range in the Last Updated field.

Status: ● Show open only ○ Show closed only ○ Show both open and closed

Severit	Message	Target Name
⚠	CPU Utilization is 9.303%, crossed warning (1) or critical (95) threshold.	slc03zzw.us.oracle.com
⊗	Host CPU Usage (%) exceeds critical level threshold (>90)	/EMGC_GCDomain/GCDomain/EMGC_
⚠	Memory Utilization is 81.709%, crossed warning (80) or critical (95) threshold	slc07dsx.us.oracle.com

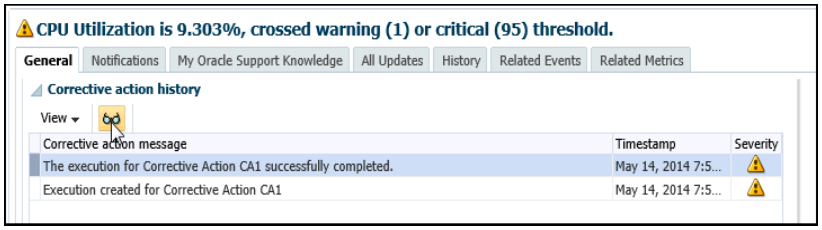
Rows Selected 1 Columns Hidden 15

⚠ CPU Utilization is 9.303%, crossed warning (1) or critical (95) thr...

Corrective action history

Corrective action message	Timestamp	Severity
The execution for Correcti...	May 14, 2014 7:5...	⚠
Execution created for Corr...	May 14, 2014 7:5...	⚠

4. Select the desired message in the history table, then click the glasses icon as shown below.



⚠ CPU Utilization is 9.303%, crossed warning (1) or critical (95) threshold.

Corrective action history

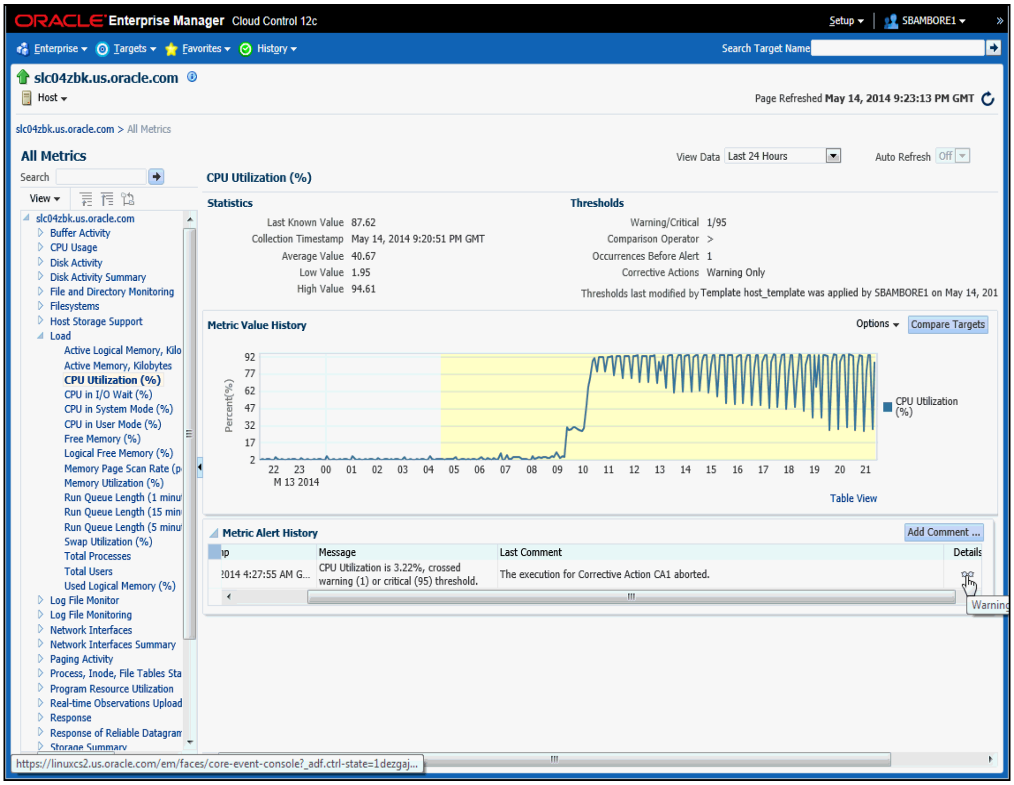
Corrective action message	Timestamp	Severity
The execution for Corrective Action CA1 successfully completed.	May 14, 2014 7:5...	⚠
Execution created for Corrective Action CA1	May 14, 2014 7:5...	⚠

The Corrective Action Execution page now appears, which displays the output of the corrective action, status, start time, end time, and so forth.

- All Metrics method

1. From the target's home page, select **Monitoring**, then **All Metrics**.
2. From the tree panel on the left, click the desired metric name.

   A row for the metric alert now appears in the Metric Alert History table.
3. Click the glasses icon in the Details column as shown below.



slc04zbk.us.oracle.com

Page Refreshed May 14, 2014 9:23:13 PM GMT

slc04zbk.us.oracle.com > All Metrics

All Metrics

Search

View Data: Last 24 Hours

Auto Refresh: Off

CPU Utilization (%)

Statistics

Last Known Value 87.62
Collection Timestamp May 14, 2014 9:20:51 PM GMT
Average Value 40.67
Low Value 1.95
High Value 94.61

Thresholds

Warning/Critical 1/95
Comparison Operator >
Occurrences Before Alert 1
Corrective Actions Warning Only
Thresholds last modified by Template host_template was applied by SBAMBORE1 on May 14, 201

Metric Value History

Metric Alert History

ıp	Message	Last Comment	Details
2014 4:27:55 AM G...	CPU Utilization is 3.22%, crossed warning (1) or critical (95) threshold.	The execution for Corrective Action CA1 aborted.	👓

https://linuxcs2.us.oracle.com/em/faces/core-event-console?_adf.ctrl-state=1dezgaj...

The Incident Manager Event Details page now appears.

4. In the Corrective Action History table at the bottom of the page, select the message in the history table, then click the glasses icon.

   The Corrective Action Execution page now appears, which displays the output of the corrective action, status, start time, end time, and so forth.

Part II

Administering Cloud Control

This section contains the following chapters:

12

Maintaining Enterprise Manager

Enterprise Manager provides extensive monitoring and management capabilities for various Oracle and non-Oracle products. Used to manage your heterogeneous IT infrastructure, Enterprise Manager plays an integral role in monitoring and maintaining the health of your IT resources. It is therefore essential to ensure Enterprise Manager itself is operating at peak efficiency.

To help you maintain your Enterprise Manager installation, a variety of enhanced self-monitoring and diagnostic functionality is available from the Enterprise Manager console. These functions are designed to help you understand and monitor various components of Enterprise Manger, monitor/measure the quality of services Enterprise Manager provides, diagnose failures quickly, and manage Agents more easily.

This chapter covers the following topics:

- Overview: Managing the Manager
- Health Overview
- Repository
- Controlling and Configuring Management Agents
- Management Servers

12.1 Overview: Managing the Manager

Although Enterprise Manager functions as a single entity to manage your IT infrastructure, in reality it is composed of multiple components working in concert to provide a complete management framework from a functional standpoint. All major components of Enterprise Manager have been grouped into a single system. A special set of services has been created (based on the system) to model Enterprise Manager functions.

Management Features

- Topology view that allows you to see all major components of Enterprise Manager and their current status.
- Dashboard displaying the overall health of Enterprise Manager.
- Full control of the Agent directly from the Enterprise Manager console. Functions include:
  - View/edit Agent configuration properties.
  - View Agent(s) configuration history and compare the results against other Agents.

- Perform Agent control operations (start/stop/secure).
- Upgrade Management Agents

12.2 Health Overview

The Health Overview provides a comprehensive overview of OMS and Repository operation and performance, and therefore allows you to view the overall health of your Enteprise Manager environment.

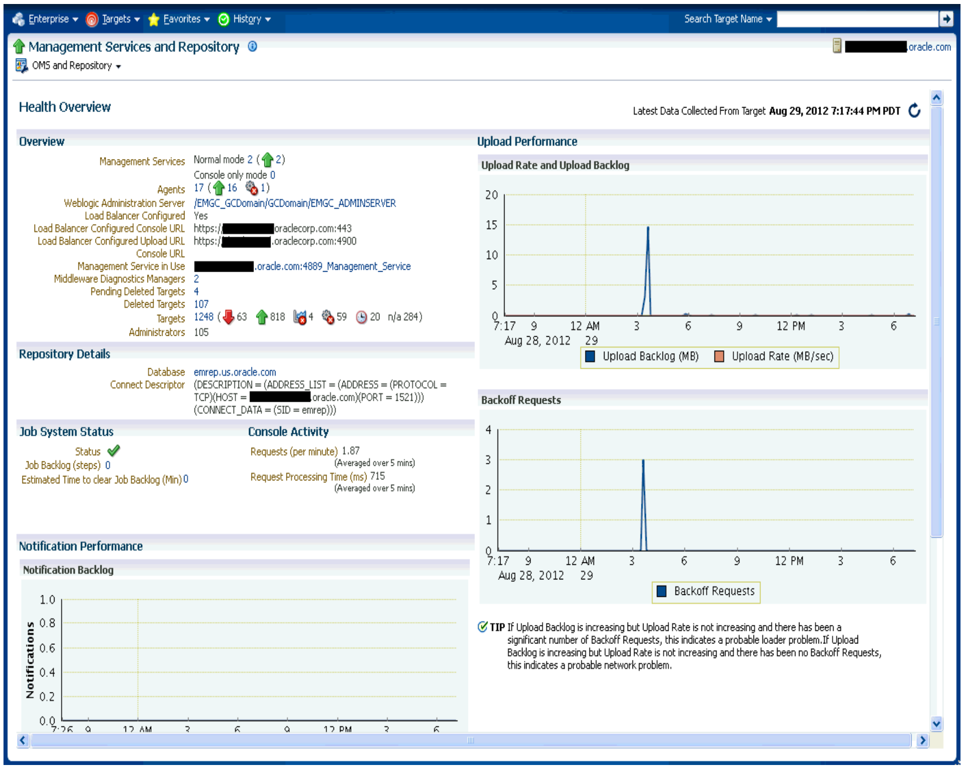
Accessing the Health Overview

From the **Setup** menu, select **Manage Cloud Control** and then **Health Overview**.

All major areas of Enterprise Manager are represented.

- **Overview**: Provides key information for active Management Services such as the Management Agents, the WebLogic Administration Server, total number of monitored targets, number of administrators, and server load balancer (SLB) upload and console URLs, provided SLB is configured. If configured, the SLB upload and console URLs are also displayed.
- **Repository Details**: Provides physical information about the Management Repository and the host on which the database is located. You can drill down into the database home page for more information and carry out administrative operations.
- **Job System Status:** Displays key operational parameters of the Enterprise Manager Job service. For detailed information, you can click on the status icon to drill down into the Enterprise Manager Job Service home page.
- **Console Activity:** Displays the overall load on the Enterprise Manager console through the average number of requests per minute and the average time required to process those requests.
- **Alerts**: Provides details on the metric errors recorded and when an alert was triggered. In-context links to Incident Manager are also provided.
- **Performance Charts**: Upload Backlog and Upload Rate, Backoff Requests, Notification backlog. You can drill down into any chart to view detailed metric information.

Figure 12–1 Health Overview Page



Latest Data Collected From Target **Aug 29, 2012 7:17:44 PM PDT**

Overview

Management Services	Normal mode 2 (2) Console only mode 0
Agents	17 (16 1)
Weblogic Administration Server	/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER
Load Balancer Configured	Yes
Load Balancer Configured Console URL	https://[redacted]oraclecorp.com:443
Load Balancer Configured Upload URL	https://[redacted].oraclecorp.com:4900
Console URL	
Management Service in Use	[redacted].oracle.com:4889_Management_Service
Middleware Diagnostics Managers	2
Pending Deleted Targets	4
Deleted Targets	107
Targets	1248 (63 818 4 59 20 n/a 284)
Administrators	105

Repository Details

Database	emrep.us.oracle.com
Connect Descriptor	(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = [redacted].oracle.com)(PORT = 1521))) (CONNECT_DATA = (SID = emrep)))

Job System Status

Status	✓
Job Backlog (steps)	0
Estimated Time to clear Job Backlog (Min)	0

Console Activity

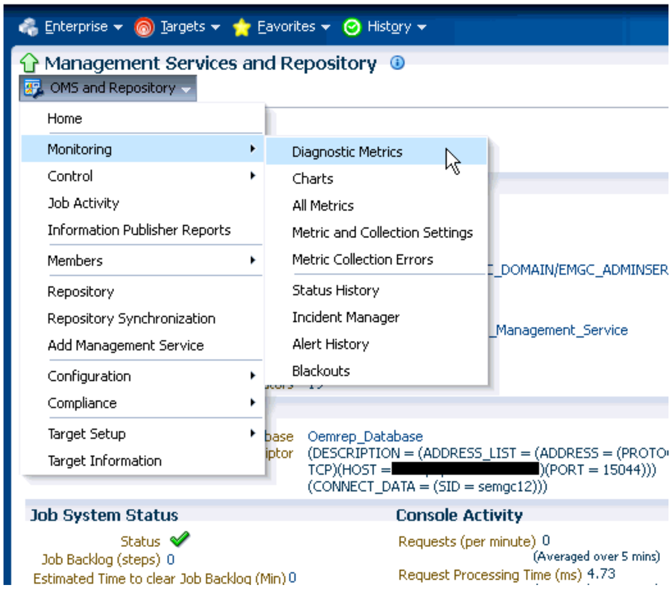
Requests (per minute)	1.87 (Averaged over 5 mins)
Request Processing Time (ms)	715 (Averaged over 5 mins)

✓ **TIP** If Upload Backlog is increasing but Upload Rate is not increasing and there has been a significant number of Backoff Requests, this indicates a probable loader problem.If Upload Backlog is increasing but Upload Rate is not increasing and there has been no Backoff Requests, this indicates a probable network problem.

From this page, you can carry out all monitoring and management operations using the **OMS and Repository** menu.

Note: The Diagnostic Metrics page is intended for use by Oracle Support when diagnosing issues with the OMS. The page can be accessed by selecting **Monitoring** and then **Diagnostic Metrics** from the **OMS and Repository** menu.

Figure 12–2 OMS and Repository Menu



_DOMAIN/EMGC_ADMINSER

_Management_Service

base Oemrep_Database
iptor (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTO
TCP)(HOST = [redacted])(PORT = 15044)))
(CONNECT_DATA = (SID = semgc12)))

Status ✓
Job Backlog (steps) 0
Estimated Time to clear Job Backlog (Min) 0

Requests (per minute) 0
(Averaged over 5 mins)
Request Processing Time (ms) 4.73

12.2.1 Viewing Enterprise Manager Topology and Charts

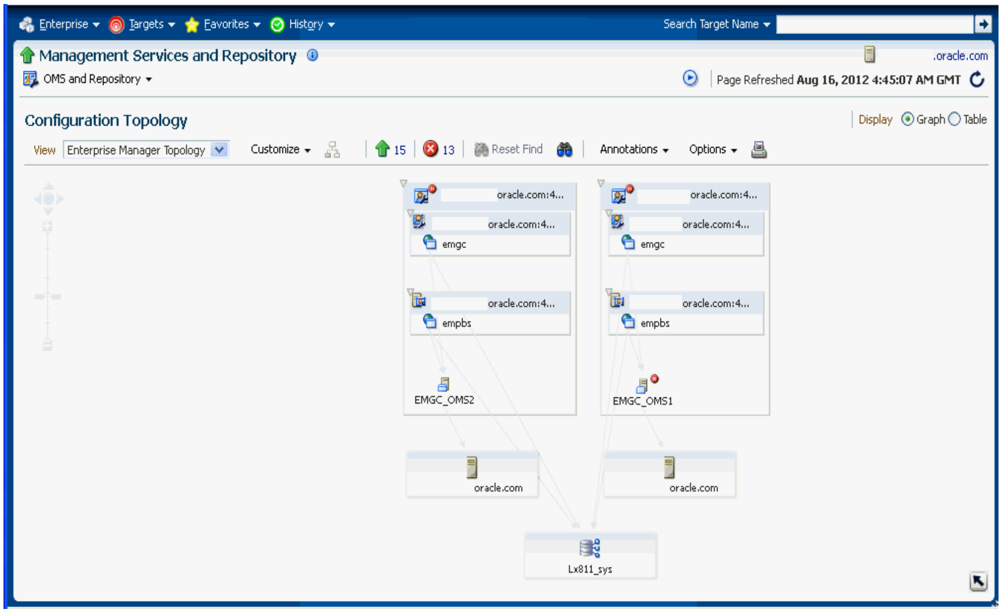
The Enterprise Manager Topology page provides a graphical representation of the Enterprise Manager infrastructure components and their association. Each node in the hierarchy displays key information about the member type, the host on which it resides, and the number of incidents, if any. The incident icons on each of the nodes expand to display a global view of current status for each node in the hierarchy.

Note: In order for the Enterprise Manager repository database to appear in the Topology page, you must first manually discover the database. Manual discovery is also required in order to have the database's metric data (Database Time (centiseconds per second)) displayed in the charts.

Accessing the Enterprise Manager Topology

1. From the Setup menu, select **Manage Cloud Control** and then **Health Overview**.
2. Click on the **OMS and Repository** menu to display available operations that can be performed from this page.
3. Select **Members** and then **Topology**.

Figure 12–3 Enterprise Manager Topology



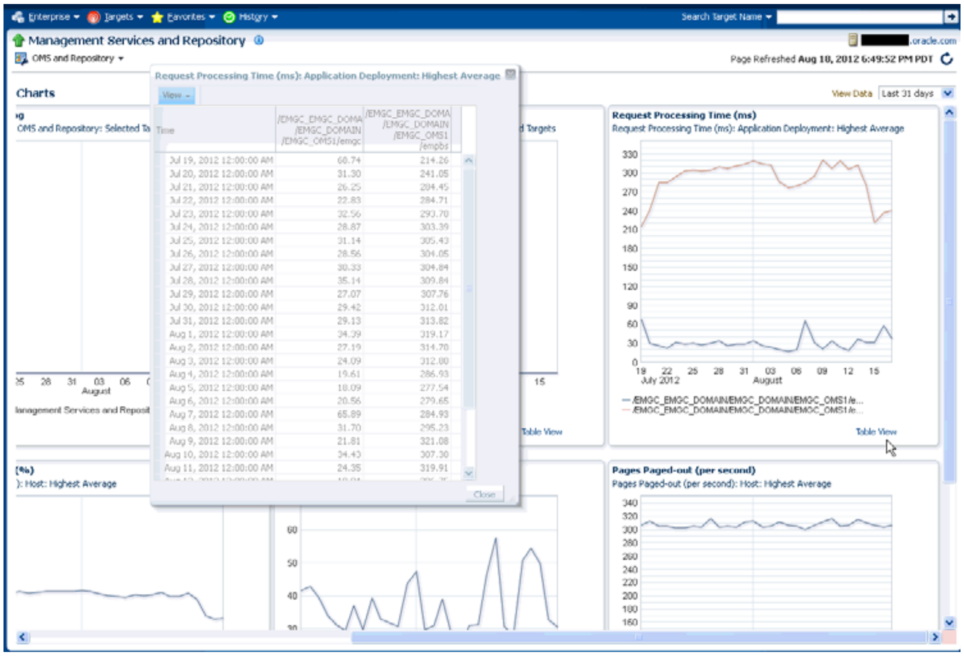
Enterprise Manager Charts

The Enterprise Manager Charts page displays eight charts representing key areas that together indicate the overall health of Enterprise Manager. These are Overall Files Pending Load -Agent, Job Step Backlog, Job Step Throughput (per second), Request Processing Time (ms), Database Time (centiseconds per second), CPU Utilization (%), Pages Paged-in (per second), Pages Paged-out (per second). Data can be viewed for the Last 24 hours, last 7 days or last 31 days.

Accessing the Enterprise Manager Charts

1. From the Setup menu, select **Manage Cloud Control and then Health Overview**.
2. Click on the **OMS and Repository** menu to display available operations that can be performed from this page.
3. Select **Monitoring** and then **Charts**.

Figure 12–4 Enterprise Manager Charts


Enterprise
Targets
Favorites
History
Search Target Name
Management Services and Repository
[redacted].oracle.com
OMS and Repository
Page Refreshed Aug 18, 2012 6:49:52 PM PDT
Charts
View Data
Last 31 days
Request Processing Time (ms)
Request Processing Time (ms): Application Deployment: Highest Average
July 2012
August
Table View
Pages Paged-out (per second)
Pages Paged-out (per second): Host: Highest Average
View
Close

Request Processing Time (ms): Application Deployment: Highest Average

Time	/EMGC_EMGC_DOMA /EMGC_DOMAIN /EMGC_OMS1/emgc	/EMGC_EMGC_DOMA /EMGC_DOMAIN /EMGC_OMS1 /empbs
Jul 19, 2012 12:00:00 AM	60.74	214.26
Jul 20, 2012 12:00:00 AM	31.30	241.05
Jul 21, 2012 12:00:00 AM	26.25	284.45
Jul 22, 2012 12:00:00 AM	22.83	284.71
Jul 23, 2012 12:00:00 AM	32.56	293.70
Jul 24, 2012 12:00:00 AM	28.87	303.39
Jul 25, 2012 12:00:00 AM	31.14	305.43
Jul 26, 2012 12:00:00 AM	28.56	304.05
Jul 27, 2012 12:00:00 AM	30.33	304.84
Jul 28, 2012 12:00:00 AM	35.14	309.84
Jul 29, 2012 12:00:00 AM	27.07	307.76
Jul 30, 2012 12:00:00 AM	29.42	312.01
Jul 31, 2012 12:00:00 AM	29.13	313.82
Aug 1, 2012 12:00:00 AM	34.39	319.17
Aug 2, 2012 12:00:00 AM	27.19	314.70
Aug 3, 2012 12:00:00 AM	24.09	312.00
Aug 4, 2012 12:00:00 AM	19.61	286.93
Aug 5, 2012 12:00:00 AM	18.09	277.54
Aug 6, 2012 12:00:00 AM	20.56	279.65
Aug 7, 2012 12:00:00 AM	65.89	284.93
Aug 8, 2012 12:00:00 AM	31.70	295.23
Aug 9, 2012 12:00:00 AM	21.81	321.08
Aug 10, 2012 12:00:00 AM	34.43	307.30
Aug 11, 2012 12:00:00 AM	24.35	319.91

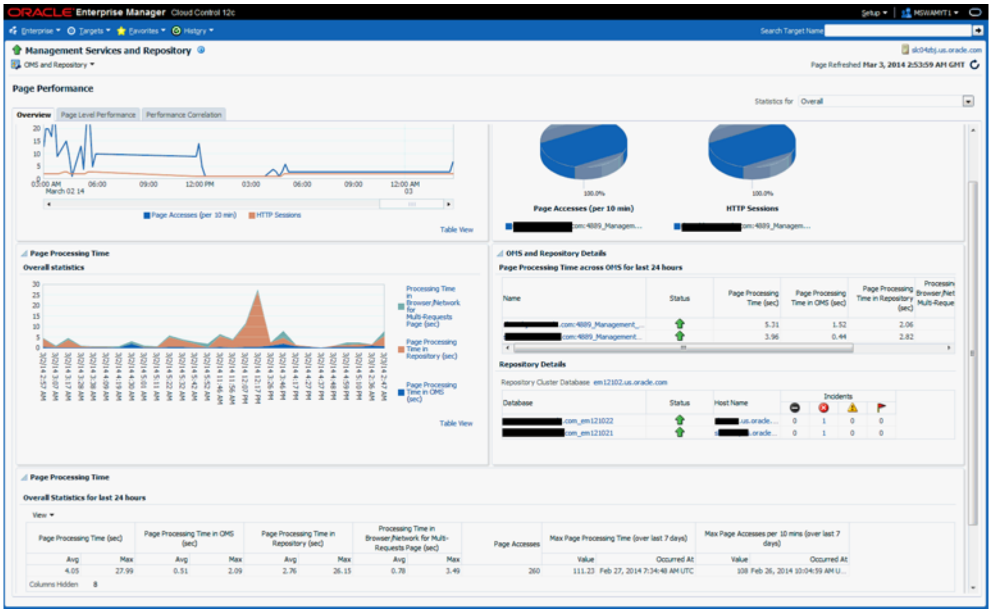
12.2.2 Determining Enterprise Manager Page Performance

Page Performance Monitoring and diagnosis feature provides you with the ability to identify and diagnose performance issues with Enterprise Manager pages without having to contact Oracle support.

> **Important:** The Enterprise Manager page performance tracing feature requires Agent version 12.1.0.4 or later.
>
> The charts and tables in this page will display data only if the Agent that is monitoring Management Services and Repository target is version 12.1.0.4 or later. If you have upgraded Enterprise Manager 12.1.0.4, you should also upgrade the Agents on Management Service (OMS) machines to 12.1.0.4 in order to access the latest monitoring capabilities for the Management Services and Repository, as well as related targets.
>
> See the Oracle® Enterprise Manager Cloud Control Upgrade Guide for more information on upgrading Agents.

To access Page Performance Monitoring and Diagnosis functionality:

1. From the **Setup** menu, select **Manage Cloud Control**, and then **Health Overview** or **Repository**.
2. From the **OMS and Repository** menu, select **Monitoring** and then **Page Performance**. The Page Performance page displays.



Management Services and Repository

OMS and Repository ▾

slc04zbj.us.oracle.com

Page Refreshed **Mar 3, 2014 2:53:59 AM GMT**

Page Performance

Statistics for Overall

Overview | Page Level Performance | Performance Correlation

Page Accesses (per 10 min)

■ [redacted]com:4889_Managem...

HTTP Sessions

■ [redacted]com:4889_Managem...

Page Processing Time

Overall statistics

OMS and Repository Details

Page Processing Time across OMS for last 24 hours

Name	Status	Page Processing Time (sec)	Page Processing Time in OMS (sec)	Page Processing Time in Repository (sec)	Processin Browser/Net Multi-Reque
[redacted].com:4889_Management_...	⬆	5.31	1.52	2.06	
[redacted]com:4889_Management...	⬆	3.96	0.44	2.82	

Repository Details

Repository Cluster Database em12102.us.oracle.com

Database	Status	Host Name	Incidents			
			⊖	⊗	⚠	🚩
[redacted].com_em121022	⬆	[redacted].us.oracle....	0	1	0	0
[redacted]com_em121021	⬆	s[redacted].oracle...	0	1	0	0

Page Processing Time

Overall Statistics for last 24 hours

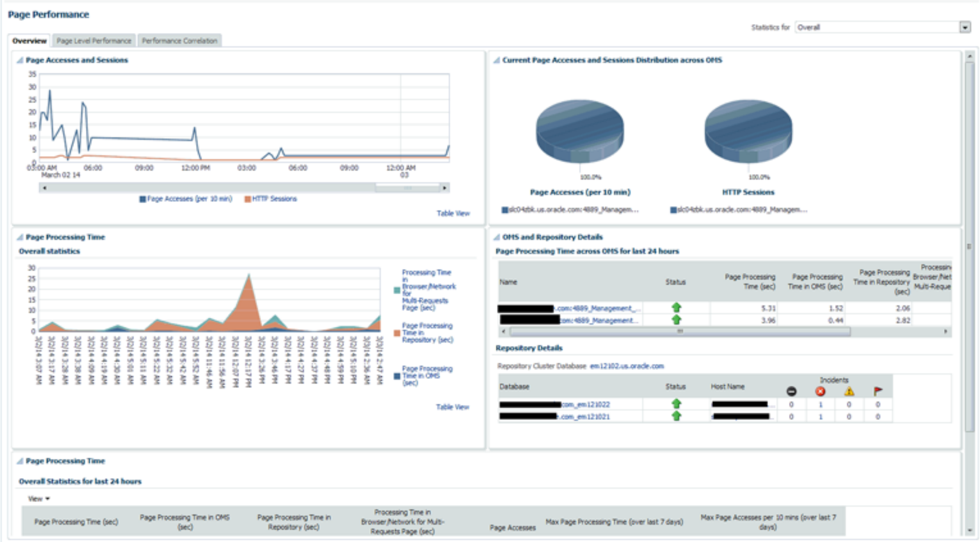
View ▾

Page Processing Time (sec)		Page Processing Time in OMS (sec)		Page Processing Time in Repository (sec)		Processing Time in Browser/Network for Multi-Requests Page (sec)		Page Accesses	Max Page Processing Time (over last 7 days)		Max Page Accesses per 10 mins (over last 7 days)	
Avg	Max	Avg	Max	Avg	Max	Avg	Max		Value	Occurred At	Value	Occurred At
4.05	27.99	0.51	2.09	2.76	26.15	0.78	3.49	260	111.23	Feb 27, 2014 7:34:48 AM UTC	108	Feb 26, 2014 10:04:59 AM U...

Columns Hidden 8

Overview

The overview tab provides details of the overall page performance in Enterprise Manager.



35
30
25
20
15
10
5
0
03:00 AM
March 02 14
06:00
09:00
12:00 PM
03:00
06:00
09:00
12:00 AM
03
■ Page Accesses (per 10 min)
■ HTTP Sessions
Table View
100.0%
100.0%
30
25
20
15
10
5
0
■ Processing Time in Browser/Network for Multi-Requests Page (sec)
■ Page Processing Time in Repository (sec)
■ Page Processing Time in OMS (sec)
Table View

Page Performance

Statistics for Overall

Overview | Page Level Performance | Performance Correlation

Page Accesses and Sessions

Current Page Accesses and Sessions Distribution across OMS

Page Accesses (per 10 min)

■ slc04zbk.us.oracle.com:4889_Managem...

HTTP Sessions

■ slc04zbk.us.oracle.com:4889_Managem...

Page Processing Time

Overall statistics

OMS and Repository Details

Page Processing Time across OMS for last 24 hours

Name	Status	Page Processing Time (sec)	Page Processing Time in OMS (sec)	Page Processing Time in Repository (sec)	Processin Browser/Net Multi-Reque
[redacted].com:4889_Management_...	⬆	5.31	1.52	2.06	
[redacted]com:4889_Management...	⬆	3.96	0.44	2.82	

Repository Details

Repository Cluster Database em12102.us.oracle.com

Database	Status	Host Name	Incidents			
			⊖	⊗	⚠	🚩
[redacted]com_em121022	⬆	[redacted]	0	1	0	0
[redacted].com_em121021	⬆	s[redacted]	0	1	0	0

Page Processing Time

Overall Statistics for last 24 hours

View ▾

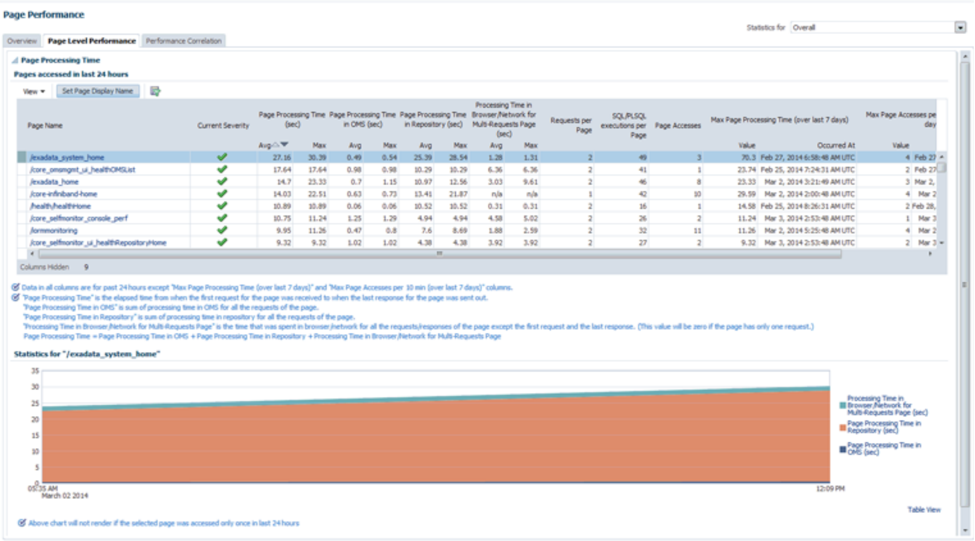
Page Processing Time (sec)	Page Processing Time in OMS (sec)	Page Processing Time in Repository (sec)	Processing Time in Browser/Network for Multi-Requests Page (sec)	Page Accesses	Max Page Processing Time (over last 7 days)	Max Page Accesses per 10 mins (over last 7 days)

The charts display the Page Accesses and Sessions, Current Page Accesses and Sessions Distribution across OMSs and the Overall Statistics of page performance in the last 24 hours. There are details of the page performance in each of the OMSs as well as the details of the available repositories.

The Overall Statistics table provides the breakdown of times spent in the Repository, the OMS and network and the number of page accesses, the maximum time taken by page in the last 24 hours.

Page Level Performance

The page level performance tab shows the list of pages accessed in the last 24 hours.



Pages accessed in last 24 hours

Page Name	Current Severity	Page Processing Time (sec)		Page Processing Time in OMS (sec)		Page Processing Time in Repository (sec)		Processing Time in Browser/Network for Multi-Requests Page (sec)		Requests per Page	SQL/PLSQL executions per Page	Page Accesses	Max Page Processing Time (over last 7 days)		Max Page Accesses pe day	
		Avg	Max	Avg	Max	Avg	Max	Avg	Max				Value	Occurred At	Value	
/exadata_system_home	✓	27.16	30.39	0.49	0.54	25.39	28.54	1.28	1.31	2	49	3	70.3	Feb 27, 2014 6:58:48 AM UTC	4	Feb 27
/core_omsmgmt_ui_healthOMSList	✓	17.64	17.64	0.98	0.98	10.29	10.29	6.36	6.36	2	41	1	23.74	Feb 25, 2014 7:24:31 AM UTC	2	Feb 27
/exadata_home	✓	14.7	23.33	0.7	1.15	10.97	12.56	3.03	9.61	2	46	8	23.33	Mar 2, 2014 3:21:49 AM UTC	3	Mar 2,
/core-infiniband-home	✓	14.03	22.51	0.63	0.73	13.41	21.87	n/a	n/a	1	42	10	29.59	Mar 2, 2014 2:00:48 AM UTC	4	Mar 2
/health/healthHome	✓	10.89	10.89	0.06	0.06	10.52	10.52	0.31	0.31	2	16	1	14.58	Feb 25, 2014 8:26:31 AM UTC	2	Feb 28,
/core_selfmonitor_console_perf	✓	10.75	11.24	1.25	1.29	4.94	4.94	4.58	5.02	2	26	2	11.24	Mar 3, 2014 2:53:48 AM UTC	1	Mar 3
/ommonitoring	✓	9.95	11.26	0.47	0.8	7.6	8.69	1.88	2.59	2	32	11	11.26	Mar 2, 2014 5:25:48 AM UTC	4	Mar 2
/core_selfmonitor_ui_healthRepositoryHome	✓	9.32	9.32	1.02	1.02	4.38	4.38	3.92	3.92	2	27	2	9.32	Mar 3, 2014 2:53:48 AM UTC	2	Mar 3

Data in all columns are for past 24 hours except "Max Page Processing Time (over last 7 days)" and "Max Page Accesses per 10 min (over last 7 days)" columns.

"Page Processing Time" is the elapsed time from when the first request for the page was received to when the last response for the page was sent out.
"Page Processing Time in OMS" is sum of processing time in OMS for all the requests of the page.
"Page Processing Time in Repository" is sum of processing time in repository for all the requests of the page.
"Processing Time in Browser/Network for Multi-Requests Page" is the time that was spent in browser/network for all the requests/responses of the page except the first request and the last response. (This value will be zero if the page has only one request.)
Page Processing Time = Page Processing Time in OMS + Page Processing Time in Repository + Processing Time in Browser/Network for Multi-Requests Page

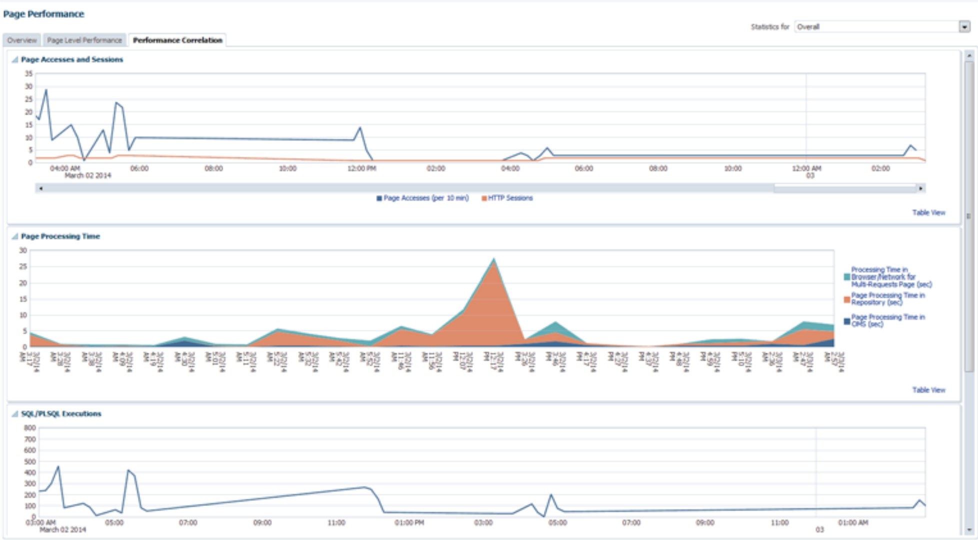
Statistics for "/exadata_system_home"

Above chart will not render if the selected page was accessed only once in last 24 hours

The page also displays the breakdown of time spent in the Repository and the OMS and network in a line graph format for each page.

Performance Correlation

The performance correlation tab displays graphs for page performance that allow you to correlate performance trends.

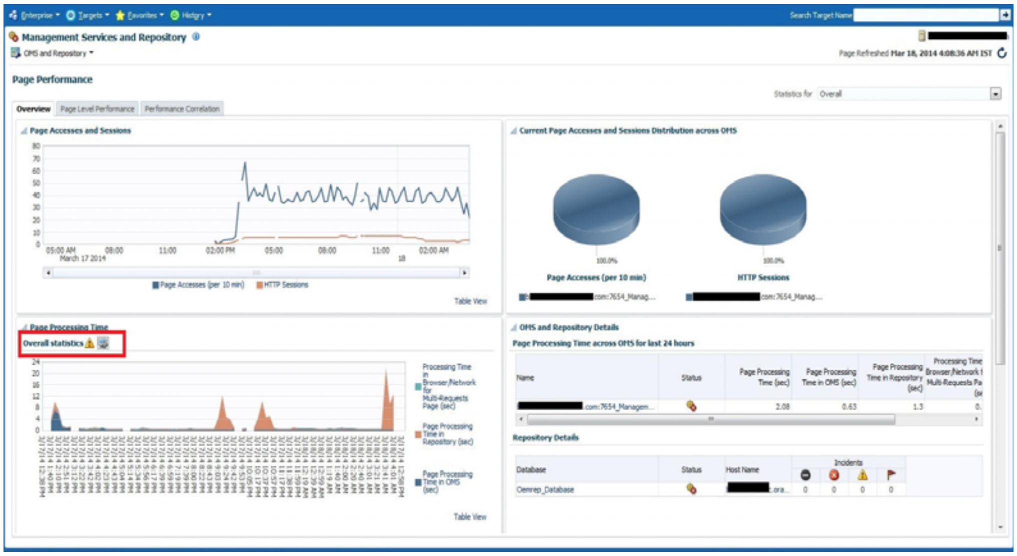


This tab provides details of page accesses and sessions, page processing time, SQL/PLSQL executions, and average active sessions.

Symptom Diagnosis

Symptom diagnosis can be performed for both overall page processing time and individual page times. Symptom diagnosis is triggered when the set metric thresholds for overall page processing time are exceeded. Diagnosis is accessed by means of an icon in the Overview tab in the Overall Statistics section when the overall page performance threshold is exceeded, as shown in the following graphic.

Figure 12–5 Symptom Diagnosis Icon


Enterprise ▾
Targets ▾
Favorites ▾
History ▾
Search Target Name
Management Services and Repository
OMS and Repository ▾
Page Refreshed Mar 18, 2014 4:08:36 AM IST
Page Performance
Statistics for Overall
Overview
Page Level Performance
Performance Correlation
Page Accesses and Sessions
80
70
60
50
40
30
20
10
0
05:00 AM March 17 2014
08:00
11:00
02:00 PM
05:00
08:00
11:00 18
02:00 AM
Page Accesses (per 10 min)
HTTP Sessions
Table View
Current Page Accesses and Sessions Distribution across OMS
100.0%
Page Accesses (per 10 min)
100.0%
HTTP Sessions
[redacted] com:7654_Manag...
[redacted] com:7654_Manag...
Page Processing Time
Overall statistics
24
20
16
12
8
4
0
Processing Time in Browser/Network for Multi-Requests Page (sec)
Page Processing Time in Repository (sec)
Page Processing Time in OMS (sec)
Table View
OMS and Repository Details

Page Processing Time across OMS for last 24 hours

Name	Status	Page Processing Time (sec)	Page Processing Time in OMS (sec)	Page Processing Time in Repository (sec)	Processing Time Browser/Network f Multi-Requests Pa (se
[redacted] .com:7654_Managem...		2.08	0.63	1.3	0.

Repository Details

Database	Status	Host Name	Incidents			
			⊖	⊗	⚠	⚑
Oemrep_Database		[redacted] .ora...	0	0	0	0

For individual pages, the symptom diagnosis icon is displayed in the table in the Current Severity column if the page performance metric threshold is exceeded.

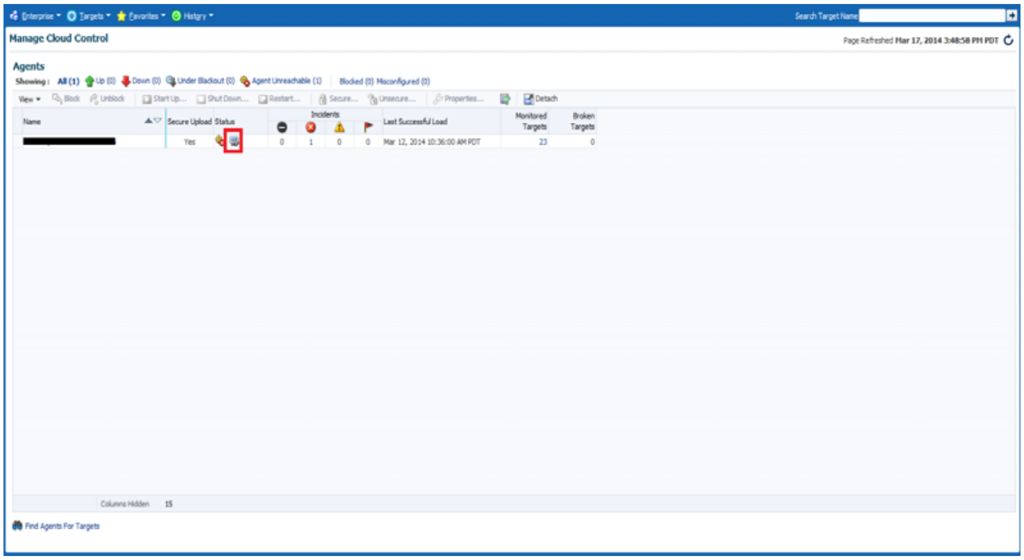
When the icon is displayed in the Overall Statistics section, it indicates that the overall performance of the Enterprise Manager pages has exceeded the threshold in the last 10 minutes. Clicking on the icon, you are taken to another tab where the details of the diagnosis are presented. The diagnosis indicates the root cause for the overall page performance exceeding the metric threshold, the findings that were deduced on diagnosis and the checks that were performed to analyze the overall page performance issue.

The checks are performed at the database level, middle-tier level and the browser/network level to isolate which part of the system might be the cause of the issue. Each check is analyzed and the checks that are identified as the top causes are reported as findings. The topmost finding is then reported as the root cause for the performance issue.

Target Availability Symptom Diagnosis:

Symptom diagnosis can be performed on the availability of the Agent as well. The icon is displayed in the Agent List and Agent Home pages in the event that the Agent target is unreachable or in pending status.

Figure 12–6 Agent List Page



Manage Cloud Control

Page Refreshed **Mar 17, 2014 3:48:58 PM PDT**

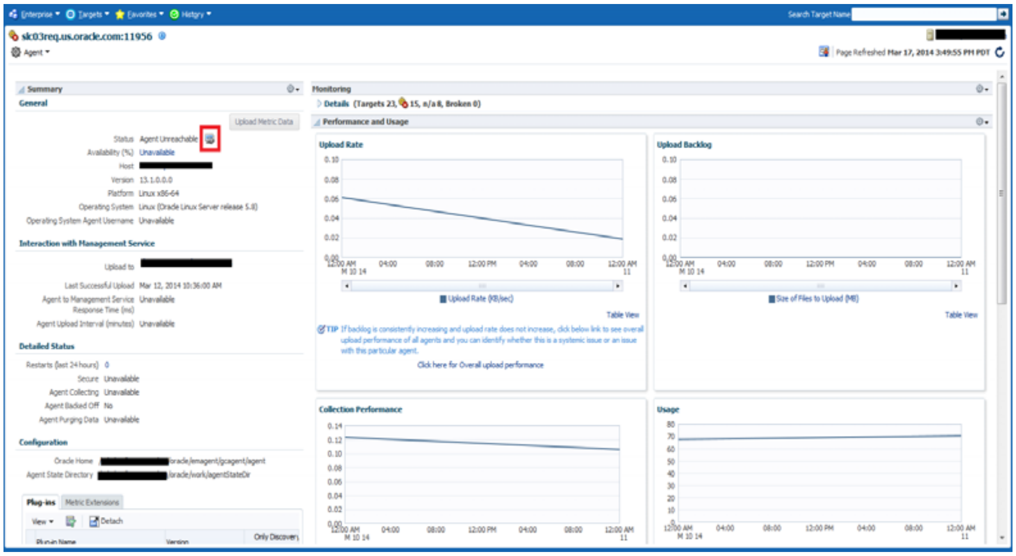
Agents

Showing : All (1) Up (0) Down (0) Under Blackout (0) Agent Unreachable (1) Blocked (0) Misconfigured (0)

Name	Secure Upload	Status	Incidents ⛔	Incidents ✖	Incidents ⚠	Incidents 🚩	Last Successful Load	Monitored Targets	Broken Targets
[redacted]	Yes		0	1	0	0	Mar 12, 2014 10:36:00 AM PDT	23	0

Columns Hidden 15

Figure 12–7 Agent Home Page



sk03req.us.oracle.com:11956

[redacted]

Page Refreshed **Mar 17, 2014 3:49:55 PM PDT**

General

Status Agent Unreachable
Availability (%) Unavailable
Host [redacted]
Version 13.1.0.0.0
Platform Linux x86-64
Operating System Linux (Oracle Linux Server release 5.8)
Operating System Agent Username Unavailable

Interaction with Management Service

Upload to [redacted]
Last Successful Upload Mar 12, 2014 10:36:00 AM
Agent to Management Service Response Time (ms) Unavailable
Agent Upload Interval (minutes) Unavailable

Detailed Status

Restarts (last 24 hours) 0
Secure Unavailable
Agent Collecting Unavailable
Agent Backed Off No
Agent Purging Data Unavailable

Configuration

Oracle Home [redacted]/oracle/emagent/gcagent/agent
Agent State Directory [redacted]/oracle/work/agentStateDir

Details (Targets 23, 15, n/a 8, Broken 0)

TIP If backlog is consistently increasing and upload rate does not increase, click below link to see overall upload performance of all agents and you can identify whether this is a systemic issue or an issue with this particular agent.

Click here for Overall upload performance

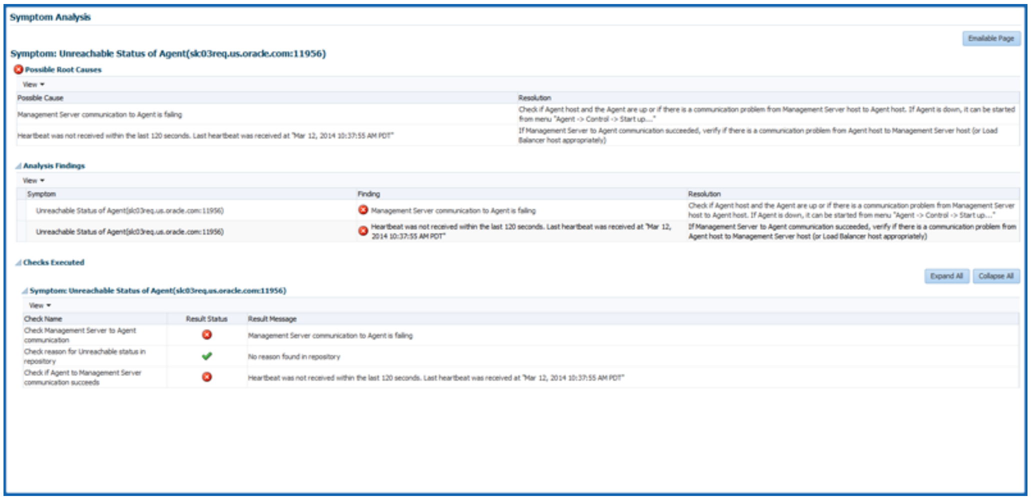
On clicking the icon, the user is navigated to another tab where the details of the diagnosis are presented. The diagnosis indicates the root cause for the Agent's unreachable/pending state, the findings that were deduced from the diagnosis and the checks that were performed to analyze the Agent availability issue.

The checks performed to diagnose the issue consist of the following:

- if the communication between the Management Service and the Agent is successful
- if the Agent has communicated with the Management Service
- if reasons can be deduced from the Repository
- if further reasons can be deduced by performing checks from the Agent side (whether communication between the OMS and the Agent exists).

Each check is analyzed and the checks that are identified as the top causes are reported as findings. The topmost finding is then reported as the root cause for the performance issue.

Figure 12–8 Agent Symptom Diagnosis



Symptom Analysis

Emailable Page

Symptom: Unreachable Status of Agent(slc03req.us.oracle.com:11956)

✗ Possible Root Causes

View ▾

Possible Cause	Resolution
Management Server communication to Agent is failing	Check if Agent host and the Agent are up or if there is a communication problem from Management Server host to Agent host. If Agent is down, it can be started from menu "Agent -> Control -> Start up..."
Heartbeat was not received within the last 120 seconds. Last heartbeat was received at "Mar 12, 2014 10:37:55 AM PDT"	If Management Server to Agent communication succeeded, verify if there is a communication problem from Agent host to Management Server host (or Load Balancer host appropriately)

Analysis Findings

View ▾

Symptom	Finding	Resolution
Unreachable Status of Agent(slc03req.us.oracle.com:11956)	✗ Management Server communication to Agent is failing	Check if Agent host and the Agent are up or if there is a communication problem from Management Server host to Agent host. If Agent is down, it can be started from menu "Agent -> Control -> Start up..."
Unreachable Status of Agent(slc03req.us.oracle.com:11956)	✗ Heartbeat was not received within the last 120 seconds. Last heartbeat was received at "Mar 12, 2014 10:37:55 AM PDT"	If Management Server to Agent communication succeeded, verify if there is a communication problem from Agent host to Management Server host (or Load Balancer host appropriately)

Checks Executed

Expand All | Collapse All

Symptom: Unreachable Status of Agent(slc03req.us.oracle.com:11956)

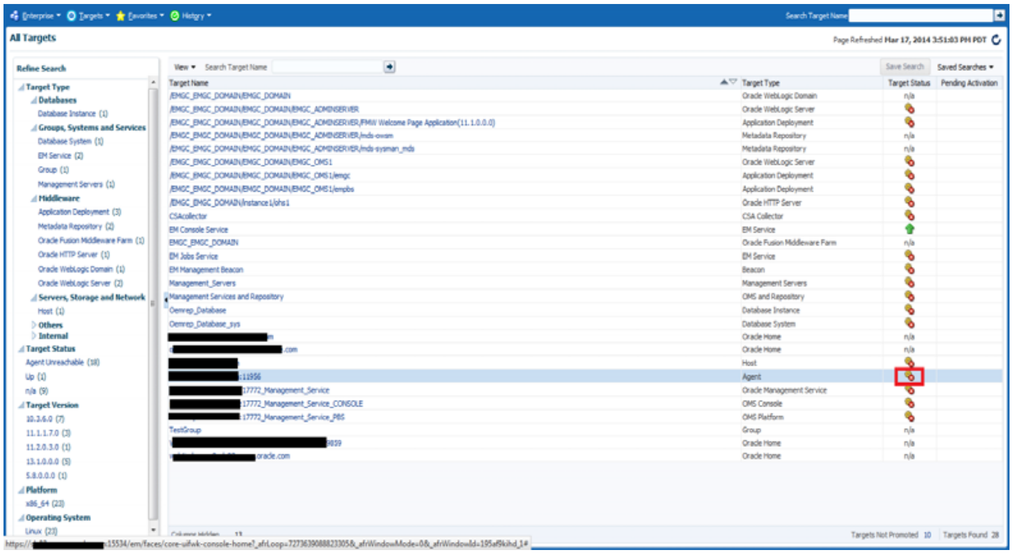
View ▾

Check Name	Result Status	Result Message
Check Management Server to Agent communication	✗	Management Server communication to Agent is failing
Check reason for Unreachable status in repository	✓	No reason found in repository
Check if Agent to Management Server communication succeeds	✗	Heartbeat was not received within the last 120 seconds. Last heartbeat was received at "Mar 12, 2014 10:37:55 AM PDT"

Note: If communication between the OMS and Agent cannot be established, then the diagnosis will report findings based on the data available in Management Repository, which may not be the real cause for the issue.

The symptom diagnosis feature is also available in the All Targets page for targets in unreachable or pending status by clicking on the status icon.

Figure 12–9 All Targets Page



All Targets

Page Refreshed **Mar 17, 2014 3:51:03 PM PDT**

Refine Search

- Target Type
  - Databases
    - Database Instance (1)
  - Groups, Systems and Services
    - Database System (1)
    - EM Service (2)
    - Group (1)
    - Management Servers (1)
  - Middleware
    - Application Deployment (3)
    - Metadata Repository (2)
    - Oracle Fusion Middleware Farm (1)
    - Oracle HTTP Server (1)
    - Oracle WebLogic Domain (1)
    - Oracle WebLogic Server (2)
  - Servers, Storage and Network
    - Host (1)
  - Others
  - Internal
- Target Status
  - Agent Unreachable (18)
  - Up (1)
  - n/a (9)
- Target Version
  - 10.3.6.0 (7)
  - 11.1.1.7.0 (3)
  - 11.2.0.3.0 (1)
  - 13.1.0.0.0 (5)
  - 5.8.0.0.0 (1)
- Platform
  - x86_64 (23)
- Operating System
  - Linux (23)

View ▾ Search Target Name

Save Search | Saved Searches ▾

Target Name	Target Type	Target Status	Pending Activation
/EMGC_EMGC_DOMAIN/EMGC_DOMAIN	Oracle WebLogic Domain	n/a	
/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_ADMINSERVER	Oracle WebLogic Server	⊗	
/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_ADMINSERVER/FMW Welcome Page Application(11.1.0.0.0)	Application Deployment	⊗	
/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_ADMINSERVER/mds-owsm	Metadata Repository	n/a	
/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_ADMINSERVER/mds-sysman_mds	Metadata Repository	n/a	
/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_OMS1	Oracle WebLogic Server	⊗	
/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_OMS1/emgc	Application Deployment	⊗	
/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_OMS1/empbs	Application Deployment	⊗	
/EMGC_EMGC_DOMAIN/instance1/ohs1	Oracle HTTP Server	⊗	
CSAcollector	CSA Collector	⊗	
EM Console Service	EM Service	↑	
EMGC_EMGC_DOMAIN	Oracle Fusion Middleware Farm	n/a	
EM Jobs Service	EM Service	⊗	
EM Management Beacon	Beacon	⊗	
Management_Servers	Management Servers	⊗	
Management Services and Repository	OMS and Repository	⊗	
Oemrep_Database	Database Instance	⊗	
Oemrep_Database_sys	Database System	⊗	
[redacted]m	Oracle Home	n/a	
[redacted].com	Oracle Home	n/a	
[redacted]	Host	⊗	
[redacted]:11956	Agent	⊗	
[redacted]17772_Management_Service	Oracle Management Service	⊗	
[redacted]17772_Management_Service_CONSOLE	OMS Console	⊗	
[redacted]17772_Management_Service_PBS	OMS Platform	⊗	
TestGroup	Group	n/a	
[redacted]9059	Oracle Home	n/a	
[redacted]oracle.com	Oracle Home	n/a	

Columns Hidden 13 | Targets Not Promoted 10 | Targets Found 28

https://[redacted]:15534/em/faces/core-uifwk-console-home?_afrLoop=7273639088823305&_afrWindowMode=0&_afrWindowId=195af9kihd_1#

12.3 Repository

The Repository page provides you with an overview of the status and performance of the Repository DBMS Jobs that handle part of Enterprise Manager's maintenance and monitoring functionality. These DBMS jobs run within the Management Repository and require no user input. Charts showing the key Repository Details and Backlog in Repository Collection are provided The Scheduler Status region provides the status of the scheduler and the number of Job Queue Processes.

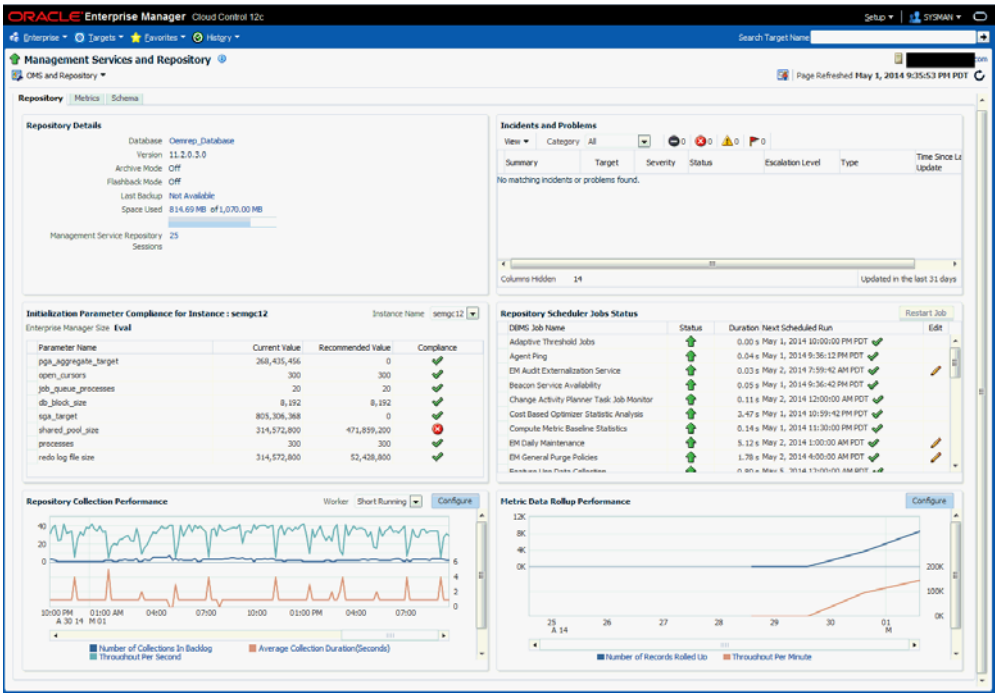
Accessing Repository Information

From the **Setup** menu, select **Manage Cloud Control** and then **Repository.**

Three tabs are displayed providing a comprehensive view of repository attributes, performance, as well as access to requisite operational parameters.

- Repository Tab
- Metrics Tab
- Schema Tab

Figure 12–10 Repository Page



Management Services and Repository

OMS and Repository ▾

[redacted]com

Page Refreshed **May 1, 2014 9:35:53 PM PDT**

Repository Details

Database Oemrep_Database
Version 11.2.0.3.0
Archive Mode Off
Flashback Mode Off
Last Backup Not Available
Space Used 814.69 MB of 1,070.00 MB
Management Service Repository Sessions 25

Incidents and Problems

View ▾ Category All ⊖0 ⊗0 ⚠0 ⚑0

Summary	Target	Severity	Status	Escalation Level	Type	Time Since Last Update

No matching incidents or problems found.

Columns Hidden 14 Updated in the last 31 days

Initialization Parameter Compliance for Instance : semgc12

Instance Name semgc12

Enterprise Manager Size **Eval**

Parameter Name	Current Value	Recommended Value	Compliance
pga_aggregate_target	268,435,456	0	✓
open_cursors	300	300	✓
job_queue_processes	20	20	✓
db_block_size	8,192	8,192	✓
sga_target	805,306,368	0	✓
shared_pool_size	314,572,800	471,859,200	⊗
processes	300	300	✓
redo log file size	314,572,800	52,428,800	✓

Repository Scheduler Jobs Status

Restart Job

DBMS Job Name	Status	Duration	Next Scheduled Run	Edit
Adaptive Threshold Jobs	⬆	0.00 s	May 1, 2014 10:00:00 PM PDT ✓	
Agent Ping	⬆	0.04 s	May 1, 2014 9:36:12 PM PDT ✓	
EM Audit Externalization Service	⬆	0.03 s	May 2, 2014 7:59:42 AM PDT ✓	✎
Beacon Service Availability	⬆	0.05 s	May 1, 2014 9:36:42 PM PDT ✓	
Change Activity Planner Task Job Monitor	⬆	0.11 s	May 2, 2014 12:00:00 AM PDT ✓	
Cost Based Optimizer Statistic Analysis	⬆	3.47 s	May 1, 2014 10:59:42 PM PDT ✓	
Compute Metric Baseline Statistics	⬆	0.14 s	May 1, 2014 11:30:00 PM PDT ✓	
EM Daily Maintenance	⬆	5.12 s	May 2, 2014 1:00:00 AM PDT ✓	✎
EM General Purge Policies	⬆	1.78 s	May 2, 2014 4:00:00 AM PDT ✓	✎
Feature Use Data Collection	⬆	0.80 s	May 5, 2014 12:00:00 AM PDT ✓	

Repository Collection Performance

Worker Short Running

Metric Data Rollup Performance

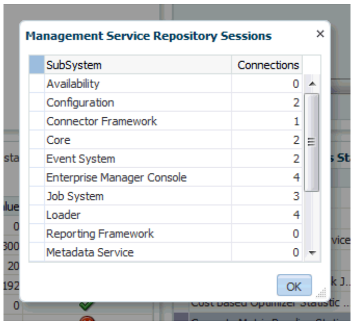
12.3.1 Repository Tab

As shown in Figure 12–10, the Repository tab provides a comprehensive snapshot of repository-specific monitoring.

Repository Details

The Repository Details region provides high-level database information for the Enterprise Manager repository. From this region, you can click on the number **Management Service Repository Sessions** details to view the exact number of repository connections per individual Enterprise Manager subcomponent such as the event system, console, job system, or connector framework.

Figure 12–11 Repository Sessions Per Subcomponent



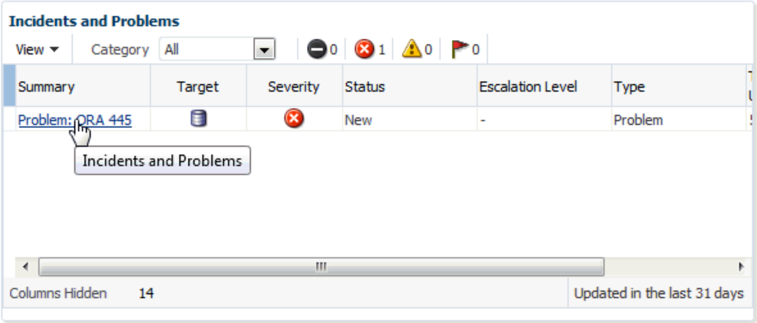
Management Service Repository Sessions

SubSystem	Connections
Availability	0
Configuration	2
Connector Framework	1
Core	2
Event System	2
Enterprise Manager Console	4
Job System	3
Loader	4
Reporting Framework	0
Metadata Service	0

Incidents and Problems

The Incidents and Problems region displays all incidents an problems associated with the repository database. For more detailed incident or problem information, you can click on the **Summary** link to access the issue in Incident Manager.

Figure 12–12 Accessing Incident/Problem Information



Incidents and Problems

View ▾ Category All ▾ ⊖ 0 ✖ 1 ⚠ 0 ⚑ 0

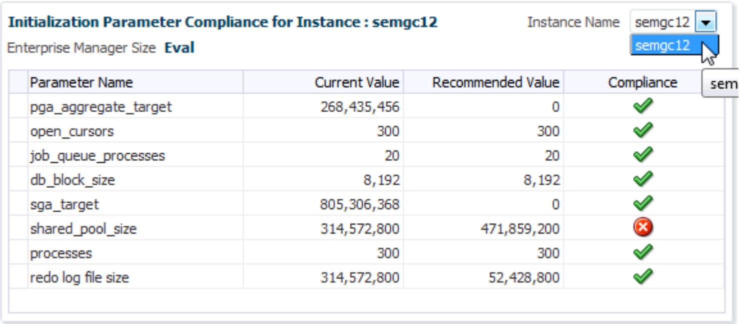
Summary	Target	Severity	Status	Escalation Level	Type
Problem: ORA 445	🛢	✖	New	-	Problem

Columns Hidden 14 Updated in the last 31 days

Initialization Parameter Compliance for Instance

This region displays the currents initialization parameter settings, recommended standards, and whether the current parameter values comply with those standard values.

Figure 12–13 Initialization Parameter Compliance



Initialization Parameter Compliance for Instance : semgc12

Instance Name semgc12

Enterprise Manager Size **Eval**

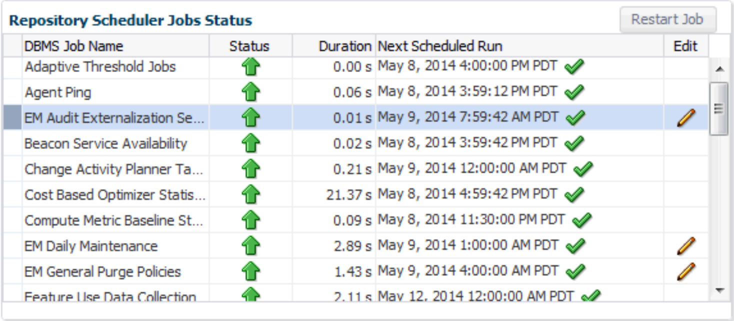
Parameter Name	Current Value	Recommended Value	Compliance
pga_aggregate_target	268,435,456	0	✓
open_cursors	300	300	✓
job_queue_processes	20	20	✓
db_block_size	8,192	8,192	✓
sga_target	805,306,368	0	✓
shared_pool_size	314,572,800	471,859,200	✖
processes	300	300	✓
redo log file size	314,572,800	52,428,800	✓

If you are running the repository in a RAC environment, this region also lets you select individual database instances in order to view initialization parameter compliance for that specific instance.

Repository Scheduler Job Status

The **Repository Scheduler Jobs Status** region provides details of the DBMS Jobs regarding their status, duration, and the next scheduled run time.

Figure 12–14 Repository Scheduler Job Status Region



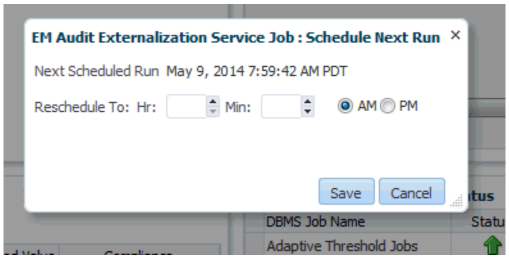
Repository Scheduler Jobs Status

DBMS Job Name	Status	Duration	Next Scheduled Run	Edit
Adaptive Threshold Jobs	⇧	0.00 s	May 8, 2014 4:00:00 PM PDT ✓	
Agent Ping	⇧	0.06 s	May 8, 2014 3:59:12 PM PDT ✓	
EM Audit Externalization Se...	⇧	0.01 s	May 9, 2014 7:59:42 AM PDT ✓	✎
Beacon Service Availability	⇧	0.02 s	May 8, 2014 3:59:42 PM PDT ✓	
Change Activity Planner Ta...	⇧	0.21 s	May 9, 2014 12:00:00 AM PDT ✓	
Cost Based Optimizer Statis...	⇧	21.37 s	May 8, 2014 4:59:42 PM PDT ✓	
Compute Metric Baseline St...	⇧	0.09 s	May 8, 2014 11:30:00 PM PDT ✓	
EM Daily Maintenance	⇧	2.89 s	May 9, 2014 1:00:00 AM PDT ✓	✎
EM General Purge Policies	⇧	1.43 s	May 9, 2014 4:00:00 AM PDT ✓	✎
Feature Use Data Collection	⇧	2.11 s	May 12, 2014 12:00:00 AM PDT ✓	

If the **Status** of a job is down, you can run the job again by clicking **Restart Job**.

For high-cost jobs requiring greater resources that, when run, can reduce repository performance, an edit icon (pencil) appears in the **Edit** column. Clicking on the icon displays a dialog allowing you to reschedule the next run time.

Figure 12–15 Job Reschedule Dialog



EM Audit Externalization Service Job : Schedule Next Run

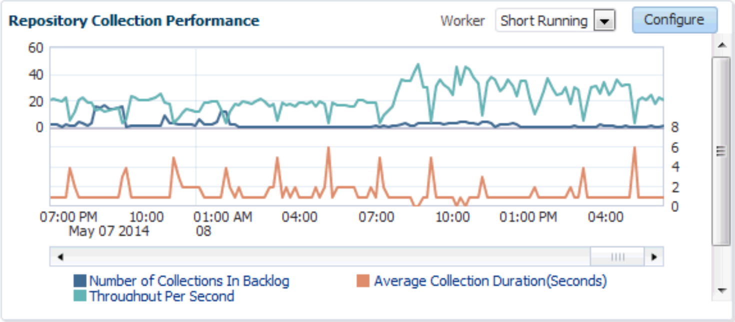
Next Scheduled Run May 9, 2014 7:59:42 AM PDT

Reschedule To: Hr: Min: ● AM ○ PM

Repository Collection Performance

The Repository Collection Performance region provides information on the performance of repository collections. They are collected by background DBMS jobs in the repository database called collection workers.

Figure 12–16 Repository Collection Performance Region



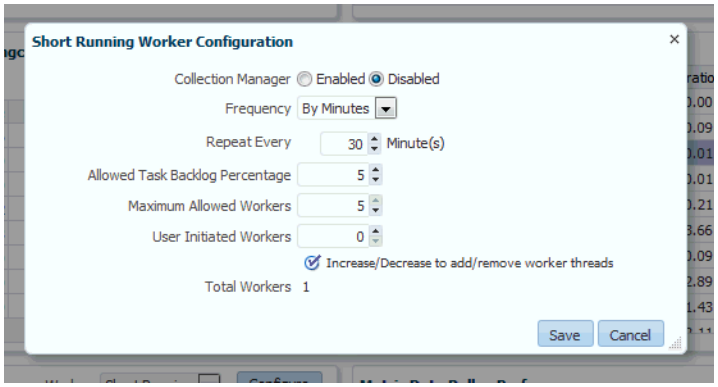
Repository Collection Performance

Worker: Short Running

Repository metrics are sub-divided into long and short running metrics. These are called task classes (short task class and long task class). Some collection workers process the short task class and some process long task class. Repository collection performance metrics measure the performance data for repository metric collections for each task class. This metric is a repository metric and hence collected by the collection workers.

You can select between **Short Running** and **Long Running** collection workers. When viewing Short Running workers, you can click **Configure** to change short worker settings.

Figure 12–17   Short Worker Configuration Dialog



Short Running Worker Configuration

Collection Manager ○ Enabled ● Disabled

Frequency By Minutes

Repeat Every 30 Minute(s)

Allowed Task Backlog Percentage 5

Maximum Allowed Workers 5

User Initiated Workers 0

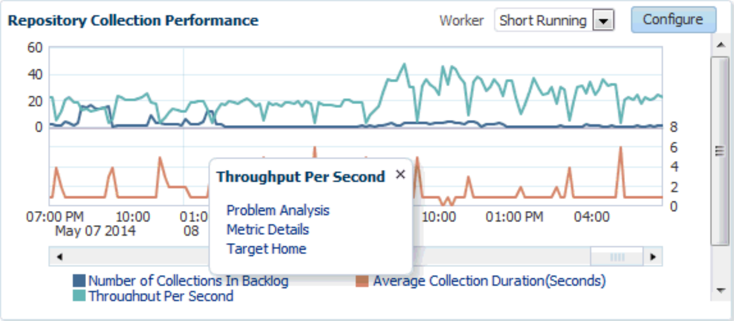
☑ Increase/Decrease to add/remove worker threads

Total Workers 1

Clicking **Save** submits a job to change the worker configuration. For this reason, the change will not be instantaneous and may require a minute or so in order to take effect.

Clicking on an item in the legend allows you to drill down into Problem Analysis, Metric Details, or the Target Home.

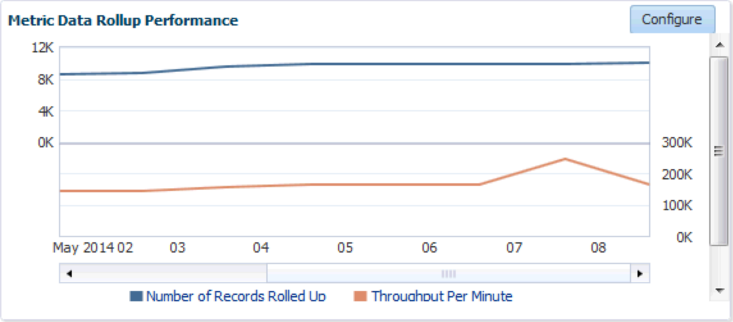
Figure 12–18   Collection Performance Information



Metric Data Rollup Performance

This region displays the rollup performance by graphically displaying the quantity of data being rolled up (Number of Records Rolled Up) and speed (Throughput per Minute) over time.

Figure 12–19 Metric Data Rollup Performance Region



The graphs for *Number of Records Rolled Up* and *Throughput per Minute* may increase over time as more targets are added, but on a daily basis should remain about the fairly level. Large spikes could indicate that agents are not communicating properly to the OMS

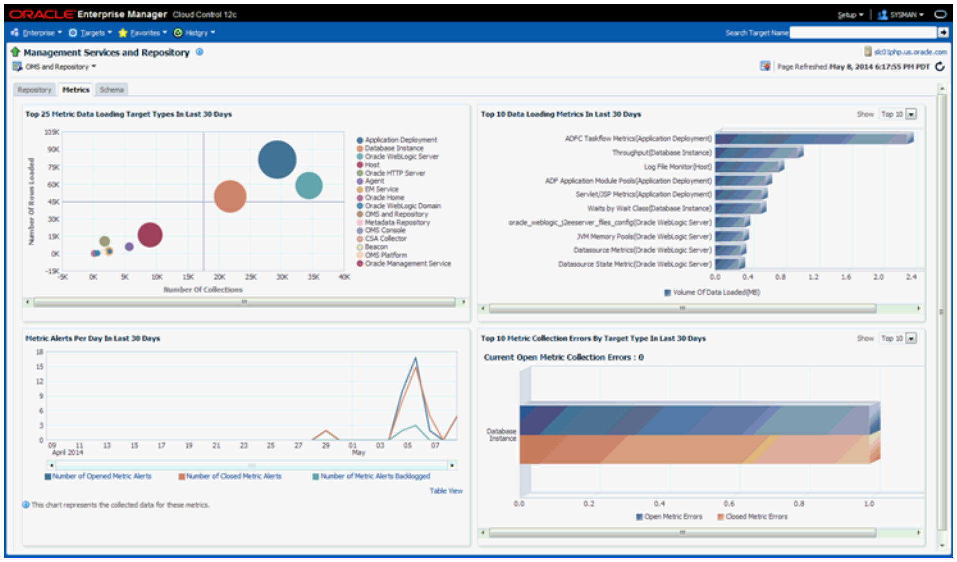
Clicking **Configure** allows you to change the number of rollup worker threads that will be started.

12.3.2 Metrics Tab

The Metrics tab provides a graphical rollup of key repository performance measurements. Information includes:

- Top 25 Metric Data Loading Target Types In Last 30 Days
- Top 10 Data Loading Metrics In Last 30 Days
- Metric Alerts Per Day In Last 30 Days
- Top 10 Metric Collection Errors By Target Type In Last 30 Days

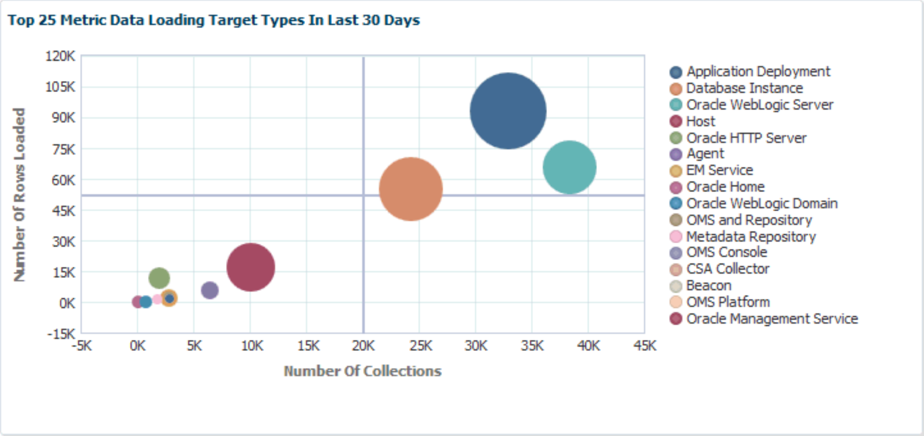
Figure 12–20 Metrics Tab


ORACLE Enterprise Manager Cloud Control 12c
Setup
SYSMAN
Enterprise
Targets
Favorites
History
Search Target Name
Management Services and Repository
OMS and Repository
slc01php.us.oracle.com
Page Refreshed May 8, 2014 6:17:55 PM PDT
Repository
Metrics
Schema
Top 25 Metric Data Loading Target Types In Last 30 Days
105K
90K
75K
60K
45K
30K
15K
0K
-15K
Number Of Rows Loaded
-5K
0K
5K
10K
15K
20K
25K
30K
35K
40K
Number Of Collections
Application Deployment
Database Instance
Oracle WebLogic Server
Host
Oracle HTTP Server
Agent
EM Service
Oracle Home
Oracle WebLogic Domain
OMS and Repository
Metadata Repository
OMS Console
CSA Collector
Beacon
OMS Platform
Oracle Management Service
Top 10 Data Loading Metrics In Last 30 Days
Show
Top 10
ADFC Taskflow Metrics(Application Deployment)
Throughput(Database Instance)
Log File Monitor(Host)
ADF Application Module Pools(Application Deployment)
Servlet/JSP Metrics(Application Deployment)
Waits by Wait Class(Database Instance)
oracle_weblogic_j2eeserver_files_config(Oracle WebLogic Server)
JVM Memory Pools(Oracle WebLogic Server)
Datasource Metrics(Oracle WebLogic Server)
Datasource State Metric(Oracle WebLogic Server)
0.0
0.4
0.8
1.2
1.6
2.0
2.4
Volume Of Data Loaded(MB)
Metric Alerts Per Day In Last 30 Days
18
15
12
9
6
3
0
09
April 2014
11
13
15
17
19
21
23
25
27
29
01
May
03
05
07
Number of Opened Metric Alerts
Number of Closed Metric Alerts
Number of Metric Alerts Backlogged
Table View
This chart represents the collected data for these metrics.
Top 10 Metric Collection Errors By Target Type In Last 30 Days
Show
Top 10
Current Open Metric Collection Errors : 0
Database Instance
0.0
0.2
0.4
0.6
0.8
1.0
Open Metric Errors
Closed Metric Errors

The graphs allow you to drill down to access information in greater detail.

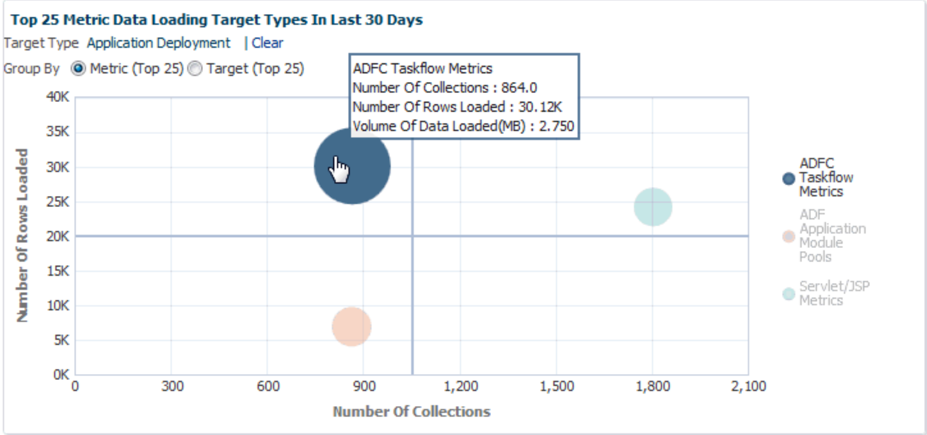
Top 25 Metric Data Loading Target Types In Last 30 Days

Figure 12–21 Top 25 Metric Data Loading Target Types In Last 30 Days



If you wish to view only metrics for a specific target type, click on a specific metric target type area within the graph. A new graph displays showing only metrics for that specific target type. You have the option grouping the results by metric or target.

Figure 12–22 Top 25 Metric Data Loading for a Single Target Type


Top 25 Metric Data Loading Target Types In Last 30 Days

Target Type Application Deployment | Clear

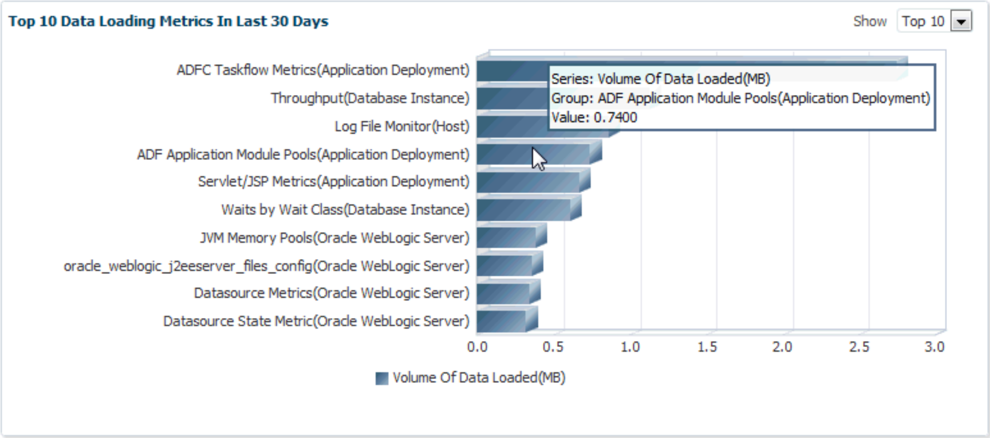
Group By ● Metric (Top 25) ○ Target (Top 25)

ADFC Taskflow Metrics
Number Of Collections : 864.0
Number Of Rows Loaded : 30.12K
Volume Of Data Loaded(MB) : 2.750

Click **Clear** to return to the original graph containing all target types.

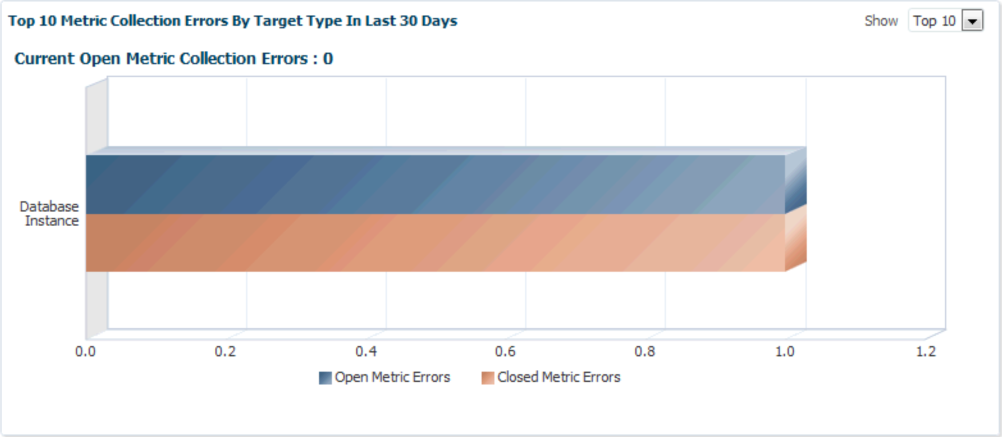
Top 10 Data Loading Metrics In Last 30 Days

Figure 12–23 Metric Data Load Volume



Top 10 Metric Collection Errors By Target Type In Last 30 Days

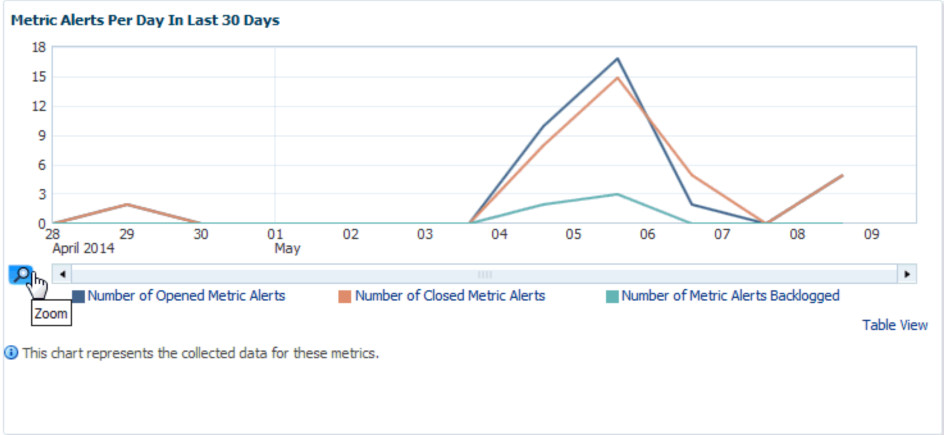
Figure 12–24



Metric Alerts Per Day In Last 30 Days

The Metric Alerts Per Day In Last 30 Days graphically displays the number of open, closed, and backlogged metric alerts over time. If you wish to focus on a narrower time span, click **Zoom**.

Figure 12–25 Metric Alerts Per Day



This chart represents the collected data for these metrics.

12.3.3 Schema Tab

The Schema tab provides physical attribute and performance data pertaining to the repository database schema. Information includes:

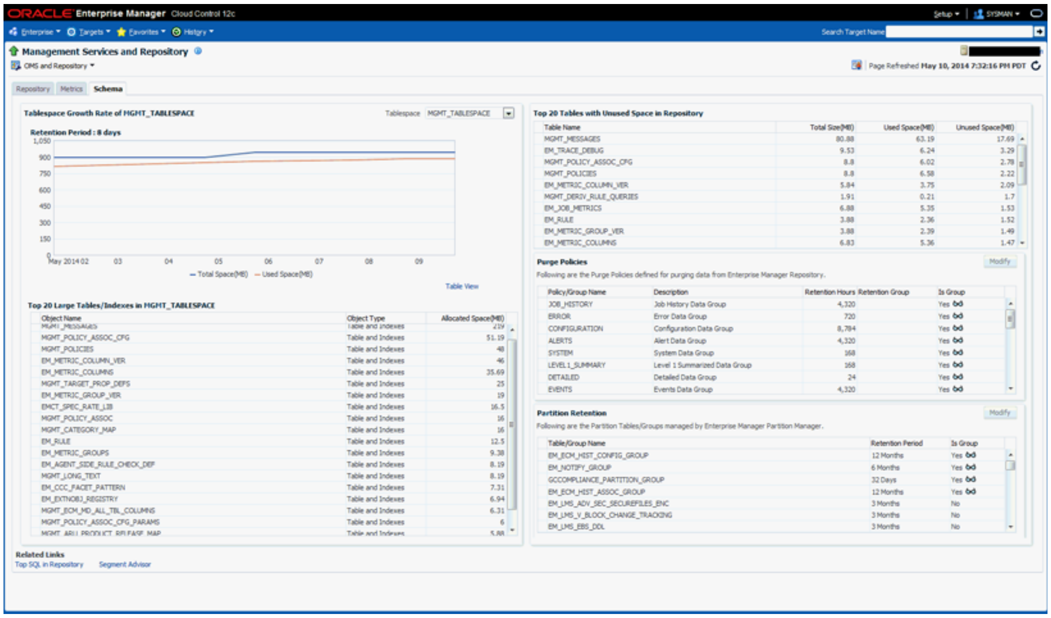
- Tablespace Growth Rate

  You can select the specific tablespace: MGMT_TABLESPACE, MGMT_ECM_DEPOT_TS, or MGMT_AD4J_TS.

  Top 20 Large Tables/Indexes are also displayed.

- Top 20 Tables with Unused Space in Repository
- Purge Policies
- Partition Retention

Figure 12–26 Schema Tab



Management Services and Repository

OMS and Repository

[redacted]

Page Refreshed **May 10, 2014 7:32:16 PM PDT**

Tablespace Growth Rate of MGMT_TABLESPACE

Retention Period : 8 days

Top 20 Large Tables/Indexes in MGMT_TABLESPACE

Object Name	Object Type	Allocated Space(MB)
MGMT_MESSAGES	Table and Indexes	219
MGMT_POLICY_ASSOC_CFG	Table and Indexes	51.19
MGMT_POLICIES	Table and Indexes	48
EM_METRIC_COLUMN_VER	Table and Indexes	46
EM_METRIC_COLUMNS	Table and Indexes	35.69
MGMT_TARGET_PROP_DEFS	Table and Indexes	25
EM_METRIC_GROUP_VER	Table and Indexes	19
EMCT_SPEC_RATE_LIB	Table and Indexes	16.5
MGMT_POLICY_ASSOC	Table and Indexes	16
MGMT_CATEGORY_MAP	Table and Indexes	16
EM_RULE	Table and Indexes	12.5
EM_METRIC_GROUPS	Table and Indexes	9.38
EM_AGENT_SIDE_RULE_CHECK_DEF	Table and Indexes	8.19
MGMT_LONG_TEXT	Table and Indexes	8.19
EM_CCC_FACET_PATTERN	Table and Indexes	7.31
EM_EXTNOBJ_REGISTRY	Table and Indexes	6.94
MGMT_ECM_MD_ALL_TBL_COLUMNS	Table and Indexes	6.31
MGMT_POLICY_ASSOC_CFG_PARAMS	Table and Indexes	6
MGMT_ARU_PRODUCT_RELEASE_MAP	Table and Indexes	5.88

Related Links

Top SQL in Repository Segment Advisor

Top 20 Tables with Unused Space in Repository

Table Name	Total Size(MB)	Used Space(MB)	Unused Space(MB)
MGMT_MESSAGES	80.88	63.19	17.69
EM_TRACE_DEBUG	9.53	6.24	3.29
MGMT_POLICY_ASSOC_CFG	8.8	6.02	2.78
MGMT_POLICIES	8.8	6.58	2.22
EM_METRIC_COLUMN_VER	5.84	3.75	2.09
MGMT_DERIV_RULE_QUERIES	1.91	0.21	1.7
EM_JOB_METRICS	6.88	5.35	1.53
EM_RULE	3.88	2.36	1.52
EM_METRIC_GROUP_VER	3.88	2.39	1.49
EM_METRIC_COLUMNS	6.83	5.36	1.47

Purge Policies

Following are the Purge Policies defined for purging data from Enterprise Manager Repository.

Policy/Group Name	Description	Retention Hours	Retention Group	Is Group
JOB_HISTORY	Job History Data Group	4,320		Yes
ERROR	Error Data Group	720		Yes
CONFIGURATION	Configuration Data Group	8,784		Yes
ALERTS	Alert Data Group	4,320		Yes
SYSTEM	System Data Group	168		Yes
LEVEL1_SUMMARY	Level 1 Summarized Data Group	168		Yes
DETAILED	Detailed Data Group	24		Yes
EVENTS	Events Data Group	4,320		Yes

Partition Retention

Following are the Partition Tables/Groups managed by Enterprise Manager Partition Manager.

Table/Group Name	Retention Period	Is Group
EM_ECM_HIST_CONFIG_GROUP	12 Months	Yes
EM_NOTIFY_GROUP	6 Months	Yes
GCCOMPLIANCE_PARTITION_GROUP	32 Days	Yes
EM_ECM_HIST_ASSOC_GROUP	12 Months	Yes
EM_LMS_ADV_SEC_SECUREFILES_ENC	3 Months	No
EM_LMS_V_BLOCK_CHANGE_TRACKING	3 Months	No
EM_LMS_EBS_DDL	3 Months	No

12.4 Controlling and Configuring Management Agents

Beginning with Enterprise Manager Cloud Control 12*c*, controlling Management Agents can be performed directly from the Enterprise Manager console. This provides a central point where all Management Agents within your monitored environment can be compared, configured and controlled.

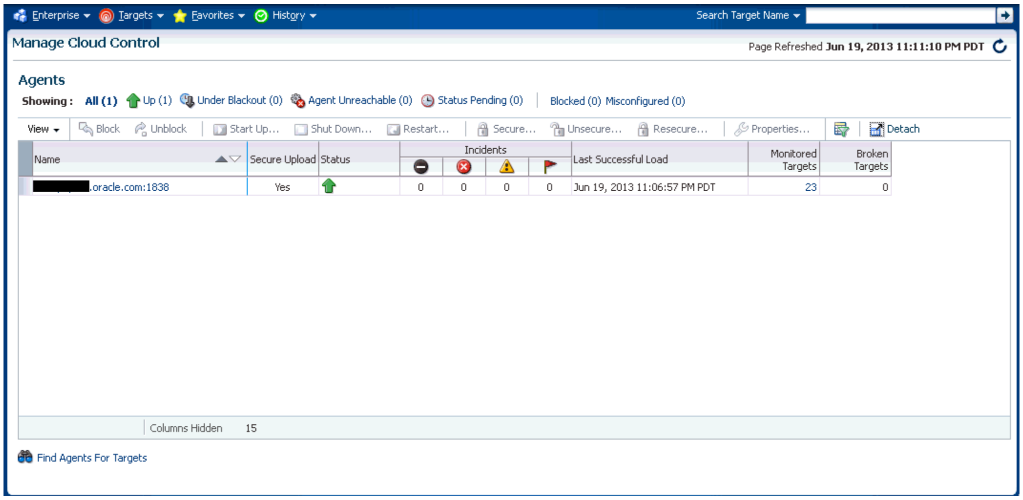
12.4.1 Manage Cloud Control Agents Page

The Agents page lists all Management Agents within your monitored environment. This page also includes misconfigured, blocked and both upgradable and non-upgradable Agents.

Accessing the Agent Page

From the **Setup** menu, select **Manage Cloud Control** and then **Agents.**

Figure 12–27 Agent List Page



Enterprise ▾
Targets ▾
Favorites ▾
History ▾
Search Target Name ▾
Manage Cloud Control
Page Refreshed **Jun 19, 2013 11:11:10 PM PDT**
Agents
Showing : All (1) Up (1) Under Blackout (0) Agent Unreachable (0) Status Pending (0) | Blocked (0) Misconfigured (0)
View ▾ | Block | Unblock | Start Up... | Shut Down... | Restart... | Secure... | Unsecure... | Resecure... | Properties... | Detach

Name	Secure Upload	Status	Incidents				Last Successful Load	Monitored Targets	Broken Targets
			⊖	⊗	⚠	⚑			
[redacted].oracle.com:1838	Yes	↑	0	0	0	0	Jun 19, 2013 11:06:57 PM PDT	23	0

Columns Hidden 15
Find Agents For Targets

Misconfigured and Blocked Agents

A *misconfigured* Agent is an Agent that is not able to perform a heartbeat or upload data to the Oracle Management Service (OMS) due to invalid configuration or invalid data. Agent misconfiguration alerts are triggered by the following metrics:

- Consecutive metadata upload failure count
- Consecutive ping failure count
- Consecutive severity upload failure count
- OMS Agent time skew

If the Agent heartbeat or upload requests are failing consistently, and the problem cannot be resolved in a timely manner, you can manually *block* the Agent to prevent excessive load on the OMS. When you block an Agent, the OMS rejects all heartbeat or upload requests from the blocked Agent. However, even though blocked Agents continue to collect monitoring data, it will not be able to upload any alerts or metric data to the OMS. Once the Agent configuration problem is resolved, you must manually *unblock* the Agent to resume normal operation.

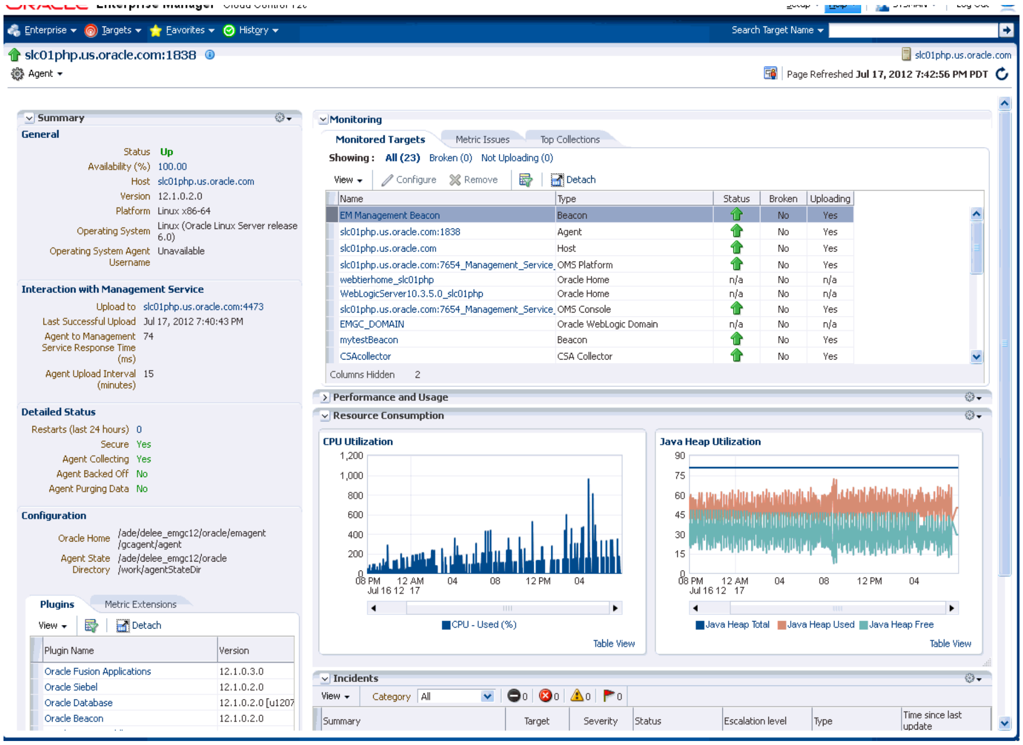
Note: Before unblocking the Agent, ensure that all issues related to Agent misconfiguration have been resolved.

From this page, you can also initiate the Agent upgrade process. For more information about upgrading Agents see "Upgrading Multiple Management Agents" on page 12-25.

12.4.2 Agent Home Page

The Agent home page provides details for a single Agent. This page also lets you drill down for more detailed information. You can access an Agent home page by clicking on a specific Agent from in the Agent list page or by selecting it from the All Targets page.

Figure 12–28 Agent Home Page



slc01php.us.oracle.com:1838

slc01php.us.oracle.com

Page Refreshed **Jul 17, 2012 7:42:56 PM PDT**

General

Status	Up
Availability (%)	100.00
Host	slc01php.us.oracle.com
Version	12.1.0.2.0
Platform	Linux x86-64
Operating System	Linux (Oracle Linux Server release 6.0)
Operating System Agent Username	Unavailable

Interaction with Management Service

Upload to	slc01php.us.oracle.com:4473
Last Successful Upload	Jul 17, 2012 7:40:43 PM
Agent to Management Service Response Time (ms)	74
Agent Upload Interval (minutes)	15

Detailed Status

Restarts (last 24 hours)	0
Secure	Yes
Agent Collecting	Yes
Agent Backed Off	No
Agent Purging Data	No

Configuration

Oracle Home	/ade/delee_emgc12/oracle/emagent /gcagent/agent
Agent State Directory	/ade/delee_emgc12/oracle /work/agentStateDir

Plugin Name	Version
Oracle Fusion Applications	12.1.0.3.0
Oracle Siebel	12.1.0.2.0
Oracle Database	12.1.0.2.0 [u1207
Oracle Beacon	12.1.0.2.0

Showing : All (23) Broken (0) Not Uploading (0)

Name	Type	Status	Broken	Uploading
EM Management Beacon	Beacon	↑	No	Yes
slc01php.us.oracle.com:1838	Agent	↑	No	Yes
slc01php.us.oracle.com	Host	↑	No	Yes
slc01php.us.oracle.com:7654_Management_Service_	OMS Platform	↑	No	Yes
webtierhome_slc01php	Oracle Home	n/a	No	n/a
WebLogicServer10.3.5.0_slc01php	Oracle Home	n/a	No	n/a
slc01php.us.oracle.com:7654_Management_Service_	OMS Console	↑	No	Yes
EMGC_DOMAIN	Oracle WebLogic Domain	n/a	No	n/a
mytestBeacon	Beacon	↑	No	Yes
CSAcollector	CSA Collector	↑	No	Yes

Columns Hidden 2

Category All 0 0 0 0

Summary	Target	Severity	Status	Escalation level	Type	Time since last update

- The **Summary** region provides primary details of the Agent such as its status and availability. The Interaction with Management Service region provides details on the communication between the OMS and the Agent and metric extensions and management plug-ins deployed in the Agent.
- The **Status** region provides further details on the Agent status such as the number of restarts, the action that the Agent is performing currently.
- The **Performance, Usage and Resource Consumption** charts provide further details on the Agent in graphical format.
- The **Incidents** region lists the incidents recorded for the Agent.
- The **Monitoring** region provides details on the targets that are being monitored by the Agent. You can filter targets in this region by All, Broken, and Not Uploading.

Separate tabs within the Monitoring section display Metric Issues and Top Collections.

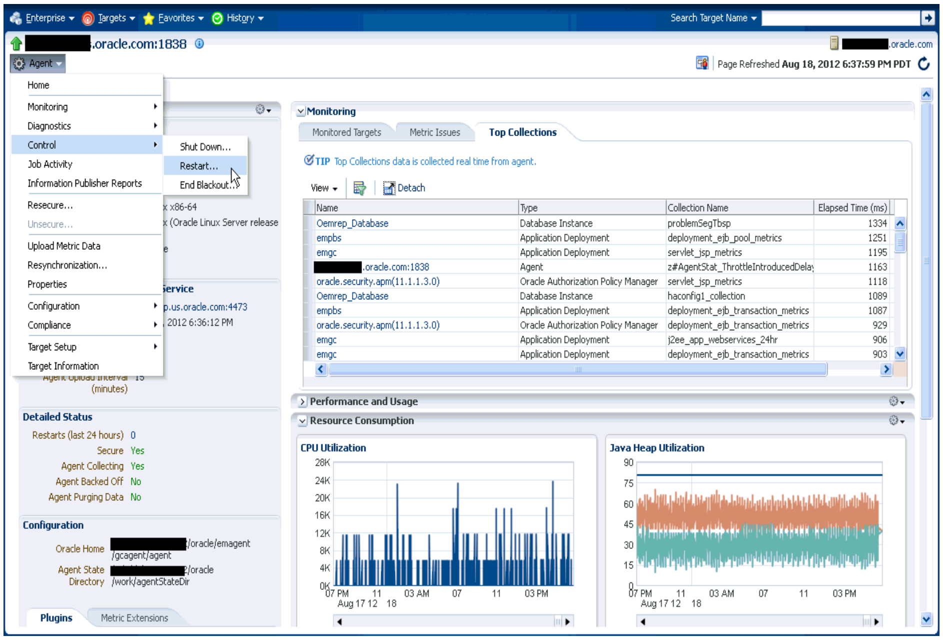
12.4.3 Controlling a Single Agent

Control operations for a single Agent can be performed on the Agent home page for that Agent.

1. Navigate to the desired Agent home page.
2. From the **Agent** drop-down menu, choose **Control** and then one of the control operations (Start Up/Shut Down, or Restart)

Note: You must have at least operator privileges in order to perform Agent control operations.

Figure 12–29 Control Operations from the Agent Home Page



[redacted].oracle.com:1838

[redacted].oracle.com

Page Refreshed **Aug 18, 2012 6:37:59 PM PDT**

x x86-64

x (Oracle Linux Server release

e

Service

p.us.oracle.com:4473

, 2012 6:36:12 PM

Agent Upload Interval (minutes) 15

Detailed Status

Restarts (last 24 hours) 0
Secure Yes
Agent Collecting Yes
Agent Backed Off No
Agent Purging Data No

Configuration

Oracle Home [redacted]/oracle/emagent/gcagent/agent
Agent State Directory [redacted]/oracle/work/agentStateDir

TIP Top Collections data is collected real time from agent.

Name	Type	Collection Name	Elapsed Time (ms)
Oemrep_Database	Database Instance	problemSegTbsp	1334
empbs	Application Deployment	deployment_ejb_pool_metrics	1251
emgc	Application Deployment	servlet_jsp_metrics	1195
[redacted].oracle.com:1838	Agent	z#AgentStat_ThrottleIntroducedDela	1163
oracle.security.apm(11.1.1.3.0)	Oracle Authorization Policy Manager	servlet_jsp_metrics	1118
Oemrep_Database	Database Instance	haconfig1_collection	1089
empbs	Application Deployment	deployment_ejb_transaction_metrics	1087
oracle.security.apm(11.1.1.3.0)	Oracle Authorization Policy Manager	deployment_ejb_transaction_metrics	929
emgc	Application Deployment	j2ee_app_webservices_24hr	906
emgc	Application Deployment	deployment_ejb_transaction_metrics	903

Upon choosing any of the above control menu options, a pop-up dialog requesting the credentials of the user displays. These operations require the credentials of the OS user who owns the Agent, or credentials of a user who has SUDO or PowerBroker privilege of the Agent owner. At this point, you can either choose from a previously stored username/password, preferred or named credential. You also have the option of choosing a new set of credentials which could also be saved as the preferred credential or as a named credential for future use.

Once you are authenticated, the chosen control operation begins and continues even if the pop-up dialog is closed. Any message of failure/success of the task is displayed in the pop-up dialog.

When choosing the Secure/Resecure/Unsecure options, you must provide the requisite Registration Password.

Agent Control When Using a Server Load Balancer

When choosing the Agent Secure/Resecure options in a multi-OMS environment with a server load balancer (SLB), the Agent will be secured/resecured against the SLB automatically without administrator intervention.

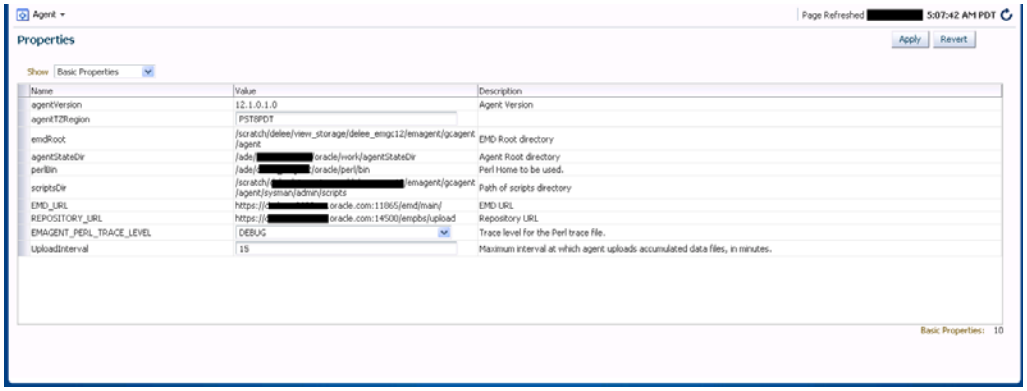
12.4.4 Configuring Single Management Agents

Configuration operations for a single Agent can be performed from the Agent home page. To access the Agent properties page:

1. Navigate to the desired Agent home page.
2. From the **Agent** drop-down menu, select **Properties**.

> **Note:** You must have at least Configure privileges in order to perform Agent configuration operations.

Figure 12–30 Agent Properties Page



Name	Value	Description
agentVersion	12.1.0.1.0	Agent Version
agentTZRegion	PST8PDT	
emdRoot	/scratch/delee/view_storage/delee_emgc12/emagent/gcagent /agent	EMD Root directory
agentStateDir	/ade/[redacted]oracle/work/agentStateDir	Agent Root directory
perlBin	/ade/[redacted]/oracle/perl/bin	Perl Home to be used.
scriptsDir	/scratch/[redacted]/emagent/gcagent /agent/sysman/admin/scripts	Path of scripts directory
EMD_URL	https://[redacted].oracle.com:11865/emd/main/	EMD URL
REPOSITORY_URL	https://[redacted]oracle.com:14500/empbs/upload	Repository URL
EMAGENT_PERL_TRACE_LEVEL	DEBUG	Trace level for the Perl trace file.
UploadInterval	15	Maximum interval at which agent uploads accumulated data files, in minutes.

The properties on this page can be filtered to show **All Properties**, **Basic Properties**, or **Advanced Properties**. The **Basic Properties** are a simple name, value combination of a property and its value. **Advanced Properties** are also a combination of name and value but can also be grouped into categories. You must have at least *configure* privileges in order to modify the existing properties and set custom properties.

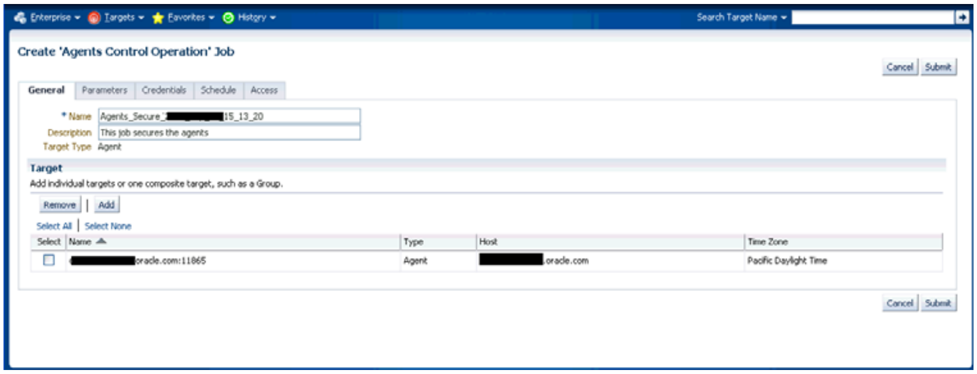
12.4.5 Controlling Multiple Management Agents

In order to perform control operations on multiple Management Agents, Enterprise Manager makes use of the Job system to automate repetitive tasks. Therefore, you must have Job privileges for controlling multiple Management Agents through a single action. To access

1. From the **Setup** menu, select **Manage Cloud Control and then Agents**. The Agent page displays.
2. Select multiple Management Agents from the list.
3. Click one of the control operation buttons (**Start Up/Shut Down/Restart/Secure/Resecure/Unsecure**).

When you click on any of the control operations, you are taken to the Job creation wizard where you schedule a new job to perform the action on the selected Agents.

Figure 12–31 Multiple Agent Control Operation: Job Creation



Create 'Agents Control Operation' Job

* Name: Agents_Secure_[redacted]15_13_20
Description: This job secures the agents
Target Type: Agent

Target

Add individual targets or one composite target, such as a Group.

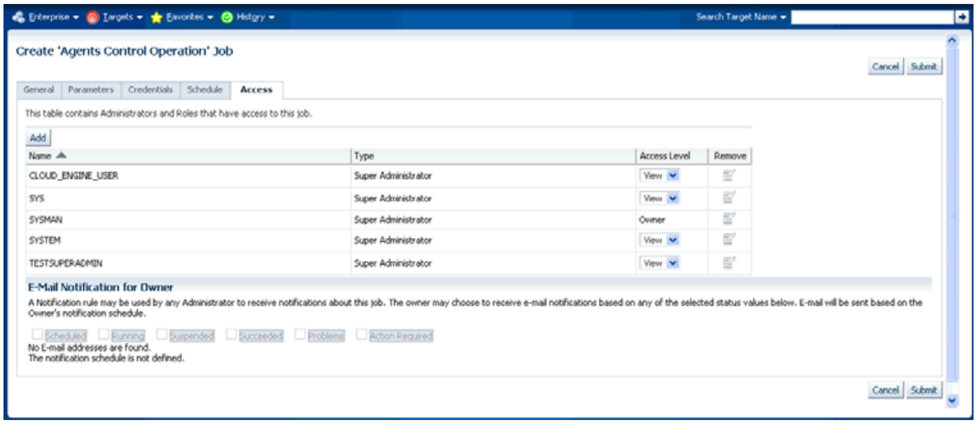
Select	Name	Type	Host	Time Zone
□	[redacted]oracle.com:11865	Agent	[redacted].oracle.com	Pacific Daylight Time

In the Jobs page, you can view the chosen Management Agents in Target section in the General tab. You can add more Management Agents by clicking the **Add** button. You then provide the parameters for the operation in the **Parameters** tab, if needed. The credentials must be specified in the **Credentials** tab where you can either choose from a previously stored username/password, preferred, or named credential. You also have the option of choosing a new set of credentials which could also be saved as the preferred credential or as a named credential for future use.

You are given the option to start the job immediately or schedule the job for a later time. At this point, you can also create a repeating job by specifying the job start time, the frequency, and the end time.

The Access tab displays the Administrator details and the access levels they have to the job. You can then add a new administrator or modify the access level to **View** or **Full**, if you have the requisite privileges.

Figure 12–32 Job Creation: Access Tab



Create 'Agents Control Operation' Job

This table contains Administrators and Roles that have access to this job.

Name	Type	Access Level	Remove
CLOUD_ENGINE_USER	Super Administrator	View	
SYS	Super Administrator	View	
SYSMAN	Super Administrator	Owner	
SYSTEM	Super Administrator	View	
TESTSUPERADMIN	Super Administrator	View	

E-Mail Notification for Owner

A Notification rule may be used by any Administrator to receive notifications about this job. The owner may choose to receive e-mail notifications based on any of the selected status values below. E-mail will be sent based on the Owner's notification schedule.

□ Scheduled □ Running □ Suspended □ Succeeded □ Problems □ Action Required

No E-mail addresses are found.
The notification schedule is not defined.

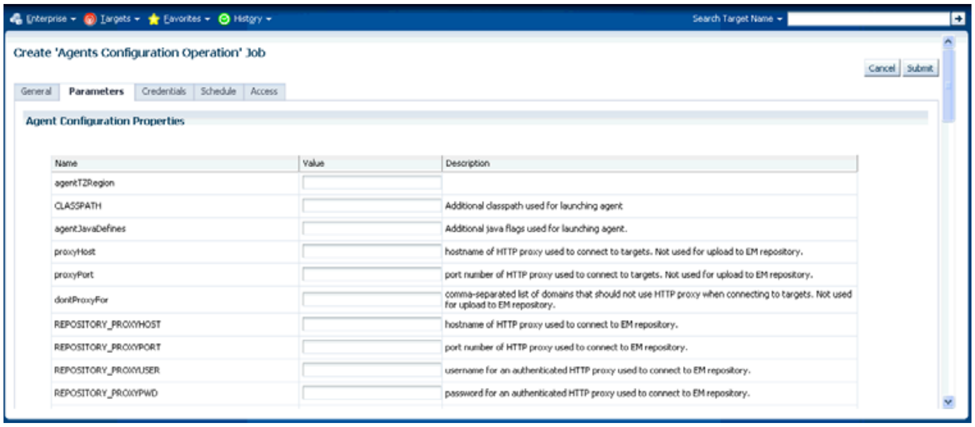
Note: Administrators with insufficient privileges can also schedule jobs for these control operations, but in this situation, the jobs will not complete successfully.

12.4.6 Configuring Multiple Agents

As with multi-Agent control operations, you can also perform Agent configuration on multiple Agents in the same way. This greatly simplifies standardizing Agent configurations across your enterprise. To access Agent properties:

1. From the **Setup** menu, select Manage Cloud Control and then **Agents**. The Agent page displays.
2. Select multiple Management Agents from the list.
3. Click **Properties**. As with any multi-Agent operation, configuration is implemented using the Job system.

Figure 12–33 Agent Properties Page



Create 'Agents Configuration Operation' Job

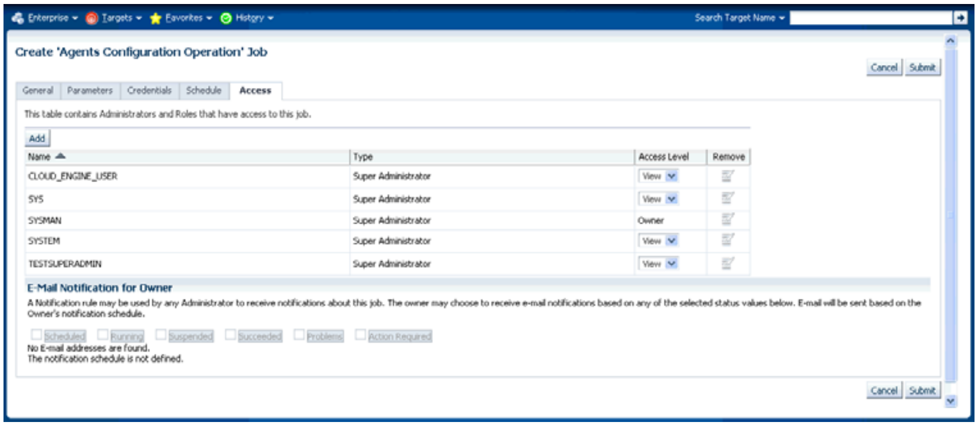
Agent Configuration Properties

Name	Value	Description
agentTZRegion		
CLASSPATH		Additional classpath used for launching agent
agentJavaDefines		Additional java flags used for launching agent.
proxyHost		hostname of HTTP proxy used to connect to targets. Not used for upload to EM repository.
proxyPort		port number of HTTP proxy used to connect to targets. Not used for upload to EM repository.
dontProxyFor		comma-separated list of domains that should not use HTTP proxy when connecting to targets. Not used for upload to EM repository.
REPOSITORY_PROXYHOST		hostname of HTTP proxy used to connect to EM repository.
REPOSITORY_PROXYPORT		port number of HTTP proxy used to connect to EM repository.
REPOSITORY_PROXYUSER		username for an authenticated HTTP proxy used to connect to EM repository.
REPOSITORY_PROXYPWD		password for an authenticated HTTP proxy used to connect to EM repository.

In the Jobs page, you can view the chosen Management Agents in the Target section of the General tab. You can add more Management Agents by clicking the **Add** button if necessary. In the **Parameters** tab, you provide the modified value for a particular set of properties that you want to change. You can also set a custom property for the chosen agents. No credentials are required for modifying Agent properties.

The **Access** tab displays the administrator details and the access levels they have to the job. You can then add a new administrator or modify the access level to View or Full if you have the requisite privileges.

Figure 12–34 Multi-Agent Configuration: Job Access



Create 'Agents Configuration Operation' Job

This table contains Administrators and Roles that have access to this job.

Name	Type	Access Level	Remove
CLOUD_ENGINE_USER	Super Administrator	View	
SYS	Super Administrator	View	
SYSMAN	Super Administrator	Owner	
SYSTEM	Super Administrator	View	
TESTSUPERADMIN	Super Administrator	View	

E-Mail Notification for Owner

A Notification rule may be used by any Administrator to receive notifications about this job. The owner may choose to receive e-mail notifications based on any of the selected status values below. E-mail will be sent based on the Owner's notification schedule.

□ Scheduled □ Running □ Suspended □ Succeeded □ Problems □ Action Required

No E-mail addresses are found.
The notification schedule is not defined.

12.4.7 Upgrading Multiple Management Agents

When you upgrade to the current Enterprise Manager Cloud Control 12c release, you upgrade your Oracle Management Services (OMS) to the current release, but not your target Oracle Management Agents (Management Agents). To mass-upgrade your Management Agents, access the Upgrade Agents page. To access this page:

1. From the **Setup** menu, select **Manage Cloud Control,** then select **Agents.**
2. Click **Upgradable,** then select the Management Agents you want to upgrade.
3. Click **Upgrade.**

Alternatively, to access the Upgrade Agents page, from the **Setup** menu, select **Manage Cloud Control,** then select **Upgrade Agent.** For more information on upgrading Management Agents, refer Upgrading Oracle Management Agents.

12.5 Management Servers

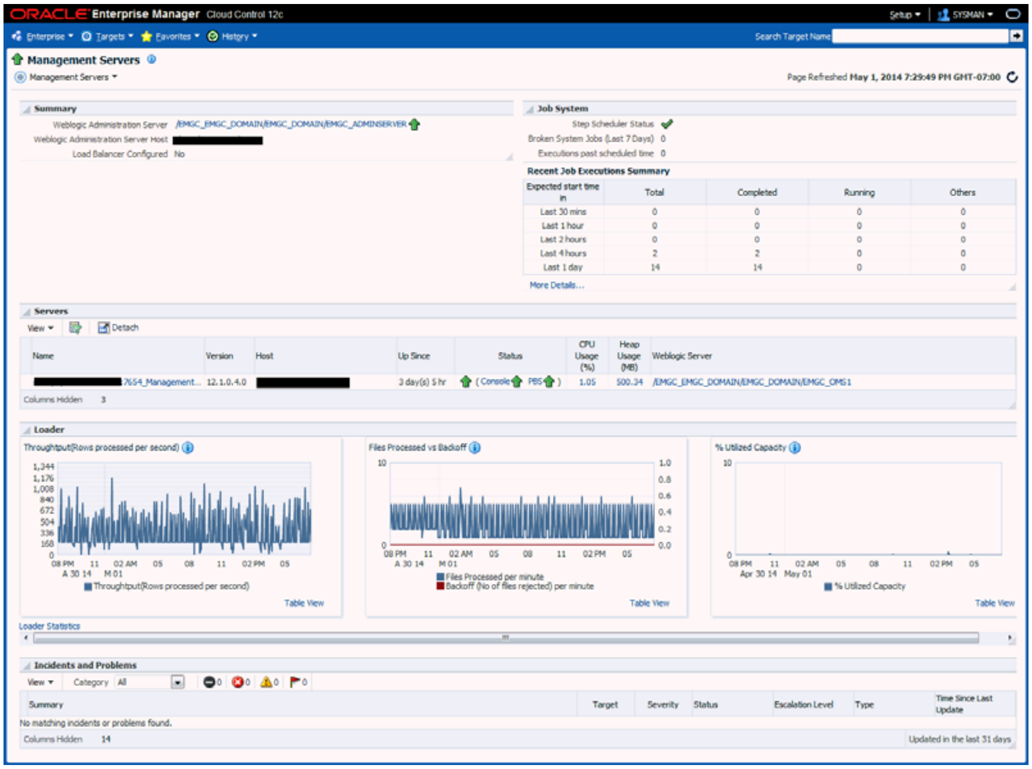
A Management Server is a composite target consisting of multiple Enterprise Manager Management Services.

The Management Servers page displays the list of Management Services, their status, incidents, the loader throughput, CPU usage, and the JVM memory usage metrics. In addition, the Management Services displayed can be filtered by Normal Mode, Console Only, PBS only and Standby Management Services.

Accessing the Management Servers Page

From the **Setup** menu, select **Manage Cloud Control** and then **Management Services**.

Figure 12–35 Management Servers Page



Page Refreshed **May 1, 2014 7:29:49 PM GMT-07:00**

Weblogic Administration Server /EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_ADMINSERVER

Weblogic Administration Server Host [redacted]

Load Balancer Configured No

Step Scheduler Status ✓

Broken System Jobs (Last 7 Days) 0

Executions past scheduled time 0

Recent Job Executions Summary

Expected start time in	Total	Completed	Running	Others
Last 30 mins	0	0	0	0
Last 1 hour	0	0	0	0
Last 2 hours	0	0	0	0
Last 4 hours	2	2	0	0
Last 1 day	14	14	0	0

More Details...

Name	Version	Host	Up Since	Status	CPU Usage (%)	Heap Usage (MB)	Weblogic Server
[redacted]7654_Management...	12.1.0.4.0	[redacted]	3 day(s) 5 hr	(Console PBS)	1.05	500.34	/EMGC_EMGC_DOMAIN/EMGC_DOMAIN/EMGC_OMS1

Columns Hidden 3

Summary	Target	Severity	Status	Escalation Level	Type	Time Since Last Update

No matching incidents or problems found.

Columns Hidden 14

Updated in the last 31 days

This page consists of the following sections:

- **Summary**: Displays the high-level information about WebLogic administration server and Load balancer.
- **Job System**: Displays information about the status of jobs over past time periods (such as the last 30 minutes, 1 hour, or 2 hours).

- **Servers**: Displays information about individual Management Services of the Management Server.
- **Loader**: Displays information that provides insight into the Loader subsystem performance as a whole.

  There are primarily 3 graphs as follows.

  - Throughtput (Rows processed per second): Indicates the rate (rows processed per second) at which the Loader is processing files.
  - Files Processed vs Backoff: Indicates the number of files processed versus backed off (rejected) by the Loader. Note: You should contact Oracle Support if consistent backoffs are being generated.
  - % Utilized Capacity: Sows the current Loader CPU utilization. If the Loader consistently runs at more than 85% capacity, contact Oracle Support to confirm whether your system capacity needs to be increased.

  To view detailed IP reports of Loader statistics, click the **Loader Statistics** link located below the graphs.
- **Incidents**: This displays the incidents and problems that have occurred against individual targets hosting Management Services.

13 Maintaining and Troubleshooting the Management Repository

This chapter describes maintenance and troubleshooting techniques for maintaining a well-performing Management Repository.

Specifically, this chapter contains the following sections:

13.1 Management Repository Deployment Guidelines

To be sure that your management data is secure, reliable, and always available, consider the following settings and configuration guidelines when you are deploying the Management Repository:

- Install a RAID-capable Logical Volume Manager (LVM) or hardware RAID on the system where the Management Repository resides. At a minimum the operating system must support disk mirroring and stripping. Configure all the Management Repository data files with some redundant configuration.
- Use Real Application Clusters to provide the highest levels of availability for the Management Repository.
- If you use Enterprise Manager to alert administrators of errors or availability issues in a production environment, be sure that the Cloud Control components are configured with the same level of availability. At a minimum, consider using Oracle Data Guard to mirror the Management Repository database. Configure Data Guard for zero data loss. Choose between Maximum Availability or Maximum Protection based on your environment and needs.

  > **See Also:** *Oracle Database High Availability Architecture and Best Practices*
  >
  > *Oracle Data Guard Concepts and Administration*

- Oracle strongly recommends that archive logging be turned on and that a comprehensive backup strategy be in place prior to an Enterprise Manager implementation going live in a production environment. The backup strategy should include archive backups and both incremental and full backups as required.

> **See Also:** *Oracle Enterprise Manager Cloud Control Installation and Basic Configuration* for information about the database initialization parameters required for the Management Repository

- Oracle recommends that you not use SQL Plan Management (SQL plan baselines and capture) with the Enterprise Manager Cloud Control repository. If you do need to use it for a specific problem, shut it off immediately after using. Issues with the Enterprise Manager Cloud Control repository may occur when using SQL Plan Management, such as very poor SQL performance using unverified plans, and deadlocks between SQL Plan Management capture and the Enterprise Manager security VPD.
- After enabling auditing for the repository database and for audit entries related to ORA- errors, error messages should be ignored if they are not reported in the Enterprise Manager application logs; for example, emoms.trc, the MGMT_SYSTEM_ERROR_LOG table, or in the alert.log of the repository database. In these cases the errors are harmless.
- To see a list of the regular maintenance activities that need to be performed for the repository, see the Sizing Your Enterprise Manager Deployment in the *Oracle® Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.
- To monitor the repository database activities using the Enterprise Manager user interface, see Chapter 12, "Maintaining Enterprise Manager".

13.2 Management Repository Data Retention Policies

When the various components of Enterprise Manager are configured and running efficiently, the Oracle Management Service gathers large amounts of raw data from the Management Agents running on your managed hosts and loads that data into the Management Repository. This data is the raw information that is later aggregated, organized, and presented to you in the Cloud Control console.

After the Oracle Management Service loads information into the Management Repository, Enterprise Manager aggregates and purges the data over time.

The following sections describe:

- The default aggregation and purging policies used to maintain data in the Management Repository.
- How you can modify the length of time the data is retained before it is aggregated and then purged from the Management Repository.

13.2.1 Management Repository Default Aggregation and Purging Policies

Enterprise Manager aggregates collected metric data by hour and by day to enhance query performance and help minimize the size of the Management Repository. Before the data is aggregated, each data point is stored in a raw metric data table. Once a day, the previous day’s raw metric data is rolled up, or aggregated, into a one-hour and a one-day table. These hourly and daily records will have hourly and daily metric data averages, minimums, maximums and standard deviations respectively.

After Enterprise Manager aggregates the data, the data is then considered eligible for purging. A certain period of time must pass for data to actually be purged. This period of time is called the retention time.

The raw data, with the highest insert volume, has the shortest default retention time, which is set to 7 days. As a result, 7 days after it is aggregated into a one-hour record, a raw data point is eligible for purging.

> **Note:** This data retention policy varies for JVMD and ADP data.

Hourly aggregate metric data records are purged after 31 days. The highest level of aggregation, one day, is kept for 12 months (roughly 365 days).

The default data retention policies are summarized in Table 13–1.

Table 13–1 Default Repository Purging Policies

Aggregate Level	Retention Time
Raw metric data	7 days
Hourly aggregated metric data	31 days
Daily aggregated metric data	24 months

If you have configured and enabled Application Performance Management, Enterprise Manager also gathers, saves, aggregates, and purges response time data. The response time data is purged using policies similar to those used for metric data. The Application Performance Management purging policies are shown in Table 13–2.

Table 13–2 Default Repository Purging Policies for Application Performance Management Data

Aggregate Level	Retention Time
Raw response time data	24 hours
One-hour aggregated response time data	7 days
One-hour distribution response time data	24 hours
One-day aggregated response time data	31 days
One-day distribution aggregated response time data	31 days

If you do not want to keep severity data for the default period (6 months), and want to reduce the retention period for the EVENTS purge policy, you can use the following command:

```
em_purge.modify_purge_policy_group('EVENTS',NULL,*l_new_purge_
hours*);
```

Events data is partitioned and maintains six months of historical data by default. You can change the default retention period using the procedure described above. The severity data is tied to the events data purge policy and will be adjusted accordingly.

The fixed set of tables affected by this data purge are listed below:

```
EM_EVENT_SEQUENCES
EM_EVENT_RAW
EM_EVENT_MSGS
EM_EVENT_CONTEXT
```

```
EM_EVENT_ANNOTATIONS
EM_EVENTS_INCIDENT
EM_ISSUES_INTERNAL
EM_ISSUES_MSG
EM_ISSUES_ANNOTATIONS
EM_INCIDENT_ISSUE
EM_PROBLEM_ISSUE
EM_INCIDENTS_PROBLEM
```

The following list is a dynamic set of tables that store data for different event types supported by Enterprise Manager. This list can vary over time as new event types or unsupported event types are added or removed:

```
EM_EV_CS_RULE_VIOLATION
EM_EV_CS_SCORE
EM_EV_JOB_STATUS_CHANGE
EM_EV_METRIC_ALERT
EM_EV_METRIC_ERROR
EM_EV_MEXT_UPDATE
EM_EV_MNTR_DISRUPTION
EM_EV_SELFUPDATE
EM_EV_SLA_ALERT
EM_EV_TARGET_AVAILABILITY
EM_EV_USER_REPORTED
EM_EV_ADP_ALERT
EM_EV_APM_KPI_ALERT
EM_EV_JVMDIAG_ALERT
EM_EV_HA_EVENT
```

13.2.2 Management Repository Default Aggregation and Purging Policies for Other Management Data

Besides the metric data and Application Performance Monitoring data, other types of Enterprise Manager data accumulates over time in the Management Repository.

For example, the last availability record for a target will also remain in the Management Repository indefinitely, so the last known state of a target is preserved.

13.2.3 Modifying the Default Aggregation and Purging Policies

The Enterprise Manager default aggregation and purging policies were designed to provide the most available data for analysis while still providing the best performance and least disk-space requirements for the Management Repository. As a result, you should not modify these policies to improve performance or increase your available disk space.

However, if you plan to extract or review the raw or aggregated data using data analysis tools other than Enterprise Manager, you may want to increase the amount of raw or aggregated data available in the Management Repository. You can accomplish this by increasing the retention times for the raw or aggregated data.

A PL/SQL API has been provided to modify the default retention time for the core metric data tables in the Enterprise Manager repository. Table 13–3 shows the default number of partitions retained for each of the three tables and the size of the partitions for each table. The API will allow you to change the number of partitions retained only.

Table 13–3 Core EM Metric Data Tables and Default Data Retention in the Management Repository

Table Name	Partitions Retained	Partition Size
EM_METRIC _VALUES	7	DAY
EM_METRIC_VALUES_HOURLY	32	DAY
EM_METRIC_VALUES_DAILY	24	MONTH

To modify the retention period for any of the above tables, execute the following command:

```
SQL> execute gc_interval_partition_mgr.set_retention('SYSMAN',
<table name>, <number of partitions to retain>);
```

Replace the <table name> by name of table as listed above. The API will allow you to change the number of partitions retained only.

For example, to modify the default retention time for the table EM_METRIC_VALUES from 7 partitions to 14 partitions, follow these steps:

1. Use SQL*Plus to connect to the repository database as the SYSMAN user.
2. Check the current value of the retention periods:

   ```
   SQL> select table_name, partitions_retained
   from em_int_partitioned_tables
   where table_name in ('EM_METRIC_VALUES','EM_METRIC_VALUES_HOURLY','EM_METRIC_
   VALUES_DAILY');

   TABLE_NAME                 PARTITIONS_RETAINED
   -------------------------  -------------------
   EM_METRIC_VALUES                             7
   EM_METRIC_VALUES_HOURLY                     32
   EM_METRIC_VALUES_DAILY                      24
   ```

3. To modify the default retention time for the table EM_METRIC_VALUES from 7 partitions to 14, execute the following command:

   ```
   SQL> execute gc_interval_partition_mgr.set_
   retention('SYSMAN', 'EM_METRIC_VALUES', 14);
   ```

4. Verify that the retention period has been modified:

   ```
   SQL> select table_name, partitions_retained
   from em_int_partitioned_tables
   where table_name in ('EM_METRIC_VALUES','EM_METRIC_VALUES_HOURLY','EM_METRIC_
   VALUES_DAILY');

   TABLE_NAME                PARTITIONS_RETAINED
   ------------------------- -------------------
   EM_METRIC_VALUES                           14
   EM_METRIC_VALUES_HOURLY                    32
   EM_METRIC_VALUES_DAILY                     24
   ```

13.2.4 How to Modify the Retention Period of Job History

Enterprise Manager Cloud Control has a default purge policy which removes all finished job details which are older than 30 days. This section provides details for modifying this default purge policy.

The actual purging of completed job history is implemented via a DBMS_SCHEDULER job that runs once a day in the repository database. When the job runs, it looks for finished jobs that are 'n' number of days older than the current time (value of sysdate in the repository database) and deletes these jobs. The value of 'n' is, by default, set to 30 days.

The default purge policy cannot be modified via the Enterprise Manager console, but it can be changed using SQL*Plus.

To modify this purge policy, follow these steps:

1. Log in to the repository database as the SYSMAN user, via SQL*Plus.
2. Check the current values for the purge policies using the following command:

   ```
   SQL> select * from mgmt_job_purge_policies;
   ```

   ```
   POLICY_NAME                      TIME_FRAME
   -------------------------------- ----------
   SYSPURGE_POLICY                          30
   REFRESHFROMMETALINKPURGEPOLICY            7
   FIXINVENTORYPURGEPOLICY                   7
   OPATCHPATCHUPDATE_PAPURGEPOLICY           7
   ```

   The purge policy responsible for the job deletion is called SYSPURGE_POLICY. As seen above, the default value is set to 30 days.
3. To change the time period, you must drop and recreate the policy with a different time frame:

   ```
   SQL> execute MGMT_JOBS.drop_purge_policy('SYSPURGE_POLICY');
   ```

   ```
   PL/SQL procedure successfully completed.
   ```

   ```
   SQL> execute MGMT_JOBS.register_purge_policy('SYSPURGE_
   POLICY', 60, null);
   ```

   ```
   PL/SQL procedure successfully completed.
   ```

   ```
   SQL> COMMIT;
   ```

   ```
   Commit complete.
   ```

   ```
   SQL> select * from mgmt_job_purge_policies;
   ```

   ```
   POLICY_NAME                      TIME_FRAME
   -------------------------------- ----------
   SYSPURGE_POLICY                          60
   ....
   ```

The above commands increase the retention period to 60 days. The time frame can also be reduced below 30 days, depending on the requirement.

You can check when the purge job will be executed next. The actual time that the purge runs is set to 5 AM repository time and can be verified using these steps:

1. Login to the Repository database using the SYSMAN account.
2. Execute the following command:

   ```
   SQL> select job_name,
              to_char(last_start_date, 'DD-MON-YY HH24:MI:SS') last_run,
              to_char(next_run_date,   'DD-MON-YY HH24:MI:SS') next_run
   from all_scheduler_jobs
   where job_name ='EM_JOB_PURGE_POLICIES';
   ```

```
JOB_NAME             LAST_RUN           NEXT_RUN
-------------------- ------------------ ------------------
EM_JOB_PURGE_POLICIES                   07-SEP-11 05:00:00
```

The schedule can also be verified from the Enterprise Manager console by following these steps:

a. From the **Setup** menu, select **Management Service**, then select **Repository**.

b. Click the **Repository Operations** tab.

c. Find the Next Scheduled Run and Last Scheduled Run information for Job Purge in the list.

Please note that the time of the next scheduled execution of the Job Purge does not represent the cutoff time for the retention period; the cutoff time is determined by the purge policy at the time the Job Purge runs.

13.2.5 DBMS_SCHEDULER Troubleshooting

Enterprise Manager uses the database scheduler (dbms_scheduler) to run various processes in the repository. When the dbms_scheduler is stopped or has insufficient resources to operate, the Enterprise Manager processes do not run or are delayed. The following is a list of common causes that may prohibit the dbms_scheduler from running normally.

Job Queue Processes

The dbms_scheduler uses a separate job-queue process for each job it runs. The maximum number of these processes is controlled by the database parameter, *job_queue_processes*. If all processes are in use, no new jobs will be started.

The following query returns the number of currently running jobs.

```
SQL> SELECT count(*)
FROM dba_scheduler_running_jobs;
```

If the count is close to the setting of *job_queue_processes*, it could mean that Enterprise Manager dbms_scheduler jobs cannot be started (on time). Determine if any of the running dbms_scheduler jobs are stuck and consider increasing the setting for job_queue_processes.

Job Slave Processes

The dbms_scheduler also depends on the setting of the dbms_scheduler property MAX_JOB_SLAVE_PROCESSES. If the number of running dbms_scheduler jobs exceeds this setting, no new jobs will be started. This attribute can be checked using this query.

```
SQL> SELECT value
FROM dba_scheduler_global_attribute
WHERE attribute_name='MAX_JOB_SLAVE_PROCESSES';
```

If the count equals the number of running dbms_scheduler jobs, then determine if any of the running dbms_scheduler jobs are stuck and consult the dbms_scheduler documentation about how to adjust this attribute.

DBMS_SCHEDULER Program Disabled

The dbms_scheduler has an attribute that can be set to disable this feature in the database. When set, the Enterprise Manager dbms_scheduler jobs will not run. To check if this attribute has been set (inadvertently), run this query.

```
SQL> SELECT *
FROM dba_scheduler_global_attribute
WHERE attribute_name = 'SCHEDULER_DISABLED';
```

When a row is returned, the dbms_scheduler is disabled. Execute `dbms_scheduler.set_scheduler_attribute('SCHEDULER_DISABLED', 'FALSE');`

Consult the dbms_scheduler documentation about how to remove this attribute.

Too Many Database Sessions

Each dbms_scheduler job requires two database sessions. When no more sessions are available, Enterprise Manager dbms_scheduler jobs will not run. The following two queries give the maximum number of allowed sessions and the current number of active sessions:

```
SQL> SELECT value
FROM v$parameter
WHERE name='sessions';

SQL> SELECT count(*)
FROM v$session;
```

When the current number of sessions approaches the maximum, then you should determine if any of the sessions are stuck and consult the Oracle Database documentation about how to increase the maximum number of sessions.

Also the high water mark of the number of sessions may indicate that this issue has played a role in the past:

```
SQL> select *
from v$resource_limit
where resource_name = 'sessions' ;
```

If the MAX_UTILIZATION column indicates a value that is close the maximum number of sessions, it could explain why some of the Enterprise Manager dbms_scheduler jobs may not have run (on time) in the past.

Insufficient Memory

The database may not be able to spawn a new job queue process when there is insufficient memory available. The following message in the database alert file, *Unable to spawn jobq slave processes*, in combination with, *(free memory = 0.00M)*, would be indicative of this problem. Please consult the Oracle Database documentation about how to diagnose this memory problem further.

13.3 Dropping and Recreating the Management Repository

This section provides information about dropping the Management Repository from your existing database and recreating the Management Repository after you install Enterprise Manager.

It should be noted here that there is no recovery from the drop command so this action is only appropriate if you are decommissioning an Enterprise Manager site.

13.3.1 Dropping the Management Repository

To recreate the Management Repository, you first remove the Enterprise Manager schema from your Management Repository database. You accomplish this task using the `-action drop` argument to the `RepManager` script, which is described in the following procedure.

To remove the Management Repository from your database:

1. Locate the `RepManager` script in the following directory of the Middleware Home where you have installed and deployed the Management Service:

   ```
   ORACLE_HOME/sysman/admin/emdrep/bin
   ```

   > **Note:** Do not use the database version of the Repmanager script. It does not delete all components which will result in a failed re-installation.
   >
   > Also, RepManager is the only way to drop the repository, so you should be sure not to delete the OMS Home until the drop has successfully completed.

2. At the command prompt, enter the following command:

   ```
   $PROMPT> RepManager repository_host repository_port repository_SID
   -sys_password password_for_sys_account -action drop
   ```

   In this syntax example:

   - *`repository_host`* is the machine name where the Management Repository database is located
   - *`repository_port`* is the Management Repository database listener port address, usually 1521
   - *`repository_SID`* is the Management Repository database system identifier
   - *`password_for_sys_account`* is the password of the SYS user for the database. For example, `change_on_install`
   - `-action drop` indicates that you want to drop the Management Repository, MDS, OPSS, APM, and Schemas. If you use drop, the command drops only the Management Repository.

   > **Note:** The drop command will remove the BI schema (SYSMAN_BIPLATFORM) if it exists.

Alternatively, you can use a connect descriptor to identify the database on the RepManager command line. The connect descriptor identifies the host, port, and name of the database using a standard Oracle database syntax.

For example, you can use the connect descriptor as follows to create the Management Repository:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=host1)(PORT=1521)) (CONNECT_DATA=(SERVICE_NAME=servicename)))"
-sys_password efkl34lmn -action drop
```

> **See Also:** "Establishing a Connection and Testing the Network" in the *Oracle Enterprise Manager Licensing Information* for more information about connecting to a database using connect descriptors.

13.3.2 Recreating the Management Repository

The preferred method for creating the Management Repository is to create the Management Repository during the Enterprise Manager installation procedure, which is performed using Oracle Universal Installer.

> **See Also:** *Oracle Enterprise Manager Cloud Control Installation and Basic Configuration* for information about installing Enterprise Manager.

In the event a repository is dropped, you cannot create the repository alone using the "RepManager create" command. The command will not create all the required users in the repository database.

To create the repository you must completely reinstall Cloud Control.

If you are following recommended best practices by regularly backing up the repository, then you can use a backup of the repository as long as any one of the following is true:

- The primary OMS home is intact
- There is an export/config of the primary OMS
- There is a file system back up of the primary OMS

13.3.2.1 Using a Connect Descriptor to Identify the Management Repository Database

You can use a connect descriptor to identify the database on the `RepManager` command line. The connect descriptor identifies the host, port, and name of the database using a standard Oracle database syntax.

For example, you can use the connect descriptor as follows to create the Management Repository:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=host1)(PORT=1521)) (CONNECT_DATA=(SERVICE_NAME=servicename)))"
-sys_password efkl34lmn -action create
```

> **See Also:** "Establishing a Connection and Testing the Network" in the *Oracle Enterprise Manager Licensing Information* for more information about connecting to a database using a connect descriptor

The ability to use a connect string allows you to provide an address list as part of the connection string. The following example shows how you can provide an address list consisting of two listeners as part of the `RepManager` command line. If a listener on one host becomes unavailable, the second listener can still accept incoming requests:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=
(ADDRESS_LIST=
(ADDRESS=(PROTOCOL=TCP)(HOST=host1)(PORT=1521)
(ADDRESS=(PROTOCOL=TCP)(HOST=host2)(PORT=1521)
(CONNECT_DATA=(SERVICE_NAME=servicename)))"
```

```
-sys_password efkl34lmn -action create
```

> **See Also:** *Oracle Database High Availability Architecture and Best Practices*
>
> *Oracle Enterprise Manager Cloud Control Installation and Basic Configuration*

13.4 Troubleshooting Management Repository Creation Errors

Oracle Universal Installer creates the Management Repository using a configuration step at the end of the installation process. If the repository configuration tool fails, note the exact error messages displayed in the configuration tools window, wait until the other configuration tools have finished, exit from Universal Installer, and then use the following sections to troubleshoot the problem.

13.4.1 Package Body Does Not Exist Error While Creating the Management Repository

If the creation of your Management Repository is interrupted, you may receive the following error when you attempt to create or drop the Management Repository at a later time:

```
SQL> ERROR:
ORA-00604: error occurred at recursive SQL level 1
ORA-04068: existing state of packages has been discarded
ORA-04067: not executed, package body "SYSMAN.MGMT_USER" does not exist
ORA-06508: PL/SQL: could not find program unit being called
ORA-06512: at "SYSMAN.SETEMUSERCONTEXT", line 5
ORA-06512: at "SYSMAN.CLEAR_EMCONTEXT_ON_LOGOFF", line 4
ORA-06512: at line 4
```

To fix this problem, see "General Troubleshooting Techniques for Creating the Management Repository" on page 13-11.

13.4.2 Server Connection Hung Error While Creating the Management Repository

If you receive an error such as the following when you try to connect to the Management Repository database, you are likely using an unsupported version of the Oracle Database:

```
Server Connection Hung
```

To remedy the problem, upgrade your database to the supported version as described in *Oracle Enterprise Manager Cloud Control Installation and Basic Configuration*.

13.4.3 General Troubleshooting Techniques for Creating the Management Repository

If you encounter an error while creating the Management Repository, drop the repository by running the `-drop` argument to the `RepManager` script.

> **See Also:** Section 13.3.1, "Dropping the Management Repository"

If the `RepManager` script drops the repository successfully, try creating the Management Repository again.

If the `RepManager -action drop/drop` fails for any reason, perform the following steps:

1. Apply the Bundle Patch to the 12c OMS home. Note that this step is only applicable to 12.1.0.1 OMS. Refer to My Oracle Support Note 1393173.1: Enterprise Manager Cloud Control Installation Instructions for Bundle Patch 1 and 12.1.0.2 Plug-ins for instructions.

2. Stop the OMS and verify that all the WLS / OMS processes have been stopped in the OMS home:

   ```
   cd <OMS_HOME>/bin
   emctl stop oms -all
   ```

   > **Note:** You should use the -all option so that the Admin Server is stopped as well

   Verify that there are no WLS / OMS processes still running:

   ```
   $ ps -ef | grep EMGC
   $ ps -ef | grep java
   ```

3. Drop the repository objects using the "Repmanager drop" command:

   ```
   cd <OMS_HOME>/sysman/admin/emdrep/bin
   RepManager <database hostname> <database listener port> <database sid> -action
   drop -dbUser sys -dbPassword <sys user password> -dbRole sysdba -mwHome
   <Middleware Home> -mwOraHome <Middleware Home> -oracleHome <OMS Home>
   ```

   For example:

   ```
   RepManager repomachine.domain 1521 orcl -action drop -dbUser sys -dbPassword
   oracle123 -dbRole sysdba -mwHome /home/oracle/Middleware
   -mwOraHome /home/oracle/Middleware -oracleHome /home/oracle/Middleware/oms
   ```

4. Log in to the Repository Database as sys or any DBA user and verify that all the repository objects have been dropped:

   ```
   SQL> select username,account_status from dba_users where username in ('SYSMAN',
   'SYSMAN_MDS','MGMT_VIEW','SYSMAN_BIPLATFORM','SYSMAN_APM','BIP','SYSMAN_
   OPSS','SYSMAN_RO') ;

   SQL> select owner,synonym_name from dba_synonyms where table_owner in
   ('SYSMAN', 'SYSMAN_MDS','MGMT_VIEW','SYSMAN_BIPLATFORM','SYSMAN_
   APM','BIP','SYSMAN_OPSS','SYSMAN_RO') ;

   SQL> select tablespace_name from dba_tablespaces where tablespace_name like
   'MGMT%';

   SQL> select comp_name from SCHEMA_VERSION_REGISTRY;
   ```

   None of the above queries should return any rows. If any of the above queries return any rows, then raise an SR with Oracle Support.

   > **Note:** The above solution is applicable if the OMS is in working condition. If the OMS home is not available or not intact, raise an SR with Oracle Support.

13.5 Cross Platform Enterprise Manager Repository Migration

There are user requirements for migrating an Enterprise Manager repository across servers - same and cross platforms.

The Enterprise Manager repository migration process is not exactly the same as database migration. In the case of Enterprise Manager Repository migration you must take care of Enterprise Manager specific data, options, and pre-requisites for the repository move. You should make sure data integrity is maintained from both the Enterprise Manager and Oracle database perspective.

This raises the need for defining the process that can be followed by end users for successful and reliable migration of repository in minimum time and with maximum efficiency.

The overall strategy for migration depends on:

- The source and target database version
- The amount of data/size of repository
- Actual data to migrate [selective/full migration]

If the source and target is not on release 12*c* then export/import is the only way to get the data migrated cross platform.

More details on cross platform transportable tablespace, data pump, and export/import options can be found at the *Oracle Technology Network* (OTN) or in the *Oracle Database Administrator's Guide*.

13.5.1 Common Prerequisites

The following lists the common prerequisites for a repository migration:

- Source and target database must use the same character set and should be at same version.
- The target database should meet all the pre-requisites for the Enterprise Manager Repository software requirements mentioned in the *Oracle Enterprise Manager Installation Guide*.
- If the source and target database are on release 10gR2 and higher rdbms versions, and provided they are meeting other prerequisites, cross platform transportable database migration can be used for cross platform repository migration.
- You cannot transport a tablespace to a target database in which a tablespace with the same name already exists. However, you can rename either the tablespace to be transported or the destination tablespace before the transport operation.
- To plug a transportable tablespace set into an Oracle Database on a different platform, both databases must have compatibility set to at least Release 10.0.
- Most of the platforms (but not all) are supported for cross-platform tablespace transport. You can query the V$TRANSPORTABLE_PLATFORM view to see the platforms that are supported, and to determine their platform IDs and their endian format (byte ordering).
- Source and Destination host should have Enterprise Manager Management Agent running and configured to the instance which is to be migrated.
- If the target database has an Enterprise Manager repository installed, it should be first dropped using RepManager before target database related steps are carried out.

13.5.2 Methodologies

The following sections discuss two methodologies for a repository migration:

- Cross Platform Transportable Database
- Migration Using Physical Standby

13.5.2.1 Cross Platform Transportable Database

Oracle's transportable database feature allows users to quickly move a user tablespace across Oracle databases. It is the most efficient way to move bulk data between databases. With the cross platform transportable database, you can transport tablespaces across platforms.

Cross platform transportable database allows a database to be migrated from one platform to another (use with Data Pump or Import/Export). The following set of steps for migration using Transportable Database can be used for migrations between same-endian platforms:

1. Verify whether migration is possible on the destination platform from v$db_ transportable_platform.

   ```
   SQL> select platform_name from v$db_transportable_platform;
   ```

   You may see a list of platforms similar to the list below:

   ```
   Microsoft Windows IA (32-bit)
   Linux IA (32-bit)
   HP Tru64 UNIX
   Linux IA (64-bit)
   HP Open VMS
   Microsoft Windows IA (64-bit)
   Linux x86 64-bit
   Microsoft Windows x86 64-bit
   Solaris Operating System (x86)
   HP IA Open VMS
   Solaris Operating System (x86-64)
   ```

2. Verify that the external tables and files exist in the database.

   ```
   SQL> set serveroutput on
   SQL> declare x boolean;
     2  begin x := dbms_tdb.check_external;
     3  end;
     4  /
   ```

   The following output results:

   ```
   The following external tables exist in the database:
   SH.SALES_TRANSACTIONS_EXT
   The following directories exist in the database:
   SYS.SUBDIR, SYS.SS_OE_XMLDIR, SYS.MEDIA_DIR, SYS.LOG_FILE_DIR,
   SYS.DATA_FILE_DIR, SYS.XMLDIR, SYS.DATA_PUMP_DIR, SYS.ORACLE_OCM_CONFIG_DIR
   The following BFILEs exist in the database:
   PM.PRINT_MEDIA
   ```

   Enter the following command:

   ```
   SQL> select directory_path from dba_directories;
   ```

   The following output results:

   ```
   DIRECTORY_PATH
   --------------------------------------------------------------------------------
   ```

```
-
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/order_
entry//2002/Sep
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/order_entry/
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/log/
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/sales_history/
/ade/b/1191423112/oracle/rdbms/xml
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/product_media/
/home/oracle/app/oracle/admin/orcl/dpdump/
/home/oracle/app/oracle/product/11.2.0/dbhome_1/ccr/state

8 rows selected.
```

Enter the following command:

```
SQL> select directory_path||'/'||location External_file_path
from dba_directories a, dba_external_locations b where
a.directory_name=b.directory_name;
```

The following output results:

```
EXTERNAL_FILE_PATH
----------------------------------------------------------------------------
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/sales_
history//sale1v3.dat
```

Enter the following command:

```
SQL> @tgt_get_bfile_dirs.sql
```

The following output results:

```
The following directories contain external files for BFILE columns
Copy the files within these directories to the same path on the target system

/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/product_media/

There are 1 directories, 4 total BFILEs

SQL> @tgt_get_bfiles.sql
External files for BFILE column AD_GRAPHIC in table PM.PRINT_MEDIA
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/product_
media//monitor.jpg
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/product_
media//mousepad.jpg
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/product_
media//keyboard.jpg
/home/oracle/app/oracle/product/11.2.0/dbhome_1/demo/schema/product_
media//modem.jpg
```

3. Stop the OMS.

   ```
   emctl stop oms -all
   ```

   Enter the following SQL commands:

   ```
   SQL> shutdown immediate
   Database closed.
   Database dismounted.
   ORACLE instance shut down.

   SQL> startup mount;
   ORACLE instance started.
   ```

```
Total System Global Area 1473089536 bytes
Fixed Size                  1336596 bytes
Variable Size            1124076268 bytes
Database Buffers          335544320 bytes
Redo Buffers               12132352 bytes
Database mounted.
```

4. Open the database in read-only mode.

   ```
   SQL> alter database open read only;
   ```

   Enter the following SQL commands:

   ```
   SQL> set serveroutput on
   SQL> declare
     2  retcode boolean;
     3  begin
     4  retcode := dbms_tdb.check_db('Linux IA (64-bit)',dbms_tdb.skip_none);
     5  end;
     6  /

   SQL> declare
     2  retcode boolean;
     3  begin
     4  retcode := dbms_tdb.check_db('Linux x86 64-bit',dbms_tdb.skip_none);
     5  end;
     6  /

   PL/SQL procedure successfully completed.
   ```

5. Generate the RMAN conversion script.

   ```
   [oracle]$ ./rman
   Recovery Manager: Release 11.2.0.1.0 - Production on Fri dd-mm-yy 12:10:29 2012
   Copyright (c) 1982, 2009, Oracle and/or its affiliates.  All rights reserved.
   RMAN> connect target /
   connected to target database: ORCL (DBID=1308105793)
   RMAN> convert database on target platform
   2> convert script '/tmp/convert_mydb.rman'
   3> transport script '/tmp/transport_mydb.sql'
   4> new database 'mydb'
   5> format '/tmp/mydb%U'
   6> db_file_name_convert '/home/oracle/app/oracle/oradata/mydb/','/tmp';

   Starting conversion at source at dd-mm-yy
   using target database control file instead of recovery catalog
   allocated channel: ORA_DISK_1
   channel ORA_DISK_1: SID=135 device type=DISK

   External table SH.SALES_TRANSACTIONS_EXT found in the database

   Directory SYS.SUBDIR found in the database
   Directory SYS.SS_OE_XMLDIR found in the database
   Directory SYS.MEDIA_DIR found in the database
   Directory SYS.LOG_FILE_DIR found in the database
   Directory SYS.DATA_FILE_DIR found in the database
   Directory SYS.XMLDIR found in the database
   Directory SYS.DATA_PUMP_DIR found in the database
   Directory SYS.ORACLE_OCM_CONFIG_DIR found in the database

   BFILE PM.PRINT_MEDIA found in the database
   ```

```
User SYS with SYSDBA and SYSOPER privilege found in password file
channel ORA_DISK_1: starting to check datafiles
input datafile file number=00001
name=/home/oracle/app/oracle/oradata/orcl/system01.dbf
channel ORA_DISK_1: datafile checking complete, elapsed time: 00:00:00
channel ORA_DISK_1: starting to check datafiles
input datafile file number=00002
name=/home/oracle/app/oracle/oradata/orcl/sysaux01.dbf
channel ORA_DISK_1: datafile checking complete, elapsed time: 00:00:00
channel ORA_DISK_1: starting to check datafiles
input datafile file number=00007
name=/home/oracle/app/oracle/oradata/orcl/mgmt.dbf
channel ORA_DISK_1: datafile checking complete, elapsed time: 00:00:00
channel ORA_DISK_1: starting to check datafiles
input datafile file number=00003
name=/home/oracle/app/oracle/oradata/orcl/undotbs01.dbf
channel ORA_DISK_1: datafile checking complete, elapsed time: 00:00:00
channel ORA_DISK_1: starting to check datafiles
input datafile file number=00008
name=/home/oracle/app/oracle/oradata/orcl/mgmt_ad4j.dbf
channel ORA_DISK_1: datafile checking complete, elapsed time: 00:00:00
channel ORA_DISK_1: starting to check datafiles
input datafile file number=00005
name=/home/oracle/app/oracle/oradata/orcl/example01.dbf
channel ORA_DISK_1: datafile checking complete, elapsed time: 00:00:00
channel ORA_DISK_1: starting to check datafiles
input datafile file number=00006
name=/home/oracle/app/oracle/oradata/orcl/mgmt_depot.dbf
channel ORA_DISK_1: datafile checking complete, elapsed time: 00:00:00
channel ORA_DISK_1: starting to check datafiles
input datafile file number=00004
name=/home/oracle/app/oracle/oradata/orcl/users01.dbf
channel ORA_DISK_1: datafile checking complete, elapsed time: 00:00:00
Edit init.ora file /tmp/init_mydb00nbs6dl_1_0.ora. This PFILE will be used to
create the database on the target platform
Run RMAN script /tmp/convert_mydb.rman on target platform to convert datafiles
Run SQL script /tmp/transport_mydb.sql on the target platform to create
database
To recompile all PL/SQL modules, run utlirp.sql and utlrp.sql on the target
platform
To change the internal database identifier, use DBNEWID Utility
Finished conversion at source at dd-mm-yy
```

6. Copy all the required files to a temporary location and mount on the target machine.

```
convert_mydb.rman
init_mydb.ora
transport_mydb.sql (and other data files listed in rman script [convert_
mydb.rman] and redolog files)
```

7. Execute the scripts generated in Step 5 on the target machine.

   The RMAN script contains convert datafile commands. The SQL script contains control file creation, invalidating objects, and recompiling objects. On the target machine, execute the following:

```
RMAN> connect target /
```

```
RMAN> @/home/oracle/migrate/convert_mydb.rman
```

8. Ensure the database is up and running and the database is registered with the listener.

   ```
   RMAN> STARTUP NOMOUNT PFILE = '/home/oracle/migrate/init_
   mydb00nbs6dl_1_0.ora'; database is already started
   ```

9. Start the OMS to ensure the admin server is up.

   ```
   [oracle]$ ./emctl status oms
   ```

   ```
   [oracle]$ ./emctl start oms
   ```

10. Stop the OMS.

    ```
    [oracle]$ ./emctl stop oms
    ```

11. Update repository database connection details.

    ```
    [oracle]$ ./emctl config oms -store_repos_details -repos_
    conndesc "(DESCRIPTION=(ADDRESS_
    LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=evildead.idc.oracle.com)(PO
    RT=1521)))(CONNECT_DATA=(SID=mydb)))" -repos_user SYSMAN
    -repos_pwd Oracle123
    ```

    If there are multiple Oracle Management Services in this environment, run this store_repos_details command on all of them.

12. Restart the OMS.

    ```
    [oracle]$ ./emctl start oms
    ```

    ```
    [oracle]$ ./emctl status oms
    ```

    ```
    Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.4.0
    Copyright (c) 1996, 2013 Oracle Corporation.  All rights reserved.
    WebTier is Up
    Oracle Management Server is Up
    ```

13. Relocate Management Services and the Repository target.

13.5.2.2 Migration Using Physical Standby

The following steps describe the process you can use to migrate a repository using Physical Standby. This method can be used when the source and target platforms are supported. See My Oracle Support Note:413484.1 for details of which platform combinations are supported.

1. Install the database ORACLE_HOME on the target machine. The binaries should be the same version as the source.

   If the target machine is Windows, install and configure CYGWIN on the Windows box for Management Agent deployment.

2. Deploy the Management Agent to the target server.
3. Create a Physical Standby as described in the Data Guard documentation.
4. Configure the Data Guard broker as described in the Data Guard Broker documentation.
5. Shutdown the OMS.

   ```
   emctl stop oms -all
   ```

6. Check the OMS connect descriptor.

   ```
   ./emctl config oms -list_repos_details
   ```

7. Switchover the database using dgmgrl.

   Use the following commands:

   ```
   DGMGRL> switchover to target_db
   verify
   show configuration
   show database target_db
   show database source_db
   ```

8. Start the OMS admin server.

   ```
   emctl start oms -admin_only
   ```

9. Update connect descriptor to point to the Standby Database.

   ```
   eemctl config oms -store_repos_details -repos_conndesc
   "(DESC= )" -repos_user sysman
   ```

   ```
   [oracle]$ ./emctl config oms -store_repos_details -repos_conndesc
   "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=sample2.us.company.com)(PORT=1521))(
   CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=test_win)))" -repos_user sysman
       Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.4.0
       Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
       Enter Repository User's Password :
       Successfully updated datasources and stored repository details in
   Credential Store.
   ```

   If there are multiple Oracle Management Services in this environment, run this store_repos_details command on all of them.

10. Stop all the Oracle Management Services.

    ```
    emctl stop oms -all
    ```

11. Start the OMS.

    ```
    emctl start oms
    ```

12. Relocate Oracle Management Services and the Repository.

    ```
    emctl config emrep -agent <agent_name> -conn_desc
    ```

    ```
    [oracle]$ ./emctl config emrep -agent sample2.us.company.com:3872 -conn_desc
    "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=sample2.us.company)(PORT=1521))(CONN
    ECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=test_win)))"
    Oracle Enterprise Manager Cloud Control 12c Release 12.1.0.4.0
    Copyright (c) 1996, 2013 Oracle Corporation. All rights reserved.
    Please enter repository password:
    Enter password :
    Login successful
    Moved all targets from sample.us.company.com:3872 to
    sample2.us.company.com:3872
    Command completed successfully!
    Enter password :
    Login successful
    Moved all targets from sample.us.company.com:3872 to
    sample2.us.company.com:3872
    Command completed successfully!
    ```

13. Create a backup of the OMS (on the OMS where the Admin server is running).

    ```
    $ <OMS_HOME>/bin/emctl exportconfig oms [-sysman_pwd <sysman
    password>]
    ```

Specify the directory in which to store backup file

```
[-dir <backup dir>]
```

Specify the following parameter if the OMS was installed using a virtual hostname (using *ORACLE_HOSTNAME=<virtual_hostname>*)

```
[-keep_host]
```

13.5.3 Post Migration Verification

These verification steps should be carried out post migration to ensure that the migration was completely successful:

- Verify any discrepancy in objects by comparing source and target databases through Enterprise Manager.
- Verify the migrated database through Enterprise Manager to determine whether the database is running without any issues.
- Verify the repository operations, dbms jobs and whether any management system errors are reported.
- Verify that all Enterprise Manager functionalities are working correctly after the migration.
- Make sure Management Services and the Repository target is properly relocated by verifying it through Enterprise Manager.

14

Updating Cloud Control

The Self Update feature allows you to expand Enterprise Manager's capabilities by updating Enterprise Manager components whenever new or updated features become available. Updated plug-ins are made available via the Enterprise Manager Store, an external site that is periodically checked by Enterprise Manager Cloud Control to obtain information about updates ready for download.

This chapter contains the following sections:

- Using Self Update
- Setting Up Self Update
- Applying an Update
- Accessing Informational Updates
- Acquiring or Updating Management Agent Software

14.1 Using Self Update

The Self Update feature is accessed via the Self Update home page, a common dashboard used to obtain information about new updates and a common workflow to review, download and apply the updates. The Self Update console frees you from having to monitor multiple channels to get informed about new updates that are available from Oracle. The Self Update console automatically informs you whenever new updates are made available by Oracle. Only those updates that are applicable to your site are shown, eliminating the need to wade through unrelated updates.

14.1.1 What Can Be Updated?

Specific updates authored by Oracle that are usually bundled with specific Cloud Control releases can be updated via Self Update. Some examples are Oracle authored Management Plug-ins or Deployment Procedures. In general, Oracle-supplied entities are read-only. You can create a copy and customize the copy as per your needs but you cannot modify the original Oracle-supplied entity.

These entities can also be published on Oracle Web sites such as Oracle Technology Network (OTN) and My Oracle Support (MOS). You can download and import the entity archive into their Cloud Control deployment using specific import features provided by the updatable entity.

Entity Types That Can Be Updated

Examples of updatable entity types are:

- Management Agents

- Management Plug-ins
- Management Connectors
- Database Profiles and Gold Images
- Application Server Profiles and Gold Images
- Provisioning Bundles
- Enterprise Manager Deployment Prerequisite Checks
- Compliance Content
- Diagnostic Checks

14.2 Setting Up Self Update

Before you can use the Self Update feature, you must satisfy these prerequisites:

- My Oracle Support credentials have been set up using the SYSMAN user. This is required to enable entities to be downloaded from the My Oracle Support site.
- The Software Library (also known as the local store) has been configured. Updates are downloaded to this local store before being deployed into Cloud Control.

Review the following sections for instructions on setting up Self Update:

- Setting Up Enterprise Manager Self Update Mode
- Assigning Self Update Privileges to Users
- Setting Up the Software Library
- Setting My Oracle Support Preferred Credentials
- Registering the Proxy Details for My Oracle Support
- Setting Up the EM CLI Utility (Optional)

14.2.1 Setting Up Enterprise Manager Self Update Mode

In order to set up or modify the Enterprise Manager Self Update feature, you must have Enterprise Manager Super Administrator privileges.

1. Log in to Enterprise Manager as an administrator with Super Administrator privileges.
2. From the **Setup** menu, select **Extensibility**, then select **Self Update**. The Self Update console appears with the default setup displayed.
3. From the **General** status area, click the **Connection Mode** status to set either offline or online mode. Enterprise Manager takes you to the Patching Setup page to specify online and offline settings.

   Important: When Cloud Control runs in Online mode, it does not upload any data to MOS. It only uses MOS to download the latest updates.

4. Once the desired connection mode has been selected, return to the Self Update console.

   From here you can select entity types and schedule updates from the Enterprise Manager Update Store.

14.2.2 Assigning Self Update Privileges to Users

Enterprise Manager administrators must have the requisite privileges to use the Self Update feature. The Enterprise Manager Super Administrator must assign the following Self Update roles/privileges to these administrators:

- *View any Enterprise Manager Update*–User can view the Self Update console and can monitor the status of download and apply jobs.
- *Self Update Administrator*–User can schedule download and apply jobs. User can also suppress/unsuppress updates. This privilege implicitly contains the View any Enterprise Manager Update privilege.
- *EM_INFRASTRUCTURE_ADMIN*–User can perform all self update operations. This role implicitly contains the *Self Update Administrator* privilege.

By default, the Super Administrator will be granted EM_INFRASTRUCTURE_ADMIN privilege.

To assign Self Update privileges to regular Enterprise Manager administrators:

1. From the **Setup** menu, select **Security**, then select **Administrators**.
2. Select an administrator and click **Edit**.
3. From the Roles page, assign the appropriate Self Update roles.

14.2.3 Setting Up the Software Library

The Software Library is a repository that stores software entities such as software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. In addition to storing them, it also enables you to maintain versions, maturity levels, and states of these software entities. In the context of applying updates, it is the "local store" that entities are downloaded to before deployment.

If the Software Library is not already set up in your environment, see Chapter 8, "Configuring Software Library," for instructions on the various ways you can configure the Software Library.

14.2.4 Setting My Oracle Support Preferred Credentials

To set the preferred credentials that must be used by the OMS to connect to My Oracle Support (MOS), follow these steps:

1. From the **Setup** menu, select **My Oracle Support,** then select **Set Credentials.**
2. Specify the user name and the password.
3. Click **Apply.**

14.2.5 Registering the Proxy Details for My Oracle Support

Cloud Control uses the Internet connectivity you have on the OMS host to connect to My Oracle Support. However, if you have a proxy server set up in your environment, then you must register the proxy details. You can register the proxy details for My Oracle Support using the My Oracle Support Proxy Settings page.

Note: Beginning with Enterprise Manager Cloud Control 12c Release 3 (12.1.0.3), My Oracle Support accesses support.oracle.com directly. This means that you must provide network access to this URL, or grant proxy access to it from any client that will access My Oracle Support.

To register the proxy details for My Oracle Support (MOS), follow these steps:

1. From the **Setup** menu, select **Proxy Settings,** then select **My Oracle Support.**
2. If you want the OMS to connect to MOS directly, without using a proxy server, follow these steps:
    1. Select **No Proxy.**
    2. Click **Test** to test if the OMS can connect to MOS directly.
    3. If the connection is successful, click **Apply** to save the proxy settings to the repository.
3. If you want the OMS to connect to MOS using a proxy server, follow these steps:
    1. Select **Manual proxy configuration.**
    2. Specify the proxy server host name for **HTTPS** and an appropriate port value for **Port.**
    3. If the specified proxy server has been configured using a security realm, login credentials, or both, select **Password/Advanced Setup,** then provide values for **Realm, User Name,** and **Password.**
    4. Click **Test** to test if the OMS can connect to MOS using the specified proxy server.
    5. If the connection is successful, click **Apply** to save the proxy settings to the repository.

Note:

- If you are using a proxy server in your setup, ensure that it allows connectivity to aru-akam.oracle.com, ccr.oracle.com, login.oracle.com, support.oracle.com, and updates.oracle.com.

  NTLM (NT LAN Manager) based Microsoft proxy servers are not supported. If you are using an NTLM based Microsoft proxy server, to enable access to the above sites, add the above URLs to the Unauthenticated Sites Properties of the proxy server.
- The MOS proxy server details specified on the MOS Proxy Settings page apply to all OMSes in a multi-OMS environment.

14.2.6 Setting Up the EM CLI Utility (Optional)

If you plan to apply software updates in offline mode, you will need to use the Enterprise Manager Command Line Utility, or EM CLI, to import entity archives for deployment to Enterprise Manager.

EM CLI is set up on OMS out-of-box. If you need to set up EM CLI on another machine managed by Enterprise Manager, a page is provided in the Cloud Control console with instructions on setting up EM CLI. Access the page by appending `/console/emcli/download` to the URL used to access the Cloud Control console:

```
https://emcc_host:emcc_port/em
```

For example:

```
https://emcc_host:emcc_port/em/console/emcli/download
```

14.3 Applying an Update

The process for applying updates is essentially as follows:

- Check for the latest updates available from Oracle.
- Download the updates you want to apply to the Software Library.
- Apply the update.

Review the following sections to learn how to apply an update:

- Applying an Update in Online Mode
- Applying an Update in Offline Mode

14.3.1 Applying an Update in Online Mode

Updates must be downloaded to the Software Library (the local store) before they can be applied. You can review the latest available updates from the Self Update console.

Note that Enterprise Manager must have access to the Enterprise Manager Store via the Internet to download available updates. If this access is not possible, you can download entities in offline mode. See Section 14.3.2, "Applying an Update in Offline Mode" for details.

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. Click **Check Updates** to submit a job to check for new updates from Oracle. Click **OK** to close the confirmation message.
3. When the job completes, select the desired entity type, then select **Open** from the **Actions** menu. The entity type page appears.
4. Select an update from the list of available updates.
5. Click **Download**. The Schedule Download dialog appears.
6. Select when to download the update. Note that multiple downloads can be scheduled simultaneously.

   The following options are available:

   - Immediately
   - Later (specified time)
   - Whether or not to send a notification when the download is complete
7. Click **Select**. An Enterprise Manager job is created to download the update to the Software Library.

   Enterprise Manager starts downloading the archive from the Oracle Enterprise Manager store. Wait for the download to complete. (When in offline mode the system starts reading from the specified location.)

When the download is complete, Enterprise Manager displays the Confirmation page.

Note: The page is not refreshed automatically. Click the refresh icon to view the updated download status.

8. Once an entity has been downloaded to the Software Library, it is ready to be applied to your installation. Select an update from the list whose status is **Downloaded**, then click **Apply**.

   Note that the application process varies according to the entity type:

   - For connectors, diagnostic checks, and compliance content, clicking **Apply** will install the update to Enterprise Manager. No further action is required.
   - For plug-ins, you will be redirected to the plug-in deployment page.
   - For provisioning bundles, you will need to exit the Enterprise Manager console, run Opatch and other commands via a terminal, and then restart the OMS.

14.3.2 Applying an Update in Offline Mode

Under certain circumstances, such as in high security environments, an active Internet connection between Enterprise Manager and the Enterprise Manager Update Store may not be available. In such situations, the Self Update feature can be used in offline mode.

The update process still requires that a computer exist at your site that has Internet access, as a connection to the Enterprise Manager Update Store is still required to obtain the updates. Update files from this computer can then be transferred to a computer behind your firewall.

The generic offline mode update procedure is as follows:

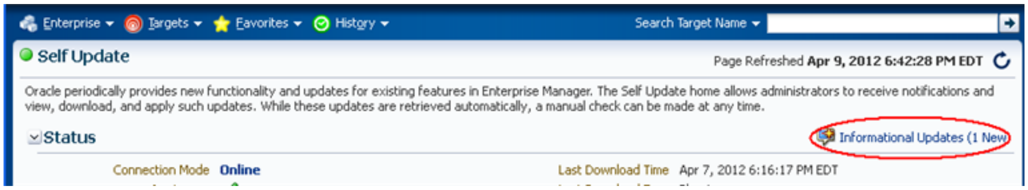
1. Ensure that Cloud Control is set to offline mode. From the **Setup** menu, select **Provisioning and Patching**, then select Offline Patching.
2. Change the setting for Connection to **Offline**.
3. Click **Check Updates** on the Self Update home page. A message is displayed that contains the URL to be accessed to download a catalog of all updates.
4. From an Internet-enabled computer, download the catalog file using the aforementioned URL.
5. Copy the downloaded file to the Oracle Management Service host or the Management Agent host you will deploy the update to.
6. Run the `emcli import_update_catalog` command to import the file into the Oracle Management Service instance or the Management Agent you want to update.
7. Review the update from Self Update Home and click **Download** in the **Actions** menu. A message displays with a URL and instructions.
8. Click **Apply** in the **Actions** menu to apply the update.

14.4 Accessing Informational Updates

The Self Update feature also serves as a news feed, providing new product announcements, news stories, industry updates, and any number of other items of interest to the Oracle community. These informational updates occur on an ad hoc basis and typically include useful links where you can obtain additional information and download items.

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. On the Self Update page, click the **Informational Updates** link at the top-right corner, as shown in Figure 14–1. The link includes the number of new updates. A number appears only if there are new (unread) updates.

Figure 14–1 Informational Updates Link on the Self Update Home Page



Page Refreshed **Apr 9, 2012 6:42:28 PM EDT**

Oracle periodically provides new functionality and updates for existing features in Enterprise Manager. The Self Update home allows administrators to receive notifications and view, download, and apply such updates. While these updates are retrieved automatically, a manual check can be made at any time.

Connection Mode **Online**

Last Download Time Apr 7, 2012 6:16:17 PM EDT

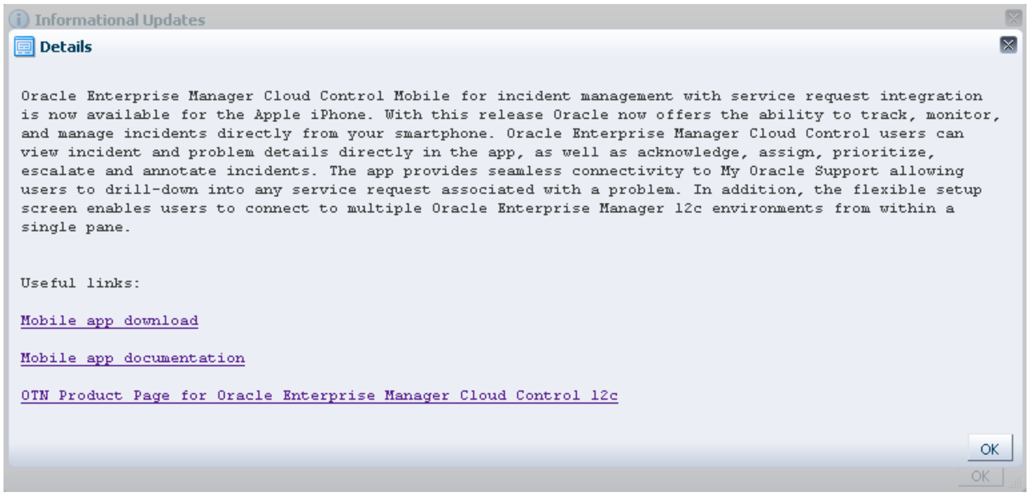
   The Informational Updates dialog opens.

3. Select an update notification in the table and click **Details**.

   A popup appears describing the new product and listing applicable links.

   Figure 14–2 shows the informational update announcing availability of Enterprise Manager Cloud Control Mobile, a new iPhone app that enables you to connect to Enterprise Manager remotely. Notice in this case that the announcement includes a link to iTunes where you can go to download the app.

Figure 14–2 Informational Update for Mobile App



```
Oracle Enterprise Manager Cloud Control Mobile for incident management with service request integration
is now available for the Apple iPhone. With this release Oracle now offers the ability to track, monitor,
and manage incidents directly from your smartphone. Oracle Enterprise Manager Cloud Control users can
view incident and problem details directly in the app, as well as acknowledge, assign, prioritize,
escalate and annotate incidents. The app provides seamless connectivity to My Oracle Support allowing
users to drill-down into any service request associated with a problem. In addition, the flexible setup
screen enables users to connect to multiple Oracle Enterprise Manager 12c environments from within a
single pane.


Useful links:

Mobile app download

Mobile app documentation

OTN Product Page for Oracle Enterprise Manager Cloud Control 12c
```

4. Click **OK** to close the details display and return to the table of announcements.

   By default, the table displays only unread announcements. You can choose to display all or only read announcements. You can also toggle selected items between read and unread states. Note that if you mark an item as read, you are doing so for all users. A warning to this effect appears.

14.5 Acquiring or Updating Management Agent Software

Management Agent software for the various platforms (operating systems) supported by Enterprise Manager Cloud Control can be downloaded to the Software Library using the Self Update console. Once a Management Agent is persisted to the Software Library, it can be installed on host machines that you want to bring under Cloud Control management using the Add Host Targets wizard.

For instructions on obtaining Management Agent software in both online and offline modes, see the section "*Meeting Management Agent Software Prerequisites*" in the *Oracle® Enterprise Manager Cloud Control Basic Installation Guide*.

15 Configuring a Software Library

This chapter describes how you can configure a new Software Library using Cloud Control console, the various users and the privileges required to access the Software Library, and finally how to maintain an existing Software Library in the Enterprise Manager Cloud Control environment.

> **Note:** Oracle strongly recommends that you select the **Configure Oracle Software Library** option and configure it at the time of installation so that the installer can automatically configure it for you, thus saving your time and effort. For more information on this, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*
>
> However, if you have not already configured the Software Library, you can do so from the Enterprise Manager Cloud Control Console as described in this chapter.

In particular, this chapter covers the following:

- Overview of Software Library
- Users, Roles, and Privileges
- What's New in Software Library
- Performing Software Library Tasks Using EM CLI Verbs or in Graphical Mode
- Software Library Storage
- Prerequisites for Configuring Software Library
- Configuring Software Library Storage Location
- Configuring Software Library on a Multi-OMS System
- Using Software Library Entities
- Tasks Performed Using the Software Library Home Page
- Maintaining Software Library

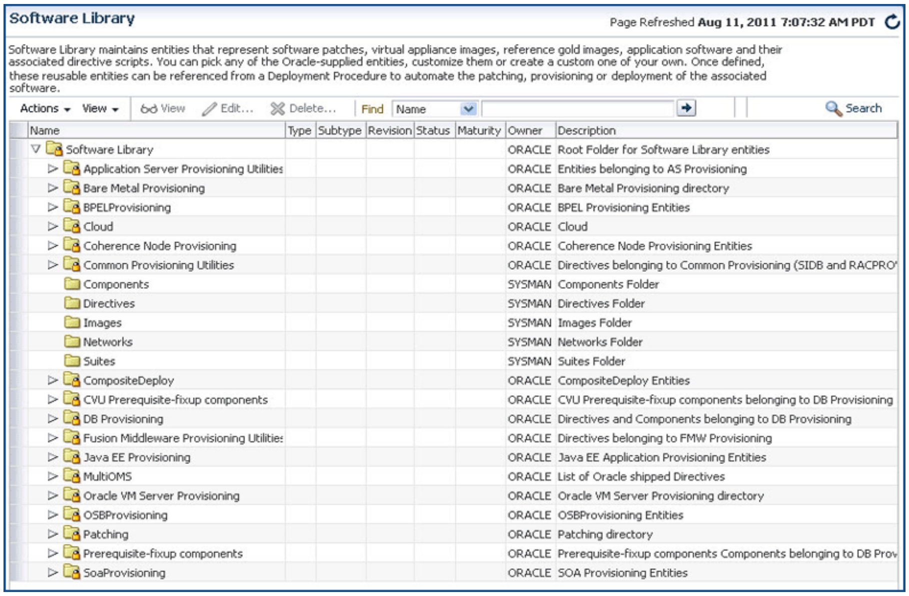
15.1 Overview of Software Library

Oracle Software Library (Software Library) is one of the core features offered by Enterprise Manager Cloud Control. Technically, it is a repository that stores software entities such as software patches, virtual appliance images, reference gold images, application software, and their associated directive scripts. In addition to storing them, it also enables you to maintain versions, maturity levels, and states of these software entities.

To access the Software Library console page, from the **Enterprise** menu, select **Provisioning and Patching**, then click **Software Library.** On the Software Library home page, as shown in Figure 15–1, there are two types of folders: Oracle-owned folders (marked by a lock symbol) and User-owned folders.

Oracle-owned folders and their contents (including other subfolders and entities) ship with the product by default, and appear on the Software Library home page after Software Library is configured. User-owned folders are logical top level folders that the user creates to organize the entities that he/she intends to create.

Figure 15–1 Software Library Console



Software Library

Page Refreshed **Aug 11, 2011 7:07:32 AM PDT**

Software Library maintains entities that represent software patches, virtual appliance images, reference gold images, application software and their associated directive scripts. You can pick any of the Oracle-supplied entities, customize them or create a custom one of your own. Once defined, these reusable entities can be referenced from a Deployment Procedure to automate the patching, provisioning or deployment of the associated software.

Name	Type	Subtype	Revision	Status	Maturity	Owner	Description
Software Library						ORACLE	Root Folder for Software Library entities
Application Server Provisioning Utilities						ORACLE	Entities belonging to AS Provisioning
Bare Metal Provisioning						ORACLE	Bare Metal Provisioning directory
BPELProvisioning						ORACLE	BPEL Provisioning Entities
Cloud						ORACLE	Cloud
Coherence Node Provisioning						ORACLE	Coherence Node Provisioning Entities
Common Provisioning Utilities						ORACLE	Directives belonging to Common Provisioning (SIDB and RACPRO'
Components						SYSMAN	Components Folder
Directives						SYSMAN	Directives Folder
Images						SYSMAN	Images Folder
Networks						SYSMAN	Networks Folder
Suites						SYSMAN	Suites Folder
CompositeDeploy						ORACLE	CompositeDeploy Entities
CVU Prerequisite-fixup components						ORACLE	CVU Prerequisite-fixup components belonging to DB Provisioning
DB Provisioning						ORACLE	Directives and Components belonging to DB Provisioning
Fusion Middleware Provisioning Utilitie:						ORACLE	Directives belonging to FMW Provisioning
Java EE Provisioning						ORACLE	Java EE Application Provisioning Entities
MultiOMS						ORACLE	List of Oracle shipped Directives
Oracle VM Server Provisioning						ORACLE	Oracle VM Server Provisioning directory
OSBProvisioning						ORACLE	OSBProvisioning Entities
Patching						ORACLE	Patching directory
Prerequisite-fixup components						ORACLE	Prerequisite-fixup components Components belonging to DB Prov
SoaProvisioning						ORACLE	SOA Provisioning Entities

The Software Library Page facilitates storage of Enterprise Manager entities. For example,

- Self Update entities like plug-ins, connectors, DB workload, and so on.
- Provisioning and Patching entities like gold images, application archives, perl/shell scripts, and so on.

Advantages:

- Software Library supports patching and provisioning in Online mode and Offline mode. For example, if database patches cannot be downloaded directly from *My Oracle Support*, you can download them separately, and stage them from Software Library for offline deployment.
- Starting with Enterprise Manager Cloud Control 12c, Referenced File Locations are supported, which means that the Software Library allows you to leverage your organizations existing IT infrastructure (like file servers, web servers, or storage systems) to stage the files to host targets as part of a provisioning or patching activity.
- Software Library allows you to organize the entities, which basically refer to the software binaries or directive scripts in your enterprise, into logical folders for efficient management.

From the Software Library Console page, you can perform the following tasks:

- Configure Software Library Storage, see Section 15.7, "Configuring Software Library Storage Location" for more information.
- Create Software Library Entities. For example, Creating a Generic Component, Creating Directives, and so on.
- Manage Software Library Entities. For example, Viewing Entities, Editing Entities, Deleting Entities, Searching Entities, and so on.

15.2 Users, Roles, and Privileges

By default, all the Software Library folders and entities that ship with the product are viewable by all the Enterprise Manager users. Fine grained privileges provide a way to control user access to the different entities in the Software Library. Administrators by default do not have any Software Library privileges, it is for the Super Administrator to grant access, privileges to an Administrator.

> **Note:** To run any procedure on a Windows host which involves executing some Software Library entities (for example, directive scripts), you ***(the Windows user)*** must be granted the following privileges:
>
> - Act as part of the operating system
> - Adjust memory quotas for a process
> - Logon as batch job
> - Replace a process level token
>
> If not, the execution of the directive steps in the procedure may fail.

Software Library users roles can be broadly classified as:

- **Designers** are administrators who perform design time tasks like setting up Software library, migrating entities, granting privileges to the Operators, deleting entities, and so on. They can perform both the design time activities, and run-time activities that the Operator can perform. Designers in Enterprise Manager Cloud Control can be granted Super Administrator role or the `EM_PROVISIONING_DESIGNER` role which allows him to create and maintain any Software Library entity.
- **Operators** are administrators who can perform run-time activities like deleting entities, changing the maturity status, and so on. Operators are typically granted roles like `EM_PROVISIONING_OPERATOR` or `EM_PATCH_OPERATOR` and so on.

Any Enterprise Manager user requires, at the very least, a view privilege on an entity for the entity to be visible on the Software Library Home page. Users will not be able to see this entity until the Super Administrator or the owner of the entity grants them at least a view privilege on the entity.

> **Note:** All the folders and entities that ship with the product also known as the Oracle-owned entities, by default are viewable by all the Enterprise Manager users.

Administrator by default do not have any Software Library privileges, it is for the Super Administrator, to grant access, privileges to an Administrator. Table 15–1 describes all the available Software Library privileges that can be granted to a user or role.

Users and roles can be granted privileges on specific entities by the owner of the entity or the Super Administrator. For more details, see *Oracle Enterprise Manager Administrator's Guide for Software and Server Provisioning and Patching.*

Table 15–1 Software Library Privileges for Administrators

Resource Type	Description
View any Template Entity	Ability to view any Template Entity
Export Any Software Library Entity	Ability to export any Software entity
Edit any Software Library Entity	Ability to edit any Software Library entity
Manage Any Software Library Entity	Ability to create, view, edit, and delete any Software Library entity
Import Any Software Library Entity	Ability to import any Software Library entity
Create Any Software Library Entity	Ability to create any Software Library entity
View Any Software Library Entity	Ability to view any Software Library entity
View Any Assembly Entity	Ability to view any Assembly entity
Grant Any Entity Privilege	Ability to grant view, edit, and delete privileges on any Software Library entity.This privilege is required if the user granting the privilege on any entity is not a Super Administrator or owner of the entity.

Table 15–2 describes all the primary users of Software Library, and their associated privileges:

Table 15–2 Roles and Privileges

Role	Software Library Privileges
Super Administrator	All Software Library Privileges
`EM_PROVISIONING_DESIGNER` (Designer)	Create Any Software Library Entity
`EM_PROVISIONING_OPERATOR` (Operator)	View Any Software Library Entity
`EM_PATCH_OPERATOR`	Create Any Software Library Entity View Any Software Library Entity
`EM_USER` (Administrator)	Access Enterprise Manager

Super Administrators have complete privileges on all the entities present in Software Library, and can exercise access control on the entities by granting one or more privileges, and later revoking the previously granted privilege to another user or role.

Designers by default are given create privileges, which allow them to create entities and manage them.

Operators by default are given view privileges, which allow them to view all the entities in Enterprise Manager Cloud Control.

Any Enterprise Manager user requires, at the very least, a view privilege on an entity for the entity to be visible on the Software Library console. The Super Administrator can choose to grant additional privileges described in Table 15–1 to the user or role. Users will not be able to see this entity till the Super Administrator grants them at least a view privilege on the entity.

15.3 What's New in Software Library

For Enterprise Manager 12*c* Software Library enhancements, refer to *Enterprise Manager Cloud Control Introduction Guide*.

15.4 Performing Software Library Tasks Using EM CLI Verbs or in Graphical Mode

Starting with Oracle Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), command line utility has been introduced for Software Library users in Oracle Enterprise Manager Cloud Control that enables you to perform some of the console-based Software Library operations using the text-based consoles.

The following table describes both approaches to perform some of the Software Library tasks:

- Enterprise Manager Command Line Interface (EM CLI)
- Enterprise Manager Graphical User Interface (EM GUI)

Note: For more information about the syntax and usage of the EM CLI verbs described in Table 15–3 , along with workflow examples, refer to *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

Table 15–3 Software Library EMCLI Verbs

Description	Approach A: Using EM CLI Verb	Approach B: Using Enterprise Manager Cloud Control Console
Adding a Software Library storage location	`add_swlib_storage_location`	Configuring an OMS Shared Filesystem Location Configuring an OMS Agent Filesystem Location Configuring a Referenced File Location
Creating a Software Library entity	`create_swlib_entity`	Creating Generic Components Creating Directives
Creating a Software Library folder	`create_swlib_folder`	Organizing Entities
Listing the Software Library entities	`list_swlib_entities`	Accessing Software Library Home Page Searching Entities
Listing Software Library entity types	`list_swlib_entity_types`	NA

Table 15–3 (Cont.) Software Library EMCLI Verbs

Description	Approach A: Using EM CLI Verb	Approach B: Using Enterprise Manager Cloud Control Console
Listing Software Library entity subtypes	`list_swlib_entity_subtypes`	NA
Listing Software Library folders	`list_swlib_folders`	NA
List Software Library storage locations	`list_swlib_storage_locations`	Accessing Software Library Administration Page
Referring files from a Software Library entity	`refer_swlib_entity_files`	Creating Entities Viewing, Editing, and Deleting Entities
Re-Importing Software Library metadata	`reimport_swlib_metadata`	Re-Importing Oracle Owned Entity Files
Removing a Software Library storage location	`remove_swlib_storage_location`	Removing (and Migrating) Software Library Storage Location
Modifying a Software Library entity	`update_swlib_entity`	Viewing, Editing, and Deleting Entities
Uploading files to a Software Library entity	`upload_swlib_entity_files`	Creating Entities Viewing, Editing, and Deleting Entities
Modify a Software Library OMS Agent storage location to change the associated OMS Host and the credential for accessing the location.	`switch_swlib_oms_agent_storage`	NA
Verify the files uploaded to software library, and report the missing files in the storage locations. This action is typically initiated when some provisioning/patching/deployment activity fails due to missing file in the associated storage location.	verify_swlib	NA

Note: For more information on the usage of EM CLI verbs, refer to *Oracle Enterprise Manager Command Line Interface Guide*.

15.5 Software Library Storage

The Software Library Administration console allows you to configure and administer Software Library. To start using the Software Library, you must add at least one upload file storage location (OMS Shared File System, or OMS Agent File System) on the host where the OMS is running. A storage location in Software Library represents a repository of files that are either uploaded to Software Library or referenced by it.

Note: If you choose to newly configure an OMS Shared Storage Location, then ensure that the file system path that you specify for the location is either a shared path or a mounted path. By doing so, the newly configured location can be made accessible in a multiple OMS environment in the future. If the new location is being added in a multiple OMS environment, then the file system path should be accessible from all the OMS hosts.

However, if you have configured the OMS Shared Storage Location on a local file system, then perform the steps listed in the Section 15.8 to migrate this location to another OMS Shared Storage Location that has a shared or mounted path.

To access the administration console, log into Enterprise Manager Cloud Control with Administration access, and follow these steps:

In Cloud Control, from **Setup** menu, select **Provisioning and Patching**, and then click **Software Library**.

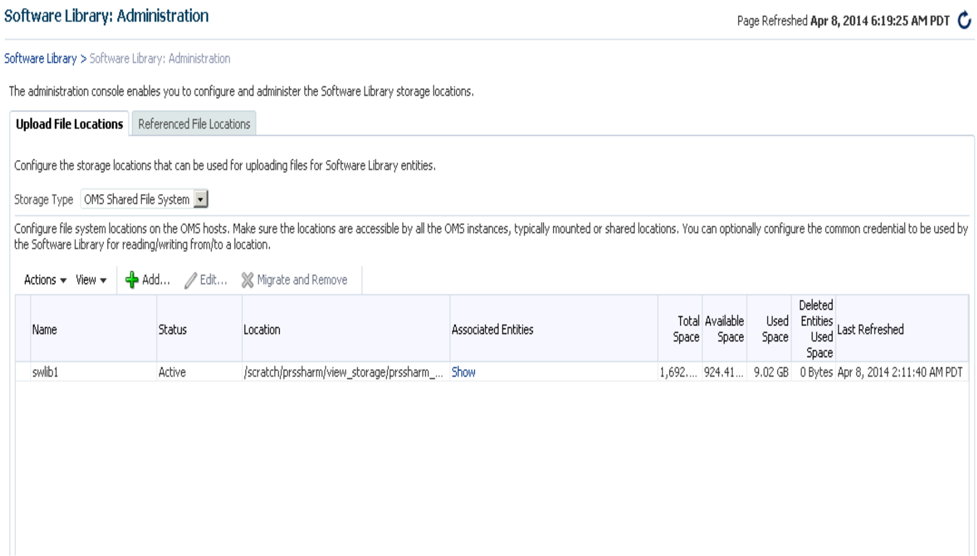
OR

In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching** and then, click **Software Library.** On the Software Library home page, from **Actions** menu, select **Administration**.

Note: For a video tutorial on configuring and using Software Library, see:

Oracle Enterprise Manager 12c: Configure and Use the Software Library

Figure 15–2 Software Library Administration



Software Library: Administration

Page Refreshed **Apr 8, 2014 6:19:25 AM PDT**

Software Library > Software Library: Administration

The administration console enables you to configure and administer the Software Library storage locations.

Configure the storage locations that can be used for uploading files for Software Library entities.

Storage Type: OMS Shared File System

Configure file system locations on the OMS hosts. Make sure the locations are accessible by all the OMS instances, typically mounted or shared locations. You can optionally configure the common credential to be used by the Software Library for reading/writing from/to a location.

Name	Status	Location	Associated Entities	Total Space	Available Space	Used Space	Deleted Entities Used Space	Last Refreshed
swlib1	Active	/scratch/prssharm/view_storage/prssharm_...	Show	1,692....	924.41...	9.02 GB	0 Bytes	Apr 8, 2014 2:11:40 AM PDT

The Software Library Administration Page as shown in Figure 15–2 is a GUI based screen, that enables you to create one or more storage locations to store or refer to files that are associated with an entity. To view the entities present in the storage location, click **show** on the Administration page. You can create a storage location on the OMS or the agent running on the same host as the OMS. With Enterprise Manager 12*c*, a new feature called Referenced File Location has been introduced, wherein Software Library entities can refer to files that are stored on another host. These locations are however read-only for Software Library, and will not be used for uploading files.

The space requirements for configuring Software Library depends on the amount of space required for storing the software binaries, and its associated scripts. Understandably, this space requirement increases over a period of time as you create more entities. Depending on the features or software required for provisioning and patching, you must decide and configure the Software Library storage space.

Note: For production environments, Oracle recommends allocating a minimum 100GB of storage for your software library. Also, ensure that this storage can easily be extended in future, if it starts running out of space.

Once the storage location starts running out of space, it is important to deactivate the configured storage location so that no new uploads can happen to this location. For more information about removing a storage location, see Section 15.11

The following types of storage locations are available:

- Upload File Locations
- Referenced File Location

15.5.1 Upload File Locations

Upload File Locations are locations configured for storing files uploaded by Software Library as part of creating or updating an entity.

For Software Library to become usable, at least one upload file location must be configured. On adding the first upload file location, a job is submitted to import the Software Library metadata from the Oracle home of each of the installed Enterprise Manager plug-in. Ensure that you wait for this job to complete successfully, before performing other patching or provisioning operations.

Note: To physically delete a file system configured as an Upload storage location with Software Library, you must ensure that you first configure an alternate storage location where you can migrate the existing contents (entities). If you fail to perform this migration, then the entities dependent on the files from this location will be rendered unusable. For more information about deleting a storage location, and migrating the contents, see Section 15.11.3.

Prerequisites

As a prerequisite, before using Upload File Locations as storage option, you must set credentials for using an OMS Shared File System or OMS Agent File System:

- For multiple OMS environment, all the OMS hosts must have a preferred normal host credential set.

  When OMS instances are added, it is necessary to ensure that the configured locations are accessible from the designated host where the new OMS will be provisioned. For an OMS that will be provisioned using the Add Management Service functionality, the shared location configured as upload location should be mounted on the designated host, and verified manually.

- For OMS Agent File System location configuration, a credential (preferred or named) has to be specified.

Upload File Locations support two storage options as follows:

OMS Shared File System *(Recommended Storage Option)*

An OMS Shared File System location is required to be shared (or mounted) across all the Oracle Management Server (OMS) hosts. This option is ideal for UNIX systems.

Note: Oracle recommends using OMS Shared File System option for storing files uploaded to Software Library. However, if you are not able to set up a shared file system because of some constraints, then you may use the OMS Agent File System. For more information see "OMS Agent File System"

For single OMS environments, you can configure the Software Library either on the host where the OMS is running, or in a shared location. However, in future, if you plan to expand the single OMS setup to a multiple OMS setup, then local file system path is not recommended.

Note: For a multi-OMS scenario, you must set up clustered file system using NFS, or ACFS, or DBFS. On Windows, for sharing, the OCFS2 cluster file system is recommended.

If you are implementing multiple management servers for high availability you should also make the Software Library file system highly available. Besides accessibility and availability, it is important to ensure that there is enough space (more than 100 GB for production deployment of Enterprise Manager) available for the storage of software binaries, and associated scripts for the entities that you want to create and store.

OMS Agent File System

An OMS Agent File System location should be accessible to the agent running on the host machine where the OMS is deployed. To use OMS Agent Filesystem storage option, ensure that you have a preferred, or a named credential for the OMS host. Click **Change Credential** to change the associated credential to be used to access this location.

Note: If you can not set up an OMS Shared File System for storage because of some constraints, then you may use the OMS Agent File System.

15.5.2 Referenced File Location

Referenced File Locations are locations that allow you to leverage the organization's existing IT infrastructure (like file servers, web servers, or storage systems) for sourcing software binaries and scripts. Such locations allow entities to refer to files without having to upload them explicitly to a Software Library storage.

Referenced File Locations support three storage options:

- **HTTP**: An HTTP storage location represents a base URL which acts as the source of files that can be referenced.

  For example, the base URL `http://my.files.com/scripts` could be configured as an HTTP location for sourcing files such as `http://my.files.com/scripts/perl/installMyDB.pl` or `http://my.files.com/scripts/linux/stopMyDB.sh.`

- **NFS**: An NFS storage location represents an exported file system directory on a server. The server need not be an Enterprise Manager host target.

  For example, the directory `/exported/scripts` is exported on server `my.file.server` could be configured as an NFS location for sourcing files such as `/exported/scripts/generic/installMyDB.pl` or `/exported/scripts/linux/stopMyDB.sh` once mounted on a target host file system.

- **Agent**: An Agent storage location is similar to the OMS Agent File System option, but can be any host monitored by an Enterprise Manager Agent. The Agent can be configured to serve the files located on that host.

  For example, the directory `/u01/binaries` on the Enterprise Manager Host `my.em.file.server` could be configured as an Agent location for sourcing files such as `/u01/binaries/rpms/myCustomDB.rpm` or `/u01/binaries/templates/myTemplate.tar.gz`.

  These locations require a named credential to be associated which will be used to access the files from the base location on the host through the Enterprise Manager Agent.

Note: To use entities referring files of a location, you must have view privilege on the credentials associated with the locations.

15.6 Prerequisites for Configuring Software Library

To administer the different storage types, and to configure software library, keep the following points in mind:

- Depending on the features or software required for provisioning and patching, you must decide and configure the Software Library storage space. The storage needs change based on the usage pattern.
- Each OMS host must have a preferred normal host credential set before configuring the location. For OMS Agent File System location configuration, a credential (preferred or named) has to be specified.
- You (the user configuring the Software Library) must have view privilege on all the OMS, and the agent targets running on the host machine. As per the accessibility verification, you must be able to view, and edit these newly configured locations.
- To add an OMS Agent storage location, ensure that you have view privileges on the target OMS host, and the agents running on that target host.

15.7 Configuring Software Library Storage Location

System Administrators are responsible for configuring a storage location. Only after the storage location is configured, you can start uploading the entity files.

You can configure the Software Library in one of the following locations:

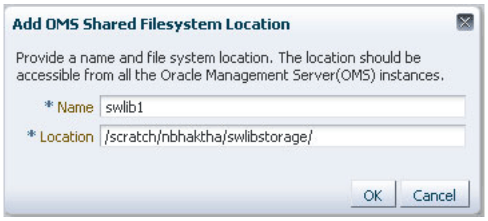
- Configuring an OMS Shared Filesystem Location
- Configuring an OMS Agent Filesystem Location
- Configuring a Referenced File Location

> **Note:** Starting with Oracle Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), in addition to using the GUI as described in this section, you can alternatively use the command line interface tool to Configure the Software Library. To do so, refer to *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

15.7.1 Configuring an OMS Shared Filesystem Location

To configure an OMS Shared File System storage location that can be used for uploading Software Library entity files, perform the following steps:

1. From the **Setup** menu, select **Provisioning and Patching**, then select **Software Library.**
2. On Software Library: Administration page, select **OMS Shared Filesystem**.
3. To add a new OMS Shared File System, click **+Add**.
4. In the Add OMS Shared File System location dialog box, provide a unique name, and location on the OMS host, where you want to set up the upload location.



Add OMS Shared Filesystem Location

Provide a name and file system location. The location should be accessible from all the Oracle Management Server(OMS) instances.

* Name: swlib1

* Location: /scratch/nbhaktha/swlibstorage/

Ensure that the configured storage location is a shared location that is accessible by all the OMS instances. For a Multi OMS setup, set the Normal Preferred Credentials for all the OMS(s).

When you configure an upload location for the first time, a metadata registration job is submitted which imports all the metadata information of all the installed plug-ins from the Oracle home of the OMS.

To track the progress of the job, click **Show Detailed Results.** Typically, the name of the job starts with `SWLIBREGISTERMETADATA_*`.

If the Import job fails, see Section 15.11 for information on Re-importing metadata for Oracle-owned files.

5. Click **OK** to create a new entry for the storage location in the table, with details like **Name**, **Location**, **Host**, **Status**, and **Host Credentials.**

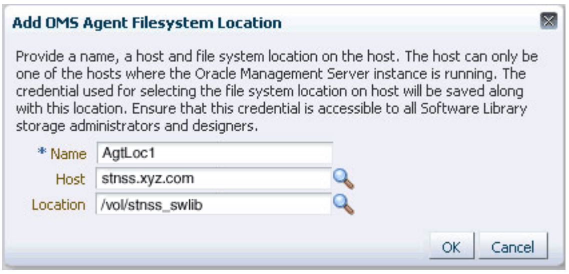
   In addition to this, you can click **Associated Entities** to view or search the entities present in the selected upload location.

15.7.2 Configuring an OMS Agent Filesystem Location

> **Note:** The OMS Agent File system must be set up only when the recommended storage option, which is the OMS Shared File System cannot be setup because of some constraints. For more information, see Section 15.5.1.

To configure an OMS Agent location, perform the following steps:

1. From the **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library: Administration page, select **OMS Agent Filesystem**.
3. Click **+Add,** in the Add OMS Agent File System Location dialog box, enter the following details:



Add OMS Agent Filesystem Location

Provide a name, a host and file system location on the host. The host can only be one of the hosts where the Oracle Management Server instance is running. The credential used for selecting the file system location on host will be saved along with this location. Ensure that this credential is accessible to all Software Library storage administrators and designers.

* Name: AgtLoc1

Host: stnss.xyz.com

Location: /vol/stnss_swlib

   a. In the **Name** field, enter a unique name for the storage.
   b. In the **Host** field, click the magnifier icon. From the Search and Select: Hosts dialog box, select a host where the OMS is running, and click **Select**.

For example, `xyz.acme.com`

c. In the **Location** field, click the magnifier icon. In the Remote File Browser dialog box, click **Login As** to log into the host machine with either Preferred, Named or New credentials.

Note: For a user to access and leverage an OMS Agent Filesystem upload location successfully, the owner of the Named Credential (basically, the credential used to connect to the host machine), must grant a View Privilege on the credential chosen to all the Administrators (or users) accessing this OMS Agent Filesystem location.

For more information about granting privileges on a Named Credential, refer to *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

Navigate to the location on the host where you want to create the Agent File System, and click **OK**.

The selected credential is saved along with the host and selected file system path. The saved credential is used to upload files and stage the uploaded files to a host target as part of some provisioning or patching activity.

Note: The administrator configuring the Software Library must grant view privilege (at least) on the credential chosen to all designers uploading or staging the files to or from this location.

4. Click **OK** to create a new entry for the storage location in the table, with details like **Name**, **Location**, **Host**, **Status**, and **Host Credentials.**

   In addition to this, you can click **Associated Entities** to view or search the entities present in the selected upload location.

These newly configured OMS Agent locations are now available for storing entity files.

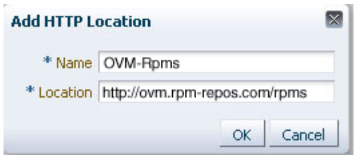
15.7.3 Configuring a Referenced File Location

To configure storage location that can be used for referring to files from the Software Library entities, perform the following steps:

1. From the **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**

2. On the Software Library: Administration page, click **Referenced File Locations** tab.

3. To add an HTTP location that can be accessed through a HTTP URL, select **HTTP** from the Storage Type list and click **+Add**.



Add HTTP Location

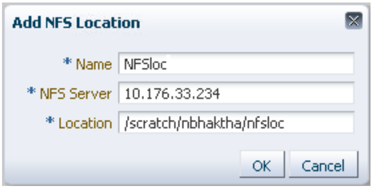
* Name OVM-Rpms

* Location http://ovm.rpm-repos.com/rpms

   In the Add HTTP Location dialog box, enter a unique name and a HTTP location for the storage that you want to reference, and click **OK**.

A new entry for the storage location is created, with details like **Name**, **Location**, and **Status**.

4. To add an NFS shared location, select **NFS** from the Storage Type list and click **+Add**.



Add NFS Location

* Name	NFSloc
* NFS Server	10.176.33.234
* Location	/scratch/nbhaktha/nfsloc

In the Add NFS Location dialog box, do the following:

a. Enter a unique name in the **Name** field for the storage.

b. In **NFS server** field, provide a fully qualified domain name or the IP address of the hosted machine that has NFS services running on them.

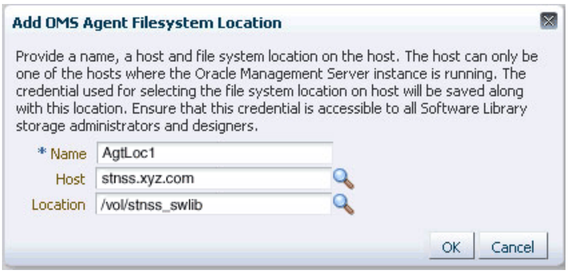
c. In the **Location** field, provide the shared location or directory path on the NFS server to define a storage location, then click **OK**.

A new entry for the storage location is created in the table, with details like **Name**, **Location**, and **Status**.

Note: While creating a procedure, if you have a component step or a directive step that refers to an NFS file location, then you must ensure that you set the preferred privileged credentials for the target host before the procedure is submitted for execution.

---

5. To add an Agent location that has read-only privileges set on it, select **Agent** from the Storage Type list and click **+Add**.



Add OMS Agent Filesystem Location

Provide a name, a host and file system location on the host. The host can only be one of the hosts where the Oracle Management Server instance is running. The credential used for selecting the file system location on host will be saved along with this location. Ensure that this credential is accessible to all Software Library storage administrators and designers.

* Name	AgtLoc1
Host	stnss.xyz.com
Location	/vol/stnss_swlib

In the Add Agent Location dialog box, enter the following details:

a. In the **Name** field, enter a unique name for the storage.

b. In the **Host** field, click the magnifier icon to select a target from the list available.

   For example, `xyz.company.com`

c. In the **Location** field, click **Login As** to select the credentials and browse the previously selected host.

   The credential selected, either Preferred, Named or New, is saved along with the host and selected file system path. The saved credential is used for staging the files to a host target as part of some provisioning or patching activity.

> **Note:** The administrator configuring the Software Library must grant view privilege (at least) on the credential chosen to all designers uploading or staging the files to or from this location.

Note: When you create a new entity, these newly configured Referenced File Locations are available as storage options.

15.8 Configuring Software Library on a Multi-OMS System

Oracle recommends that you configure each OMS Shared Storage Location to use a shared or mounted file system path. Doing this will ensure that this newly configured location remains accessible from any OMS host as and when they are added. All upload and stage requests for the files will happen through the Management Agent monitoring the OMS host.

> **Note:** Starting with Enterprise Manager 12c, use the EM CLI utility to migrate files across upload locations of different storage types. To migrate files from an OMS Shared storage location to an OMS Agent storage location, use the EM CLI verb `remove_swlib_storage_location`. The same verb supports the reverse action as well. Alternatively, you can also use the Cloud Control UI. For information about how to use the Cloud Control to migrate files across storage locations, see Section 15.11.3.

If however, you have configured the OMS Shared storage location to use a local file system path, then you must migrate it to another OMS Shared Storage Location that uses a shared or mounted path. To do so, follow these steps:

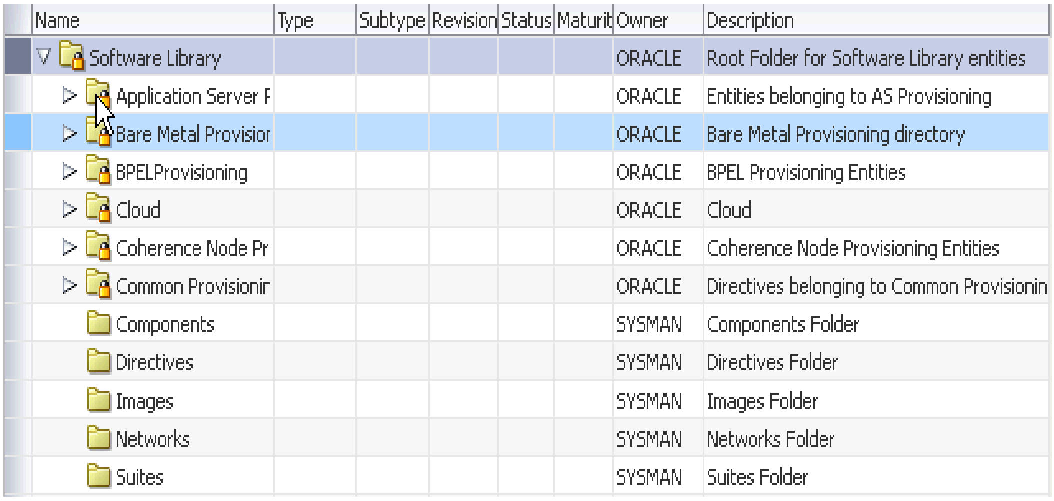
1. In Cloud Control, from **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Administration page, add a new OMS Shared storage location by specifying a name (for example: NewShared), and a shared file system path.
3. On successful completion, select the location you want to migrate, (For example: OldNonShared), and click **Migrate and Remove.**
4. In the popup dialog box, select the new OMS Shared File System as the storage plugin type, and the new OMS shared storage location (NewShared) as the destination to migrate the files.
5. Click **Remove** to submit a job, which on successful completion deletes the storage location entry from the table.

15.9 Using Software Library Entities

To access the Software Library Home Page, in Cloud Control, from the **Enterprise menu,** select **Provisioning and Patching** and then, click **Software Library.** Software Library is a repository that stores certified software binaries such as software patches, virtual appliance images, reference gold images, application software and their associated directive scripts, generally referred to as *Entities.* Accesses and privileges on these entities are decided by the Super Administrators or the owner of the entity.

Entities can broadly be classified as:

Types	Description
Oracle-owned Entities	These entities are available by default on the Software Library Home page, once the Software Library is configured. In the following graphic, all the entities that are owned by **Oracle**, qualify as Oracle-owned entities, and all the folders that appear with a lock icon against them are Oracle-owned folders like Application Server Provisioning, Bare Metal Provisioning, Cloud, and so on.
Custom Entities	These entities are created by the Software Library users. For example, in the following graphic you can see a custom folder called My Entities, and entities called os2 and os1 created by the owner of the entity. These entities are called User-owned entities.

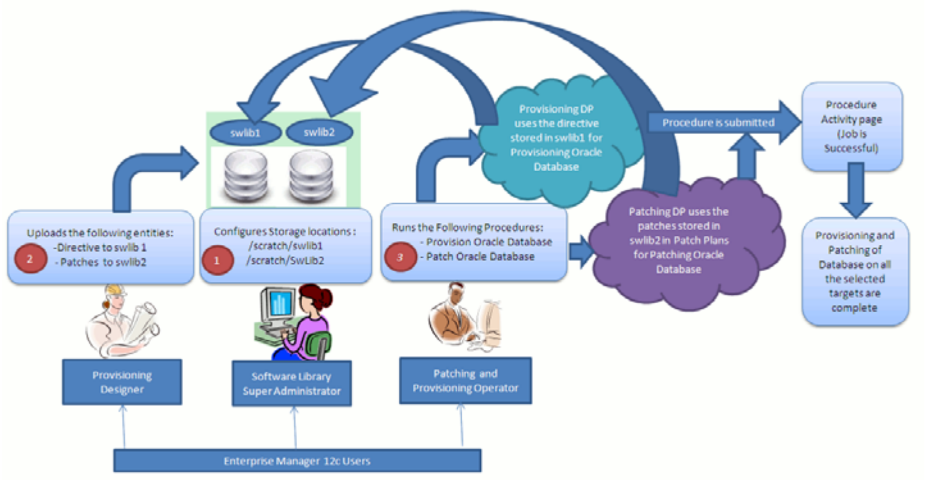


Name	Type	Subtype	Revision	Status	Maturit	Owner	Description
▽ Software Library						ORACLE	Root Folder for Software Library entities
▷ Application Server F						ORACLE	Entities belonging to AS Provisioning
▷ Bare Metal Provisior						ORACLE	Bare Metal Provisioning directory
▷ BPELProvisioning						ORACLE	BPEL Provisioning Entities
▷ Cloud						ORACLE	Cloud
▷ Coherence Node Pr						ORACLE	Coherence Node Provisioning Entities
▷ Common Provisionir						ORACLE	Directives belonging to Common Provisionin
Components						SYSMAN	Components Folder
Directives						SYSMAN	Directives Folder
Images						SYSMAN	Images Folder
Networks						SYSMAN	Networks Folder
Suites						SYSMAN	Suites Folder

Note: All Oracle-owned folders (and entities) are available on the Software Library Home page by default. The Oracle-owned folders have a read-only privilege, so you cannot select these folders to create an entity. You must create a custom folder to place your entities in them.

A number of lifecycle management tasks like patching and provisioning deployment procedures make use of the entities available in Software Library to accomplish the desired goal. Here is a pictorial representation of how a Provisioning Deployment Procedure and a Patching Deployment Procedure makes use of the entities available in the Software Library:

Figure 15–3 Using Software Library Entities for Provisioning and Patching Tasks


swlib1
swlib2
Provisioning DP uses the directive stored in swlib1 for Provisioning Oracle Database
Procedure is submitted
Procedure Activity page (Job is Successful)
Uploads the following entities:
2
-Directive to swlib 1
- Patches to swlib2
Configures Storage locations :
1
/scratch/swlib1
/scratch/SwLib2
Runs the Following Procedures:
3
- Provision Oracle Database
- Patch Oracle Database
Patching DP uses the patches stored in swlib2 in Patch Plans for Patching Oracle Database
Provisioning and Patching of Database on all the selected targets are complete
Provisioning Designer
Software Library Super Administrator
Patching and Provisioning Operator
Enterprise Manager 12c Users

15.10 Tasks Performed Using the Software Library Home Page

From the Software Library Home page, you can do the following:

- Organizing Entities
- Creating Entities
- Customizing Entities
- Managing Entities

15.10.1 Organizing Entities

Only designers who have the privilege to create any Software Library entity, can create folders.

> **Note:** Starting with Oracle Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), in addition to using the GUI as described in this section, you can alternatively use the command line interface tool to Create Folders. To do so, refer to *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

To create a custom folder, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library.**
2. On the Software Library Home page, from **Actions** menu, click **Create Folder** to create a custom folder of your own.

   The custom folder can contain User-owned folders, entities, and customized entities created by using the *Create Like* option.
3. In the Create Folder dialog box, enter a unique name for the folder. Also, select the parent folder in which you want to create this new custom folder and click **Save.**

   For example, if the root folder is `Software Library` and you created a custom folder in it called `Cloud12gTest`, then the Parent Folder field is populated as follows: `/Software Library/Cloud12gTest.`

Note: Only the owner of the folder or the Super Administrator has the privilege to delete the folder, nobody else can.

15.10.2 Creating Entities

From the Software Library Home page, you can create the following entities:

- Creating Generic Components
- Creating Directives

Note: Starting with Oracle Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), in addition to using the GUI as described in this section, you can alternatively use the command line interface tool to Create Entities. To do so, refer to *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

15.10.2.1 Creating Generic Components

To create a generic component from the Software Library Home page, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library.**
2. On the Software Library Home page, select a custom folder that is not owned by Oracle.

   Note: You cannot create a generic component in an Oracle Owned Folder. To create a custom folder, see Section 15.10.1.
3. From the **Actions** menu, select **Create Entity** and click **Component**. Alternately, right click the custom folder, and from the menu, select **Create Entity** and click **Component**.
4. From the Create Entity: Component dialog box, select **Generic Component** and click **Continue**.

   Enterprise Manager Cloud Control displays the Create Generic Component: Describe page.
5. On the Describe page, enter the **Name**, **Description,** and **Other Attributes** that describe the entity.

   Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

   Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

   In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.
6. On the Configure page, you can customize the generic component that you are creating by adding some new properties or updating the existing properties of the component.

   Note: Select **Shared Type** to reuse the component property. Shared Type can be stored as a template, which can be used for creating different and more complicated top level types.

To add a new property, do the following, and click **Next**:

a. Select **Top Level Type** or **Shared Type**, and click **Add**.

b. Enter a unique name for the property. Depending on the property type selected, enter an initial or default value for the property.

c. To add a constraint, specify the Minimum or Maximum value for the selected property type, and click **Add Constraint**.

   The Configured Constraints table lists all the constraints added. To remove a particular constraint from the property, select the property and click **Remove**.

7. On the Select Files page, you can select one or more files to be associated with the entity. Select one of the following options:

   - **Upload Files:** If you want to upload some entity files from the local file system or the agent machine to the selected destination location.

     To select the destination location, in the Specify Destination section, in the **Upload Location** field, click the magnifier icon to select one of the following options:

     – **OMS Shared FileSystem**

     – **OMS Agent FileSystem**

     The corresponding Storage Type and Location Path of the selected location is populated.

     Note: To upload the files, the status of the storage location to which the files are to be uploaded should be **Active**.

     If you select OMS Agent Filesystem location, then ensure that you have the necessary privileges to access the location

     In the Specify Source section, enter the location from where the files are being sourced, these locations can either be local file system or a remote file system monitored by the Management Agent. Select one of the following options for File Source:,:

     – If you select **Local Machine**, and click **Add**, the Add File dialog box appears. Click **Browse** to select the entity file from the source location, and give a unique name, and click **OK**.

       You can upload the files to any of the configured storage locations available in OMS Shared Filesystem location or OMS Agent Filesystem location

     – If you select **Agent Machine**, select the name of the host machine from where you want to pick up the entity files. Click **+Add** and log into the host machine with the desired credentials. For more information about the different credential types and their setup, see *Oracle Enterprise Manager Lifecycle Management Guide*.

       Once you log into the host machine, browse to the location where the files to be uploaded are present. You can upload the files to any of the configured storage locations available in OMS Shared Filesystem location or OMS Agent Filesystem location.

   - **Refer Files:** If you select the **Refer Files** option, you only need to enter the source location details, since you are not technically uploading anything to the Software Library. In the Specify Source section, select from **HTTP**, **NFS**, or

Agent Storage types, and click OK. The corresponding Storage Type and Location Path of the selected location is populated.

Click **+Add** to reference the entity present at the selected Referenced File Location. In the Add Referenced File dialog box, enter a relative path to the file under Base Location. Click **Stage As** to organize the file in a temporary stage location with a unique name.

For details about each of these storage options, see Section 15.7.3

8. On the Set Directives page, click **Choose Directives** to associate a component with one or more directives. Click **Next**.
9. On the Review page, review all the details, and click **Finish** to create the component and upload it on the Software Library.

15.10.2.2 Creating Directives

Directives are entities in the Software Library that represent a set of instructions to be performed. These are constructs used to associate scripts with software components and images. These scripts contain directions on how to interpret and process the contents of a particular component or an image.

To create a directive from a Software Library Home page, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Home page, select a custom folder that is not owned by Oracle.

   Note: You cannot create a generic component in an Oracle Owned Folder. To create a custom folder, see Section 15.10.1.
3. From **Actions** menu, select **Create Entity** and click **Directive**. Enterprise Manager Cloud Control displays the Create Entity: Directives wizard.
4. On the Describe page, enter the **Name**, **Description,** and **Other Attributes** that describe the entity.

   Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, and it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

   Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

   In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.
5. On the Configure page, specify the command line arguments that must be passed to the directive to configure it. This command provides the parameters required to execute the directive.

   To add the command line arguments or parameters, click **Add**.

   In the Add Command Line Arguments dialog box, enter the values in the following fields:

   - **Argument Prefix,** is a switch or a constant command line argument.

     The Argument Prefix eliminates the error-prone task of manually specifying the order of the parameter executions in a given directive. This is specially useful when a directive is made of multiple parameters.

Oracle recommends that you create command line arguments using an Argument Prefix.

- **Property Name,** is the name of the property, that must be a string value.
- **Argument Suffix,** is the text that must follow the command line property.

  Though the suffix is rarely used, it determines how the parameters must be executed, based on the suffix value.

For example, if the command line argument you want to pass is as follows:

```
./test.sh -user={username}
```

Then,

Argument Prefix is: `-user`

Property Name is: `username`

All the parameters added appear in the order of addition against the **Command Line** field.

To change the order of the parameter or edit any property of an existing parameter, click **Edit**.

To remove any of the parameters, click **Remove**.

In the Configuration Properties section, select either **Bash** or **Perl** as defined in the script.

Select **Run Privileged** to run the script with `root` privileges.

6. On the Select Files page, you can select one or more files to be associated with the entity. Select one of the following options:

   - **Upload Files:** If you want to upload some entity files from the local file system or the agent machine to the selected destination location.

     To select the destination location, in the Specify Destination section, in the **Upload Location** field, click the magnifier icon to select one of the following options:

     – **OMS Shared FileSystem**

     – **OMS Agent FileSystem**

     The corresponding Storage Type and Location Path of the selected location is populated.

     Note:

     To upload the files, the status of the storage location to which the files are to be uploaded should be **Active**.

     If you select OMS Agent Filesystem location, then ensure that you have the necessary privileges to access the location

     In the Specify Source section, enter the location from where the files are being sourced, these locations can either be local file system or a remote file system monitored by the Management Agent. Select one of the following options for File Source:

  - If you select **Local Machine**, and click **Add**, the Add File dialog box appears. Click **Browse** to select the entity file from the source location, and give a unique name, and click **OK**.

    You can upload the files to any of the configured storage locations available in OMS Shared Filesystem location or OMS Agent Filesystem location

  - If you select **Agent Machine**, select the name of the host machine from where you want to pick up the entity files. Click **+Add** and log into the host machine with the desired credentials. For more information about the different credential types and their setup, see *Oracle Enterprise Manager Lifecycle Management Guide*.

    Once you log into the host machine, browse to the location where the files to be uploaded are present. You can upload the files to any of the configured storage locations available in OMS Shared Filesystem location or OMS Agent Filesystem location.

- **Refer Files:** If you select the **Refer Files** option, you only need to enter the source location details, since you are not technically uploading anything to the Software Library. In the Specify Source section, select from **HTTP**, **NFS**, or **Agent** Storage types, and click OK. The corresponding Storage Type and Location Path of the selected location is populated.

  Click **+Add** to reference the entity present at the selected Referenced File Location. In the Add Referenced File dialog box, enter a relative path to the file under Base Location. Click **Stage As** to organize the file in a temporary stage location with a unique name.

  For details about each of these storage options, see Section 15.7.3

7. On the Review page, review all the details, and click **Finish** to create the component and upload it on the Software Library.

15.10.3 Customizing Entities

You cannot edit an entity present in an Oracle owned folder. However, to edit an Oracle-owned entity, you can make a copy of the entity and store it in a custom folder. Since you now have full access on the entity, you can customize the entity based on your requirement and may even choose to grant other users access to this entity.

To create a custom entity from an Oracle owned entity, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

   For more information about searching for an entity, see Section 15.10.4.10.
3. From **Actions** menu, select **Create Like**.
4. On the Create Like: <Entity Name> dialog box, enter a name that is unique to the parent folder and a description for the entity.

   By default, the root directory Software Library is preselected in the **Parent Folder** field.

   To change the parent folder and organize the entities, click **Change Parent Folder**. and select the desired folder.
5. Click **OK** to apply the changes.

The new entity appears in the Entities table, under the selected parent folder.

You as the owner have all the privileges on the entity, and can update the properties as per your requirement.

To update the properties of the entity, see Section 15.10.4.8.

For more information on Oracle Owned Entities and User Owned Entities, see Section 15.9.

15.10.4 Managing Entities

From the Software Library Home page you can perform the following maintenance tasks on the existing entities:

- Accessing Software Library Home Page
- Accessing Software Library Administration Page
- Granting or Revoking Privileges
- Moving Entities
- Changing Entity Maturity
- Adding Notes to Entities
- Adding Attachments to Entities
- Viewing, Editing, and Deleting Entities
- Searching Entities
- Exporting Entities
- Importing Entities
- Staging Files Associated With an Entity

> **Note:** Starting with Oracle Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), you can either use the GUI or use the command line interface tool for performing all the tasks listed in Table 15–3.

15.10.4.1 Accessing Software Library Home Page

To access the Software Library Home page, from the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**

15.10.4.2 Accessing Software Library Administration Page

To access the Software Library Administration page, from the **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**

15.10.4.3 Granting or Revoking Privileges

An Enterprise Manager user requires, at the very least, a view privilege on an entity for the entity to be visible on the Software Library Home. The owner or super administrator can choose to grant additional privileges like edit (Update notion) or manage (or full) or at a later point of time, revoke the previously granted privilege.

To grant or revoke privileges, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**

2. To grant or revoke fine-grained privileges to the other users on any entity that you own, select the custom entity and from **Actions** menu, click **Grant/Revoke Privileges.**
3. On Grant/Revoke Privileges on: <entity_name> window, you can either grant or revoke Software Library privileges depending on the users roles and responsibilities in the organization.

   Granting Privileges: To grant one or more new privileges, click **+Add** and search for the users. You can grant them one of the following privileges on the entity you own:

   - **View Software Library Entity:** This is normally an operator privilege where the user can only view the entity on the Software Library Home. The user cannot edit or manage the entity. All the Oracle owned entities can be viewed by all Enterprise Manager users.
   - **Edit Software Library Entity:** This is a designer privilege where a user has Create, Update, and Edit privileges on the entity.
   - **Manage Software Library Entity:** This is a super-administrator privilege where the user has complete access on the entity. With this privilege, you can grant or revoke accesses on this entity to other users, or delete the entity.

   Revoking Privileges: To revoke previously granted privileges, select the user and click **Remove**.
4. Click **Update** to apply the selected grants on the entity.

15.10.4.4 Moving Entities

To move all the revisions of an entity from one folder to another, do the following:

1. From the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

   For more information about searching for an entity, see Section 15.10.4.10.
3. From the **Actions** menu, click **Move Entity** and accept the confirmation.
4. From the Move Entity dialog box, select the destination folder for the entities and click **Set New Parent Folder**.

   Note: Ensure that the source and the destination folders are not owned by Oracle, as you cannot move or edit them.

15.10.4.5 Changing Entity Maturity

When an entity is created from the Enterprise Manager Home, it is present in an Untested state. It is the responsibility of a designer to test the entity, and change the maturity level based on the test result.

To manage the lifecycle and indicate the quality (maturity level) of an entity, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

   For more information about searching for an entity, see Section 15.10.4.10.

3. From the **Actions** menu, click **Change Maturity** to change the maturity value an entity after testing.

For example, an Oracle Database Clone component would be tested by selecting it in a deployment procedure interview flow that provisions a database. Once the entity is tested, the designer can change the maturity of the entity to either Beta or Production based on test results. Only when the entity is marked with Production level, the Operator can use it.

15.10.4.6 Adding Notes to Entities

To log information about the changes or updates made to an existing entity, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library.**
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

   For more information about searching for an entity, see Section 15.10.4.10.
3. From **Actions** menu, click **Notes** to include any important information related to the entity. You can also add notes while editing an entity.

   The most recent note appears on top of the table, and the older notes appear below.
4. After updating the details, click **Finish** to submit the changes, and return to the Software Library Home page.

15.10.4.7 Adding Attachments to Entities

To add or upload files that are typically documents (like README, installation, configuration) related to the software the entity represents, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

   For more information about searching for an entity, see Section 15.10.4.10.
3. From **Actions** menu, click **Attachments** to include one or more files related to the entity. These files contain some important information about the entity. You can also attach files while editing an entity.

   For example, you can attach a readme file to a patch or a component, attach a test script to a directive and so on. However, you must ensure that the file size of each attachment is not more than 2 MB.
4. Click **Finish** to submit the changes, and return to the Software Library Home page.

15.10.4.8 Viewing, Editing, and Deleting Entities

To view, edit, or delete the details of an entity, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library.**

2. On the Software Library Home page, select an entity or alternately, search and select an entity.

   For more information about searching for an entity, see Section 15.10.4.10.

3. To manage an existing entity, select the entity and perform any of the following functions:

   - **View:** Click **View** icon on the table to view the details of an entity. You cannot update the properties of the entity from here.
   - **Edit:** Click **Edit** icon on the table or right-click the entity and select **Edit** from the context menu to update the properties of an entity.

     If you are satisfied with the details, click **Save and Upload** to make the changes available on the Software Library Home page.
   - **Delete:** Click **Delete** icon to remove the entity from the Software Library Home page.

     Note: By deleting an entity, the entity is no longer available for selection, viewing, or editing, and will not be displayed on the Software Library Home page. However, the entity continues to exist in the repository and the associated files, if uploaded, continue to exist in the respective disk storage. To delete the entity completely from the repository and the associated files from the file system, you must purge the deleted entities from the administration page. The purge job not only deletes the files associated with the deleted entity, but removes the deleted entities itself from the repository tables.

     For more information about how to purge the deleted entities from the storage location, see Section 15.10.4.9.

15.10.4.9 Purging Deleted Entities

To purge the deleted entities from all the configured Agent Storage locations, you can run a purge job. To do so, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library.**
2. On the Software Library home page, from **Actions** menu, select **Deleted Entities.** A list of entities that are deleted from Software Library are displayed.

   Note: The **Space Used** attribute is displayed only for the deleted entities that had uploaded files to Software Library.

3. On the Deleted Entities page, click **Purge** to permanently remove these entities from Oracle Management Repository, and the associated files from upload storage locations.
4. A Confirmation Message dialog box is displayed. Click **Job Details** to view the status of the purge job submitted.

   Note: A periodic job named `SWLIBPURGE` runs daily to purge the deleted entities from the Software Library.

15.10.4.10 Searching Entities

This section contains the following topics:

- Performing Basic and Advanced Search
- Saving Searches
- Retrieving Saved Searches
- Managing Saved Searches

Performing Basic and Advanced Search

To perform a basic or an advanced search for an entity, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**
2. To search for an entity, perform one of the following operations:

   a. **Find:** On the Software Library Home page, you can search for an entity by its **Name**, **Description**, or **Type.** Select the search category, enter the desired value and then click the arrow icon.

      On clicking the arrow icon, the result page displays a number of matching results, and allows you to toggle between the result rows by clicking the up and down arrows.

   b. **Search:** To perform a detailed search for an entity, click **Search**. The search option, by default, allows you to search by **Type, Name**, **Description**, **Revision, Maturity**, **Status**, and **File Name** to retrieve a more granular search result.

      Note: If you choose entities that have associated subtypes (like Components), then the page is refreshed with **Subtype** as an additional search category.

      Specify appropriate values in **All** or **Any** of the search fields, and click **Search**.

      To add more search parameters, in the Advanced Search section, click **Add Fields** menu and, select the desired search fields. The selected fields appear in the Advanced Search section as new search parameters. This new search feature enables you to refine your search, and drill down to the most accurate and desired search result.

      To revert to the simple search view, click **Close Search**.

Saving Searches

Optionally, search criteria on the Advanced Search screen of the console, can be saved. Saved searches can be retrieved and executed again. They can also be edited and deleted.

1. Search for entities using the steps listed in Section 15.10.4.10.
2. Click **Save Search.**
3. Enter the preferred name for the search in the text box, and click **Ok.**

Retrieving Saved Searches

To retrieve saved searches, follow these steps:

1. Search for entities using the steps listed in Section 15.10.4.10.
2. Click **Saved Searches**, and select the preferred saved search from the list.

   Alternatively, you can also select the preferred saved search from the Favorites menu. To do so, from the **Favorites** menu, select **Saved Software Library Searches,** and select the preferred saved search.

Managing Saved Searches

Using the Manage Saved Searches option, you can edit the name of the saved search, or delete the saved search. To do so, follow these steps:

- To manage saved searches, you can perform one of the following steps:
  - From the **Favorites** menu, select **Manage Favorites.**
  - Click **Saved Searches,** and select **Manage Saved Searches.**
- To edit the name of the saved search, select the preferred saved search, and in the **Name** text field, enter the new name. Click **Ok** to save changes.
- To delete or remove a saved search, select the preferred saved search, and click **Remove Selected.** Click **Ok** to save changes.

15.10.4.11 Exporting Entities

To export selected entities, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Home page, from the **Actions** menu, click **Export** to export entities present in the Software Library as a Provisioning Archive (PAR) file.

   The PAR file can be used for recreating the entities on an Enterprise Manager with a different repository.
3. On the Export Software Library Entities page, do the following:
   - Click **+Add** to search and select an entity.
   - In **Directory Location**, enter a directory location accessible to OMS for storing the generated PAR files.
   - In **PAR File**, enter the name of the PAR file with a `.par` extension generated during export.
   - To encrypt and securely store all the secret property values of the PAR file being exported, enter a value in the **Oracle Wallet Password** field.

     Note: Specify the same password for importing this PAR file. For more information on importing, see Section 15.10.4.12.
   - Select **Exclude Associated Files**, to exclude the files, binaries, or scripts associated with an entity, from being exported.

   For example, let us consider that you have a separate test and production environment and want to import only the entities that have been tested and certified in the test environment into production. The entities exported from the test system are made available as a Provisioning Archive (PAR) file. You can now choose to import this PAR file into the production system (which is identical to the test system) and use the tested entities.
4. Click **Submit** to submit an export job. Once the job runs successfully, the selected entities from the Software Library are exported as a PAR file.

> **Note:** Provisioning Archive Files that were exported from any Enterprise Manager version prior to 12*c* can not be imported into Enterprise Manager 12c.

15.10.4.12 Importing Entities

To import PAR (Provisioning Archive) files into the Software Library or deploy them to an OMS, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library.**
2. On the Software Library Home page, from **Actions** menu, click **Import** to import the PAR files.
3. On the Import Software Library Entities page, specify the **PAR File** to be imported.

   To import the PAR file successfully, in the **Password** field, enter the same password that was set on the PAR file to secure the secret property values during export.

   For example, let us consider that you have a separate test and production environment and want to import only the entities that have been tested and certified in the test environment into production. The entities exported from the test system are made available as a Provisioning Archive (PAR) file. You can now choose to import this PAR file into the production system (which is identical to the test system) and use the tested entities.
4. If a revision of the entity being imported already exists in Software Library, then you can overwrite the existing entity with a newer revision during import by selecting **Force New Revision**.

   Note: If a revision of the entity being imported already exists in the repository, and you do not select the Force New Revision option, then import process fails.
5. Click **Submit** to submit an import job. On successful completion of the job, the PAR files are imported into the Software Library.

> **Note:** Provisioning Archive Files that were exported from any Enterprise Manager version prior to 12*c* can not be imported into Enterprise Manager 12c.

15.10.4.13 Staging Files Associated With an Entity

For transferring the files associated with an entity to a specific target host follow the steps outlined in this section.

Prerequisites

Ensure that you meet the following prerequisites before staging the files associated with an entity:

1. Only hosts that are monitored by the Enterprise Manager can be specified as the destination for staging the files associated with an entity.
2. Only files that have been successfully uploaded to the entity (hence, in *Ready* status) can be selected for staging.

> **Note:** To verify if the entity has any files in the **Ready** state, follow these steps:
>
> 1. Select the entity, and click **View.**
> 2. On the View Entity page, select **Select Files** tab, to verify the files associated with the entity.
> 3. Unless there is at least one file with a *Ready* status, you cannot proceed with the staging process.

3. Only users with Create Job Privileges can stage the files associated with an entity.
4. If the source files to be staged are on NFS, then the credentials used for browsing the destination target should have `root` permissions to be able to mount the NFS location.

Staging Procedure

Log in to Enterprise Manager Cloud Control with designer privileges, and perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library.**
2. Select the entity, and from **Actions** menu, select **Stage Entity.**
3. On the Stage Entity page, the entity details, the source upload location, and the selected entity files are displayed.

   You can optionally select the **Overwrite files on the staging location** to overwrite an existing version of the same file. If not, ignore this option and proceed.
4. In the Staging Destination section, select the destination host target (Management Agent) that is reporting to the OMS, where you want to stage these entity files.

   To select a location on the Management Agent target to host the files, you must log in to the host target and select a location to host the files.
5. Click **Submit**.
6. To verify the status of the submitted job, from **Enterprise** menu, select **Job,** then click **Activity.**

15.11 Maintaining Software Library

To maintain the health and proper functionality of the Software Library, the administrator who configured the Software Library, or the Designer who has administration access on it must perform the tasks listed here.

This section includes:

- Periodic Maintenance Tasks
- Re-Importing Oracle Owned Entity Files
- Removing (and Migrating) Software Library Storage Location
- Removing a Referenced Storage Location
- Deactivating and Activating a Storage Location
- Scheduling Purge Job
- Backing Up Software Library

15.11.1 Periodic Maintenance Tasks

Periodically, the Administrator must perform the following tasks for proper functioning of the Software Library:

- Refresh the Software Library regularly to compute the free and used disk space. To do so, on the Administration page, in the upload file locations tab, select the storage location. From the **Actions** menu, select **Refresh.** On successful refersh, a confirmation is displayed. Alternately, you can search for the periodic refresh job `SWLIBREFRESHLOCSTATS`, and edit the schedule and other attributes to suit your requirements. By default, this job is scheduled to run every 6 hours.
- Purge deleted entities to conserve disk space. To do so, see Section 15.11.6. Alternatively, you can search for the periodic purge job `SWLIBPURGE`, and edit the schedule and attributes to suit your requirements. By default, this job is scheduled to run every 24 hours.
- Check accessibility of the configured Software Library locations. To do so, on the Administration page, in the upload file locations tab, select the storage location. From the **Actions** menu, select **Check Accessibility**.

15.11.2 Re-Importing Oracle Owned Entity Files

Note: Re-importing metadata applies only to the Oracle owned files, which means all the entity files that ship with the Enterprise Manager product by default. The metadata of User owned entity files cannot be recovered through the Re-import functionality.

Re-Importing the metadata of Oracle owned entity files is not a periodic activity. Re-import helps to recover the metadata files in one of the following situations:

- If you delete the file system location where the metadata was imported. For example, `/scratch/swlib1/`
- If the import job submitted while creating the first upload location fails.

To re-import the metadata of Oracle owned files, do the following:

1. In Cloud Control, from **Setup** menu, select **Provisioning and Patching,** and then click **Software Library.**
2. On the Software Library Administration page, in the Upload File Location tab, from **Actions** menu, select **Re-Import Metadata** option to submit a job that re-initiates the re-import process.

15.11.3 Removing (and Migrating) Software Library Storage Location

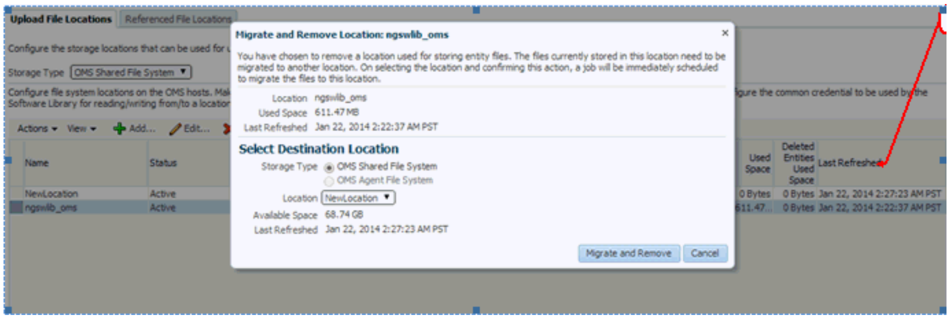
Software Library Storage Administrators have the required privileges to delete a storage location. If a storage location is not in use, then you can remove it instantly. However, if it is in use, then you must migrate the contents to another location so that the entities using these files continue to remain usable.

Before removing a storage location that is currently in use, you are prompted for an alternate location for the files. After you select an alternate location, a migration job is submitted, and the location is marked as **Migrating**. After successful migration of the entity files to the new location, the location configuration is deleted. In case of any errors during migration, the location is marked as **Inactive**. Once the errors are fixed, and the storage administrator ascertains that the location is good to use, the location is marked as **Active**.

> **Note:** To remove a location from OMS Agent File System or Referenced Agent File System storage, you must have a view privilege on the credentials for the location being removed, and the alternate location where the files are migrated.

To delete a configured storage location, perform the following steps:

1. In Cloud Control, from **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Administration page, select the storage location, and click **Migrate and Remove**.



Migrate and Remove Location: ngswlib_oms

You have chosen to remove a location used for storing entity files. The files currently stored in this location need to be migrated to another location. On selecting the location and confirming this action, a job will be immediately scheduled to migrate the files to this location.

Location ngswlib_oms
Used Space 611.47 MB
Last Refreshed Jan 22, 2014 2:22:37 AM PST

Select Destination Location

Storage Type ● OMS Shared File System
○ OMS Agent File System
Location NewLocation
Available Space 68.74 GB
Last Refreshed Jan 22, 2014 2:27:23 AM PST

Name	Status	Used Space	Deleted Entities Used Space	Last Refreshed
NewLocation	Active	0 Bytes	0 Bytes	Jan 22, 2014 2:27:23 AM PST
ngswlib_oms	Active	611.47...	0 Bytes	Jan 22, 2014 2:22:37 AM PST

Upload File Locations
Referenced File Locations
Configure the storage locations that can be used for u
Storage Type OMS Shared File System
Configure file system locations on the OMS hosts. Mak
Software Library for reading/writing from/to a location
igure the common credential to be used by the
Actions
View
Add...
Edit...
Migrate and Remove
Cancel

3. On the Migrate and Remove Locations dialog box, select either **OMS Shared File System** or **OMS Agent File System.** A list of available active storage locations are displayed, select one and click **Migrate and Remove.**

> **Note:** At least one upload location (either OMS Shared File System or OMS Agent File System) should be present. The last active upload location cannot be removed. Use either Cloud Control or EMCLI to migrate an upload location to another upload location of either upload storage types (either OMS Shared File System or OMS Agent File System). For example, you can migrate an OMS Shared File System storage location to an OMS Agent File System storage location. Even the reverse operation is supported. However, note that this type of migration, across storage types, is supported specifically for *upload* storage types, and is not applicable for the reference storage types.
>
> For a storage location, if there are no active upload locations (OMS Shared File System or OMS Agent File System), then the **Migrate and Remove** button will not be enabled for that location
>
> To migrate the files from one upload location to another, you can also use the EM CLI verb `emcli remove_swlib_storage_location`. For more information about this command, see Section 15.4.

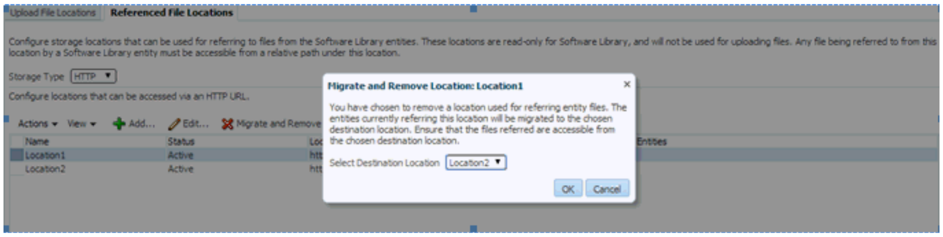
4. In the confirmation dialog box, click **Migrate and Remove** to submit a job, which on successful completion deletes the storage entry from the table.

Note: When one storage location is migrated to another location, for example, from `/vol/swlib1` to `/vol/swlib2`, the file system contents of the source location (`/vol/swlib1`) are not deleted during the migration. However, going forward, the source location and the files are never referenced by Software Library.

15.11.4 Removing a Referenced Storage Location

To remove a configured reference storage location (HTTP/ NFS/ External Agent Location), perform the following steps:

1. In Cloud Control, from **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Administration page, select the storage location, and click **Migrate and Remove**.



Configure storage locations that can be used for referring to files from the Software Library entities. These locations are read-only for Software Library, and will not be used for uploading files. Any file being referred to from this location by a Software Library entity must be accessible from a relative path under this location.

Storage Type: HTTP

Configure locations that can be accessed via an HTTP URL.

Name	Status	Loc	Entities
Location1	Active	htt	
Location2	Active	htt	

Migrate and Remove Location: Location1

You have chosen to remove a location used for referring entity files. The entities currently referring this location will be migrated to the chosen destination location. Ensure that the files referred are accessible from the chosen destination location.

Select Destination Location: Location2

Note: If a location is not in use, then select the storage location and click **OK** to remove the location. However, if some entities are using a storage location, then you must migrate the files to another location before deleting the existing location.

3. To migrate the files to another location from the Migrate and Remove Locations dialog box, select a destination location from the list of active storage locations, then click **OK.**

Note: If there are no active locations of the same storage type available for migration, then the **Migrate and Remove** button is disabled for the location.

15.11.5 Deactivating and Activating a Storage Location

An upload or reference storage location can be deactivated. Once deactivated, the status of the storage location becomes **Inactive** and no further uploads will be allowed to the upload storage location. A storage location in an inactive state can be activated to be put back in use.

To deactivate a storage location, follow these steps:

1. In Cloud Control, from **Setup** menu, select **Provisioning and Patching,** then select **Software Library**.
2. On the Software Library Administration page, select the storage location that is in an **Active** state, then from the **Actions** menu select **Deactivate**. A confirmation dialog is displayed.

3. Upon confirmation, the storage location is deactivated, and state changes to **Inactive**.

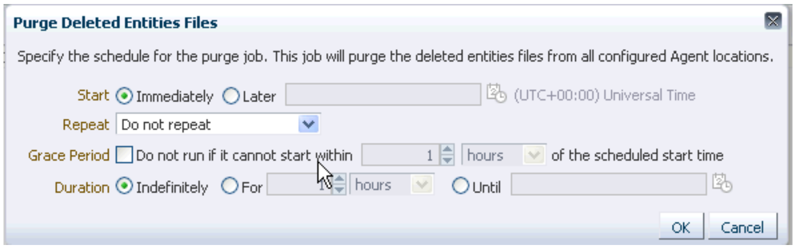
To activate a storage location, follow these steps:

1. In Cloud Control, from **Setup** menu, select **Provisioning and Patching,** then select **Software Library**.
2. On the Software Library Administration page, select the storage location that is in an inactive state, then from the **Actions** menu select **Activate**. A confirmation dialog is displayed.
3. Upon confirmation, the storage location is activated, and state changes to **Active**.

15.11.6 Scheduling Purge Job

Starting with Enterprise Manager 12*c* the purge job can be scheduled. To do so follow these steps:

1. In Cloud Control, from **Setup** menu, select **Provisioning and Patching,** then select **Software Library.**
2. On the Software Library Administration page, select the storage location, and from the Actions menu select **Purge**. The following dialog box appears where you can schedule the purge job:



Purge Deleted Entities Files

Specify the schedule for the purge job. This job will purge the deleted entities files from all configured Agent locations.

Start ● Immediately ○ Later (UTC+00:00) Universal Time

Repeat Do not repeat

Grace Period □ Do not run if it cannot start within 1 hours of the scheduled start time

Duration ● Indefinitely ○ For 1 hours ○ Until

3. Enter all the details and click **OK** to submit the job, on successful completion of the job all the deleted entities are removed from the storage location.

15.11.7 Backing Up Software Library

For information about backing up your Software Library, see the chapter on "Backing Up and Recovering Enterprise Manager" in the Enterprise Manager Advanced Installation and Configurtion Guide.

16

Managing Plug-Ins

This chapter provides an overview of Plug-In Manager, and describes how you can use it to view, deploy, administer, and undeploy plug-ins.

In particular, this chapter covers the following:

- Introduction to Plug-ins
- Workflow of Plug-In Deployment
- Introduction to Plug-In Manager
- Knowing Your Plug-Ins
- Downloading, Deploying, and Upgrading Plug-Ins
- Undeploying Plug-Ins
- Advanced Operations with Plug-Ins
- Troubleshooting

16.1 Getting Started

Table 16–1 provides a quick view of the sections within this chapter that might be of interest to you.

Table 16–1 Getting Started

User	Sections of Interest
Beginner	■ Introduction to Plug-ins ■ Workflow of Plug-In Deployment ■ Introduction to Plug-In Manager
Basic	■ Workflow of Plug-In Deployment ■ Customizing Your View ■ Checking the Availability of Plug-Ins ■ Viewing Information about Plug-Ins

Table 16–1 (Cont.) Getting Started

User	Sections of Interest
Intermediate	■ Customizing Your View ■ Checking the Availability of Plug-Ins ■ Viewing Information about Plug-Ins ■ Downloading Plug-Ins ■ Deploying Plug-Ins to Oracle Management Service (Reduce OMS Restart time and Downtime) ■ Upgrading Plug-Ins Deployed to Oracle Management Service ■ Deploying Plug-Ins on Oracle Management Agent ■ Upgrading Plug-Ins Deployed to Oracle Management Agent ■ Undeploying Plug-Ins from Oracle Management Service ■ Undeploying Plug-Ins from Oracle Management Agent ■ Troubleshooting
Advanced	■ Re-deploying Plug-Ins on Oracle Management Agent ■ Deploying Plug-In Patches While Deploying or Upgrading Management Agent (Create Custom Plug-In Update) ■ Troubleshooting

16.2 Introduction to Plug-ins

This section covers the following:

- Enterprise Manager 12c Extensibility Paradigm
- Plug-Ins
- Plug-Ins Deployed by Default
- Plug-In Releases
- Roles Required to Manage Plug-Ins

16.2.1 Enterprise Manager 12c Extensibility Paradigm

Enterprise Manager is system management software that delivers centralized monitoring, administration, and life cycle management functionality for the complete IT infrastructure, including systems running Oracle and non-Oracle technologies.

Enterprise Manager has grown in size and magnitude over the years to offer a spectrum of powerful IT management and monitoring solutions. This growth has lead to changes in managing support for new features, enhancements, and bug fixes.

Considering these developments, Oracle has carefully redesigned the architecture of Enterprise Manager in such a way that the framework or the core base on which the product runs is clearly separated from the layer that offers IT solutions by means of features. This new architecture implemented in Enterprise Manager 12*c* enables Oracle to provide a much stronger framework with capabilities to extend itself seamlessly from time to time for supporting new features and enhancements.

You no longer have to wait for the next release of Enterprise Manager to access the latest monitoring features for released products. The pluggable framework in Enterprise Manager 12*c* allows target support to be included soon after new versions of targets ship. You can install a new Enterprise Manager system or upgrade an existing one, as soon as the Enterprise Manager release is made available by Oracle.

Based on the new design, the Enterprise Manager 12*c* architecture constitutes the following logical parts:

- EM Platform: Consists of a set of closely integrated UI and backend services that most monitoring and management functionality in Enterprise Manager depends on. Examples of platform subsystems include the Enterprise Manager target and metric model, the job, event, and provisioning framework. The platform also includes Oracle Management Agent (Management Agent) as well as the core background services such as the data loader, job dispatcher, and notification manager. The platform is delivered as part of an Enterprise Manager release, and can only be upgraded by upgrading to a new version of Enterprise Manager.
- EM Plug-ins: Modules that can be plugged to an existing Enterprise Manager Platform to provide target management or other vertical functionality in Enterprise Manager. Plug-ins offer special solutions or new features, for example, connectivity to My Oracle Support, and extend monitoring and management capability to Enterprise Manager, which enable you to monitor a particular target on a host. Plug-ins work in conjunction with OMS and Management Agent to offer monitoring services, and therefore they are deployed to the OMS as well as the Management Agent.

The plug-in releases happen more often than Enterprise Manager Core Platform releases. The plug-ins enable Enterprise Manager 12*c* to be updated with new features and management support for the latest Oracle product releases, without having to wait for the next platform release to provide such functionality.

16.2.2 Plug-Ins

Plug-ins are modules that can be plugged into an existing Enterprise Manager Cloud Control deployment to extend target management or other vertical functionality in Enterprise Manager.

At a high level, plug-ins contain archives for monitoring and discovering OMS instances and Management Agents. The archives contain Java and SQL codes, and metadata.

16.2.3 Plug-Ins Deployed by Default

As a part of Enterprise Manager Cloud Control installation, a set of basic plug-ins is deployed by default. You can deploy other plug-ins to extend the basic functionality of Enterprise Manager Cloud Control.

The plug-ins that are deployed by default, or are shipped out of box are as follows.

- Oracle Database: oracle.sysman.db
- Oracle Fusion Middleware: oracle.sysman.emas
- Oracle MOS (My Oracle Support): oracle.sysman.mos
- Oracle Exadata: oracle.sysman.xa
- Oracle Cloud Framework: oracle.sysman.cfw

Note: For a brief description about these plug-ins, see *Oracle Enterprise Manager Basic Installation Guide.*

16.2.4 Plug-In Releases

Plug-in releases happen more often than Enterprise Manager Core platform releases. This new pluggable framework enables Enterprise Manager Cloud Control to be updated with management support for the latest Oracle product releases, without having to wait for the next platform release to provide such functionality.

For example, when a new version of Oracle Database is released, you can simply download and deploy the latest Oracle Database plug-in, which will include management support for the latest Oracle Database release. You can also work with plug-ins in Offline Mode.

16.2.5 Roles Required to Manage Plug-Ins

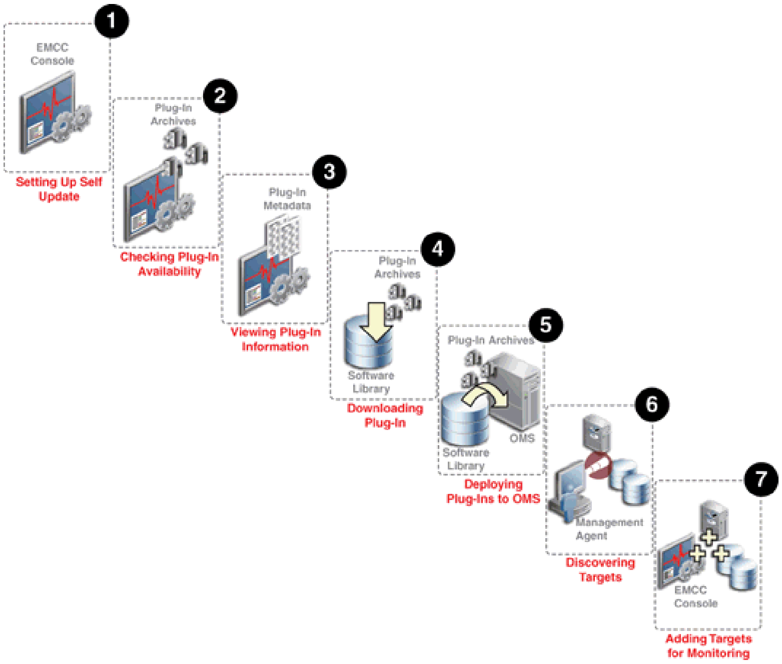
You need one or more of the following out-of-the-box roles to download, manage, and deploy plug-ins:

- EM_PLUGIN_OMS_ADMIN: Enables you to manage the lifecycle of plug-ins on Management Server instances.
- EM_PLUGIN_AGENT_ADMIN: Enables you to manage the lifecycle of plug-ins on Management Agents.
- EM_PLUGIN_USER: Enables you to view the plug-in lifecycle console.

16.3 Workflow of Plug-In Deployment

Figure 16–1 illustrates the workflow of plug-in deployment—how you typically set up the Enterprise Manager infrastructure, deploy plug-ins to OMS, and discovery and monitor targets using the deployed plug-ins.

Figure 16–1 Plug-In Deployment Workflow



Step 1: Setting up Self-Update Console

Self Update console is a common dashboard used for reviewing, downloading, and applying new updates available for Enterprise Manager. The console frees you from having to monitor multiple channels to get informed about new updates that are available from Oracle. The updates automatically downloaded by Self Update include plug-ins. For checking the availability of plug-ins and downloading them to Enterprise Manager, you must set up the Self Update Console. Set up the Self Update Console as described in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Step 2: Checking Plug-In Availability

Checking the plug-in availability essentially refers to the act of verifying whether the plug-ins are available on My Oracle Support for download and deployment in Enterprise Manager. This is a prerequisite before downloading plug-ins. To check plug-in availability, follow the steps outlined in Section 16.5.2.

Step 3: Viewing Plug-In Information

Viewing plug-in information refers to the act of viewing basic information related to a particular plug-in, such as the plug-in ID, the plug-in release number, and other basic information. You must view plug-in information to understand what targets and operating systems are certified for plug-ins. You can also check whether or not a particular plug-in has already been deployed. To view plug-in information, follow the steps outlined in Section 16.5.3.

Step 4: Downloading Plug-Ins

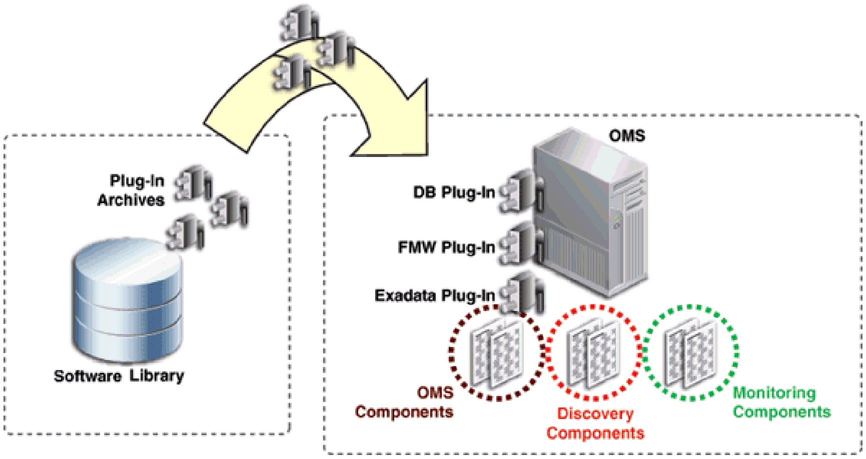
Downloading plug-ins is the act of downloading plug-in archives or components, and its metadata, from My Oracle Support to Oracle Software Library (Software Library), so that they can be deployed suitably for discovering and monitoring certain targets. If you find that a particular target is not being monitored by plug-ins, you must download the required plug-ins. You can download both in online mode and offline mode. To download plug-ins, follow the steps outlined in Section 16.6.1.

Step 5: Deploying Plug-Ins to OMS

Deploying plug-ins to OMS is the next natural course of action once a plug-in is downloaded from My Oracle Support. This is to ensure the OMS capabilities are extended to either manage a new target or to add a new vertical capability. The installation and configuration of plug-ins on the OMS is essentially referred to as *Deployment.* Some plug-ins, when deployed, require the OMS to be re-started.

Figure 16–2 illustrates how plug-ins are deployed to the OMS.

Figure 16–2 Deploying Plug-Ins to OMS



When the plug-in archives are deployed from the Software Library to the OMS, the OMS receives three different components for each plug-in, namely the OMS plug-in components, the discovery plug-in components, and the monitoring plug-in components.

Discovery plug-in components are those components that help in the discovery of unmanaged targets. Monitoring plug-in components are those components that help in the adding of discovered targets to Enterprise Manager Cloud Control Console for monitoring purposes.

To deploy plug-ins on OMS, follow the steps outlined in Section 16.6.2.

Step 6: Discovering Targets

Discovering targets refers to the process of identifying unmanaged hosts and targets in your environment. During discovery of targets, the discovery components of plug-ins are deployed to the Management Agent home. Note that this enables Enterprise Manager Cloud Control to only identify a new target in your environment; it however does not monitor the target.

After converting unmanaged hosts to managed hosts in Enterprise Manager Cloud Control, you must configure automatic discovery of targets on those hosts so that the unmanaged targets running on those hosts can be identified.

For instructions to configure automatic discovery of targets on managed hosts, refer to the Discovering and Monitoring Targets section in the Oracle Enterprise Manager Cloud Control Administrator's Guide, using the following URL:

`http://docs.oracle.com/cd/E24628_01/doc.121/e24473/discovery.htm#CBAGJFHC`

> **Note:** When you configure automatic discovery of targets on managed hosts, discovery plug-in components are copied to Management Agent.

Once you have configured automatic discovery of targets on managed hosts, you must regularly check for discovered targets so that they can be promoted and monitored in Enterprise Manager Cloud Control.

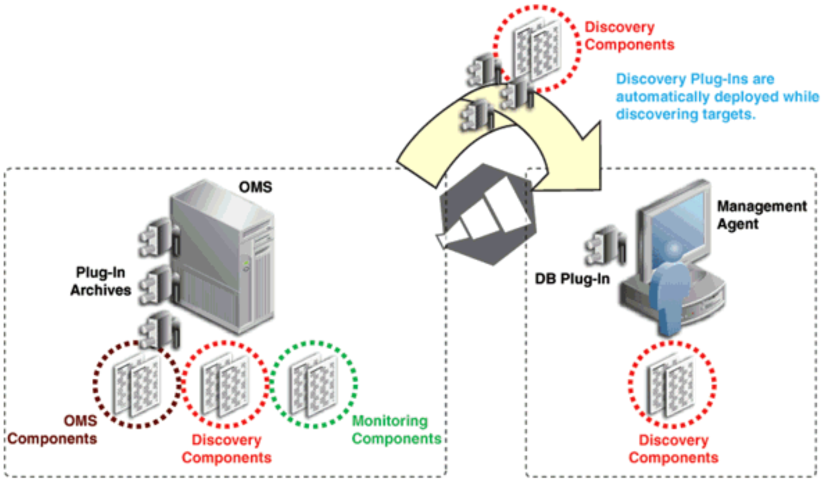
For instructions to check for and promote discovered targets to managed status, refer to the Discovering and Monitoring Targets section in the Oracle Enterprise Manager Cloud Control Administrator's Guide, using the following URL:

`http://docs.oracle.com/cd/E24628_01/doc.121/e24473/discovery.htm#CBAFHEHC`

> **Note:** The plug-in for a specific target type is automatically deployed to the Management Agent that will monitor targets of that type. For example, if you discover a database target, the discovery plug-in component of the database plug-in is automatically deployed to the Management Agent installed on the database host.
>
> However, this is true only for initial deployment. All subsequent updates to the Management Agent plug-in must be explicitly deployed. For example, if you want to deploy a new version of the database plug-in on the Management Agent, you must initiate the deployment using the instructions outlined in *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.
>
> Similarly, any patches to be applied on the Management Agent (framework or plug-in) must be explicitly applied using the instructions outlined in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Figure 16–3 illustrates how the discovery plug-in components are deployed to the Management Agent while discovering new targets.

Figure 16–3 Discovering Targets

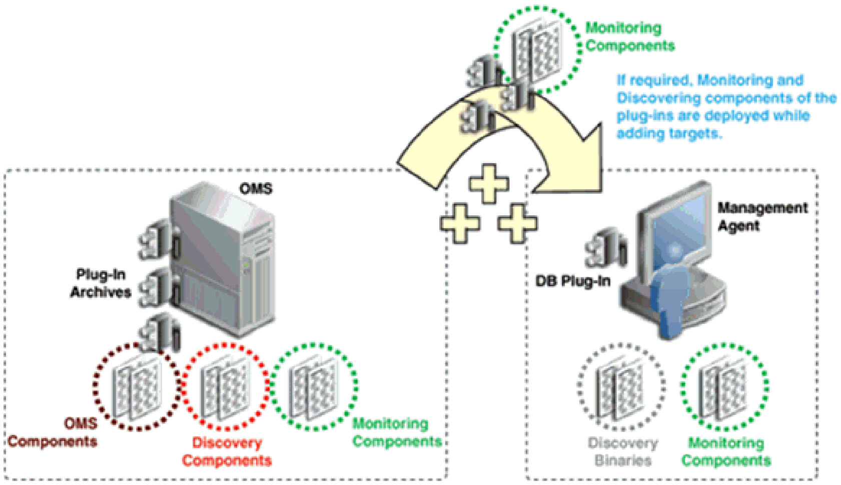


Step 7: Adding Targets for Monitoring

Once the targets are discovered, they are added to the infrastructure, so that they can be monitored in Enterprise Manager Cloud Control. While adding targets, the monitoring components of plug-ins are deployed to the Management Agent home.

Figure 16–4 illustrates how the monitoring plug-in components are deployed to the Management Agent while adding targets.

Figure 16–4 Adding Targets



16.4 Introduction to Plug-In Manager

Plug-In Manager is a feature of Enterprise Manager Cloud Control, that serves as a single window solution for performing all plug-in deployment-related activities, through GUI as well as CLI. Using Plug-In Manager, you can:

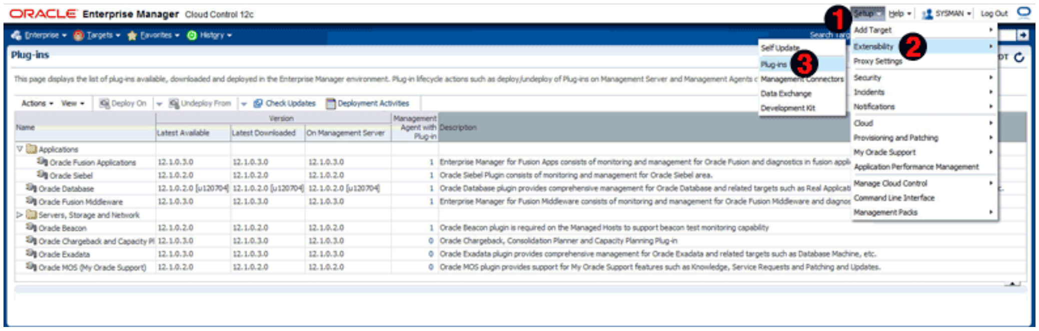
- View plug-ins available for download; plug-ins that have been downloaded; and plug-ins that have been deployed to Cloud Control.
- View certification and critical information about plug-ins such as the name of the plug-in, the vendor who supplied it, the plug-in ID and version, and a short description.
- Deploy plug-ins on OMS.
- Deploy and re-deploy plug-in on Management Agent.
- Create custom plug-in update.
- Undeploy plug-ins from OMS and Management Agent.
- View the status of a plug-in deployment operations.

16.4.1 Accessing Plug-In Manager

To access the Plug-In Manager console, from the **Setup** menu, select **Extensibility,** and then select **Plug-ins.**

Figure 16–5 illustrates how you can access Plug-in Manager.

Figure 16–5 Navigating to Plug-In Manager



Plug-ins

This page displays the list of plug-ins available, downloaded and deployed in the Enterprise Manager environment. Plug-in lifecycle actions such as deploy/undeploy of Plug-ins on Management Server and Management Agents c

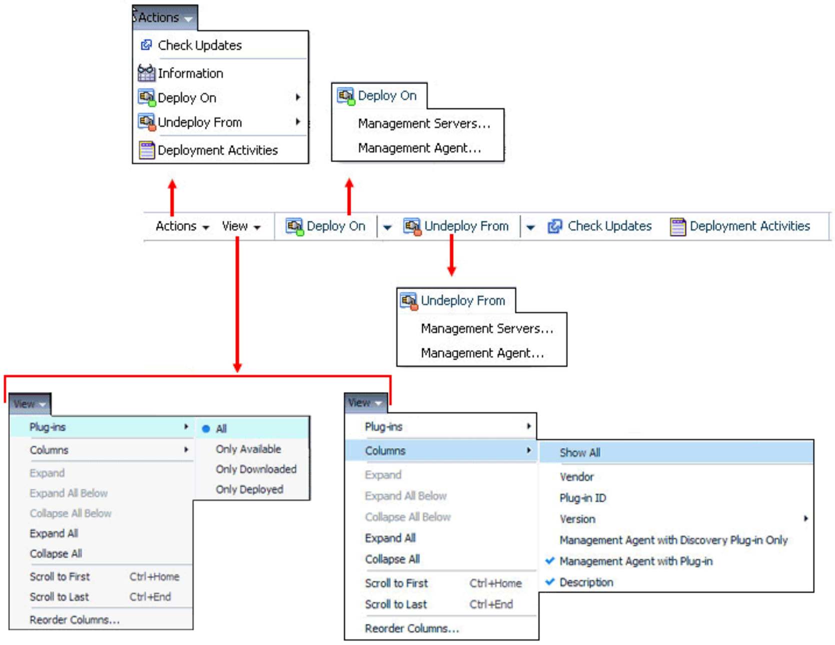
Name	Version			Management Agent with Plug-in	Description
	Latest Available	Latest Downloaded	On Management Server		
Applications					
Oracle Fusion Applications	12.1.0.3.0	12.1.0.3.0	12.1.0.3.0	1	Enterprise Manager for Fusion Apps consists of monitoring and management for Oracle Fusion and diagnostics in fusion appli
Oracle Siebel	12.1.0.2.0	12.1.0.2.0	12.1.0.2.0	1	Oracle Siebel Plugin consists of monitoring and management for Oracle Siebel area.
Oracle Database	12.1.0.2.0 [u120704]	12.1.0.2.0 [u120704]	12.1.0.2.0 [u120704]	1	Oracle Database plugin provides comprehensive management for Oracle Database and related targets such as Real Applicati
Oracle Fusion Middleware	12.1.0.3.0	12.1.0.3.0	12.1.0.3.0	1	Enterprise Manager for Fusion Middleware consists of monitoring and management for Oracle Fusion Middleware and diagnos
Servers, Storage and Network					
Oracle Beacon	12.1.0.2.0	12.1.0.2.0	12.1.0.2.0	1	Oracle Beacon plugin is required on the Managed Hosts to support beacon test monitoring capability
Oracle Chargeback and Capacity Pl	12.1.0.3.0	12.1.0.3.0	12.1.0.3.0	0	Oracle Chargeback, Consolidation Planner and Capacity Planning Plug-in
Oracle Exadata	12.1.0.3.0	12.1.0.3.0	12.1.0.3.0	0	Oracle Exadata plugin provides comprehensive management for Oracle Exadata and related targets such as Database Machine, etc.
Oracle MOS (My Oracle Support)	12.1.0.2.0	12.1.0.2.0	12.1.0.2.0	0	Oracle MOS plugin provides support for My Oracle Support features such as Knowledge, Service Requests and Patching and Updates.

16.4.2 Performing Operations Using Plug-In Manager

Using Plug-in Manager, you can deploy, upgrade, redeploy, and undeploy plug-ins.

Figure 16–6 shows the operations you can perform using the Plug-In Manager.

Figure 16–6 Plug-In Manager Operations



16.5 Knowing Your Plug-Ins

This section explains the following:

- Customizing Your View
- Checking the Availability of Plug-Ins
- Viewing Information about Plug-Ins

16.5.1 Customizing Your View

This section tells you how to customize your view, and organize the plug-ins and columns displayed.

16.5.1.1 Customizing Displayed Plug-Ins

Over a period of time, as you download and deploy plug-ins, the number of plug-ins on your list increases. You can sort these plug-ins to view only the ones you require, for example, only the plug-ins available, or only the plug-ins deployed.

In order to customize your view, follow these steps.

1. From the **View** menu, select **Plug-Ins.**
2. From the Plug-Ins menu, select one of the following filters.
   - **All,** using this filter, you can view all plug-ins, including available, downloaded, and deployed plug-ins.
   - **Only Available,** using this filter, you can view the plug-ins that are available for download.
   - **Only Downloaded,** using this filter, you can view the plug-ins that are downloaded.
   - **Only Deployed,** using this filter, you can view the plug-ins that are deployed.

16.5.1.2 Customizing Displayed Columns

By default, only a few columns of information are displayed. Optionally, you can either enable other columns of your interest, or disable ones that are already displayed.

In order to customize the displayed columns, follow these steps.

1. From the **View** menu, select **Columns.**
2. From the Columns menu, select one of the following filters for columns.
   - **Show All,** using this filter, you can view all columns.
   - **Vendor,** using this filter, you can view information about the vendor.
   - **Plug-In Id,** using this filter, you can view the plug-in id.
   - **Version,** this filter has three options you can choose from. They are as follows.
     - **Latest Available,** using this filter, you can view the newest plug-ins that are available.
     - **Latest Downloaded,** using this filter, you can view the plug-ins that have been downloaded recently.
     - **On Management Server,** using this filter, you can view the plug-ins that are deployed to the OMS.
   - **Management Agent with Discovery Plug-Ins Only,** this filter displays the Management Agent which has only Discovery Plug-Ins deployed.
   - **Management Agent with Plug-In,** this filter displays the Management Agent which has any plug-in deployed on it.
   - **Description,** this filter displays the description of the plug-ins.

16.5.2 Checking the Availability of Plug-Ins

To check the availability of plug-ins, follow these steps:

1. Set up the Self Update Console as described in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
2. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.**
3. On the Plug-ins page, in the Latest Available column of the table, check whether the plug-ins are available.

   To refresh the list of available plug-ins, click **Check Updates.** Note that clicking Check Updates will take you to the Self Update page.

16.5.3 Viewing Information about Plug-Ins

This section gives you more information on plug-ins, and functions related to plug-ins. This section covers the following sections:

- Differentiating Plug-In Releases from Enterprise Manager Platform Releases
- Identifying Plug-In ID
- Viewing Targets and Operating Systems Certified for Deployed Plug-Ins
- Viewing Plug-In Dependencies
- Verifying Deployed Plug-Ins

16.5.3.1 Differentiating Plug-In Releases from Enterprise Manager Platform Releases

Plug-ins have independent release cycles and release numbers, which may or may not be tied to Enterprise Manager Cloud Control product releases and release numbers.

Plug-in releases typically happen more often than Enterprise Manager platform releases.

Figure 16–7 describes how plug-in releases are numbered.

Figure 16–7 Plug-In Release Number Format

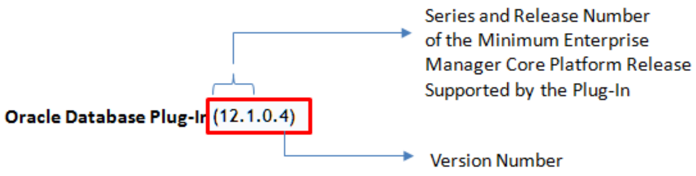
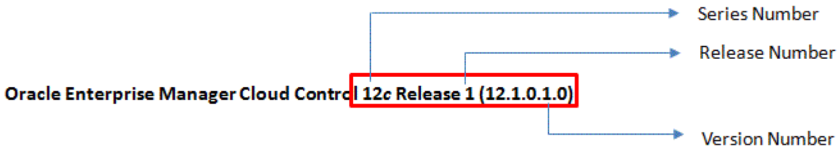

Series and Release Number of the Minimum Enterprise Manager Core Platform Release Supported by the Plug-In
Oracle Database Plug-In (12.1.0.4)
Version Number

Figure 16–8 describes how Enterprise Manager platform releases are numbered.

Figure 16–8 Enterprise Manager Core Platform Release Number Format


Series Number
Release Number
Oracle Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1.0)
Version Number

16.5.3.2 Identifying Plug-In ID

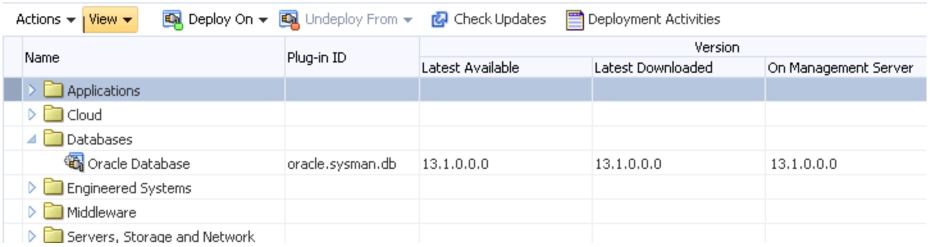
To identify the ID of a plug-in, follow these steps:

1. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.**
2. On the Plug-ins page, in the Plug-in ID column of the table, note the plug-in ID of the plug-in of your interest.

   If you do not see this column, from the **View** menu, select **Columns,** then select **Plug-in ID.**

Figure 16–9 illustrates how you can identify the plug-in ID of the Oracle Database plug-in.

Figure 16–9 Identifying Plug-In ID



Name	Plug-in ID	Version		
		Latest Available	Latest Downloaded	On Management Server
Applications				
Cloud				
Databases				
Oracle Database	oracle.sysman.db	13.1.0.0.0	13.1.0.0.0	13.1.0.0.0
Engineered Systems				
Middleware				
Servers, Storage and Network				

16.5.3.3 Viewing Targets and Operating Systems Certified for Deployed Plug-Ins

To view a list of targets and operating systems certified for a deployed plug-in, follow these steps:

1. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.**
2. On the Plug-ins page, select the plug-in of your interest, and from the **Actions** menu, select **Information.**
3. On the Plug-in Information page, in the **General** tab, review the information provided in the **Certified Targets** and **Certified Operating Systems** tables.

16.5.3.4 Viewing Plug-In Dependencies

To view the dependencies of the preferred plug-in, follow these steps:

1. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.**
2. On the Plug-ins page, select the plug-in of your interest, and from the **Actions** menu, select **Information.**
3. On the Plug-in Information page, in the **Dependencies tab,** review the information provided in the tables.

16.5.3.5 Verifying Deployed Plug-Ins

To view and administer the deployed plug-ins, from the **Setup** menu, select **Extensibility,** then select **Plug-ins.** Enterprise Manager Cloud Control displays the Plug-ins page, which is essentially the *Plug-In Manager* console.

To identify the OMS instances on which the plug-in of your interest is deployed, follow these steps using Enterprise Manager Cloud Control Console:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins.**
2. On the Plug-ins page, select the plug-in of your interest, and from the **Actions** menu, select **Information.**

3. On the Plug-in Information page, in the **Management Servers** tab, review the Oracle Management Services on which the plug-in is deployed.

To identify the Management Agents on which the plug-in of your interest is deployed, follow these steps using Enterprise Manager Cloud Control Console:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins.**
2. On the Plug-ins page, select the plug-in of your interest, and from the **Actions** menu, select **Information.**
3. On the Plug-in Information page, in the **Management Agent** tab, review the Management Agents on which the plug-in is deployed.

To identify the Plug-ins deployed on OMS, on EM CLI, log in to EMCLI, and enter the following command. The command displays a list of all the plug-ins deployed on the OMS.

```
$emcli login

-username=<EM Console Username>

[-password=<EM Console Password>]

[-force]

$emcli list_plugins_on_server
```

Example 16–1 Sample List of Plug-Ins Deployed on OMS

```
example.com:7654_Management_Service
```

Plug-in Name	Plug-in ID	Version (Revision)
Oracle Database	oracle.sysman.db	12.1.0.4.0
Oracle Fusion Middleware	oracle.sysman.emas	12.1.0.4.0
Oracle MOS (My Oracle Support)	oracle.sysman.mos	12.1.0.5.0
Oracle Exadata	oracle.sysman.xa	12.1.0.4.0

To identify and view all the Plug-ins deployed on Management Agent, on EM CLI, enter the following command:

```
$emcli list_plugins_on_agent

[agent_names="agent1,agent2,agent3..."

[-all] [-include_discovery]
```

Example 16–2 Sample List of Plug-ins Deployed on Management Agent

```
emcli list_plugins_on_agent -agent_names=agent1.example.com:3872
Lists plug-ins on the agent agent1.example.com

emcli list_plugins_on_agent -agent_
names=agent1.example.com:3872,agent2.example.com:3872 -include_discovery
Lists plug-ins on both the agents provided along with their discovery components

emcli list_plugins_on_agent -agent_names='agent*,st*93'
Lists plug-ins on all agents with name matching one of the regular expressions
agent* or st*93
```

```
emcli list_plugins_on_agent -all
Lists plug-ins on all the management agents.
```

16.6 Downloading, Deploying, and Upgrading Plug-Ins

This section explains the following:

- Downloading Plug-Ins
- Deploying Plug-Ins to Oracle Management Service (Reduce OMS Restart time and Downtime)
- Upgrading Plug-Ins Deployed to Oracle Management Service
- Deploying Plug-Ins on Oracle Management Agent
- Upgrading Plug-Ins Deployed to Oracle Management Agent

16.6.1 Downloading Plug-Ins

You can download the plug-ins in online or offline mode. Online refers to an environment where you have Internet connectivity to the Enterprise Manager Store. Offline refers to an environment where you do not have Internet connectivity. This section contains the following sections:

- Downloading Plug-Ins in Online Mode
- Downloading Plug-Ins in Offline Mode
- Importing Catalog Archives
- Importing Plug-In Archives

16.6.1.1 Downloading Plug-Ins in Online Mode

To download the plug-ins in online mode, follow these steps:

1. From the **Setup** menu, select **Extensibility,** then select **Self Update.**
2. On the Self Update page, in the table, click on **Plug-in**.
3. On the Plug-in Updates page, select the plug-in available for download, and click **Download.**

   Multiple selection of plug-ins is not supported.
4. In the Schedule Download dialog, select an appropriate option to schedule the download. You can also select Immediately which schedules the job for immediate action. Select **Notify Once downloaded** if you want to be informed once the download is complete.
5. Click **Select.**

   Enterprise Manager Cloud Control submits a job to download the selected plug-in from the Enterprise Manager Store to the Software Library.

   A confirmation dialog appears to confirm that the job has been submitted successfully. In this confirmation dialog, you can click **Job Details** to track the status of the job.

16.6.1.2 Downloading Plug-Ins in Offline Mode

To download the plug-ins in offline mode, follow these steps:

1. Set Enterprise Manager Cloud Control to Offline Mode. To do so, follow these steps.

   a. From the **Setup** menu, select **Provisioning and Patching**, then select **Offline Patching.**

   b. In the Online and Offline Settings tab, select **Offline.**

2. From the **Setup** menu, select **Extensibility,** then select **Self Update.**

3. On the Self Update page, click **Check for Updates**.

   A message appears with the following URL to an Oracle site from where the updates catalog file can be downloaded.

   ```
   https://updates.oracle.com/Orion/Download/download_
   patch/p9348486_112000_Generic.zip
   ```

4. From an Internet-enabled computer, download the catalog file using the aforementioned URL.

5. Copy the downloaded catalog file to the OMS host or the Management Agent host where you plan to deploy the plug-ins.

6. Import the catalog file to Enterprise Manager. For instructions, refer to Importing Catalog Archives.

7. On the Self Update page, in the table, click **Plug-in.**

8. On the Plug-in Updates page, select the imported update that is available for download. Click **Download.**

   A message appears with a URL to an Oracle site from where the update can be downloaded.

9. From a computer that is connected to the internet, download the update using the aforementioned URL.

10. Copy the downloaded file to the OMS host or the Management Agent host where you plan to deploy the plug-ins.

11. Import the downloaded plug-in archive to Enterprise Manager. For instructions, refer to Importing Plug-In Archives.

16.6.1.3 Importing Catalog Archives

To import a catalog archive, follow these steps:

1. Download the catalog archive as described in Section 16.6.1.2.

2. Execute the following `emcli` command to import the downloaded catalog archive.

```
$emcli import_update_catalog

-file="file"

-omslocal

emcli import_update_catalog

-file="file"

-host="hostname"

[-credential_set_name="setname"] | -credential_name="name"
-credential_owner="owner"
```

Example 16–3 Sample for Importing Catalog Archive

```
$emcli import_update_catalog
        -file="/u01/common/p9984818_121000_Generic.zip"
        -omslocal
Imports the master catalog file p9984818_121000_Generic.zip. The file must exist
on the OMS host. In a multiple OMS setup, the request can be processed by any OMS,
so the file should be accessible from the OMS processing the request. This means
that the file must be kept on a shared location that is accessible from all the
OMS instances.
$emcli import_update_catalog
        -file="/u01/common/p9984818_121000_Generic.zip"
        -host="host1.example.com"
        -credential_set_name="HostCredsNormal"

Imports the master catalog file p9984818_121000_Generic.zip that is present on the
host host1.example.com. The host must be a managed host target in Enterprise
Manager, and the Management Agent on this host must be up and running. The
preferred unprivileged credentials for host host1.example.com are used to retrieve
the remote file.
```

16.6.1.4 Importing Plug-In Archives

Import plug-in archives to Oracle Software Library in the following cases:

- When you want to deploy any non-Oracle plug-ins, that is, plug-ins that have been created by a company other than Oracle, and are not available for download on the Self Update console.
- When you want to import other types of entity archives when Self Update is used in offline mode.

To import a plug-in archive, follow these steps:

1. Download the external archive as described in the previous section.
2. Set up the Enterprise Manager Command Line (EM CLI) utility. To do so, from the **Setup** menu, click **Command Line Interface.** Follow the instructions outlined on the Enterprise Manager Command Line Interface Download page.
3. Import the external archive in one of the following ways, depending on where EMCLI is installed.
   - If Enterprise Manager server is on the system on which you downloaded the plug-in archive (`*.opar` file), run the following command:

     ```
     $emcli import_update

     -file=”<path to *.opar file>”

     -omslocal
     ```

     The `-omslocal` flag indicates that the plug-in archive path mentioned in the `-file` option is directly accessible to the EM server.
   - If Enterprise Manager server is on a different system than the plug-in archive, run the following command:

     ```
     $emcli import_update

     -file=”<path to *.opar file you created>”

     -host="host1.example.com"

     -credential_name="host1_creds"
     ```

```
-credential_owner="admin1"
```

The command syntax is as follows:

`-file`: The absolute path to the *.opar file on the system where you created the archive.

`-host`: The target name for a host target where the file is available.

`-credential_name`: The name of the credentials on the remote system you are connecting to.

`-credential_owner`: The owner of the credentials on the host system you are connecting to.

Note: As an alternative to the previous step, you can also run the following command:

```
$emcli import_update
      -file="<path to *.opar file you created>"
      -host="hostname"
      -credential_set_name="setname"
```

`-credential_set_name`: The set name of the preferred credential stored in the Management Repository for the host target. It can be one of the following:

`HostCredsNormal`: The default unprivileged credential set.

`HostCredsPriv`: The privileged credential set.

16.6.2 Deploying Plug-Ins to Oracle Management Service (Reduce OMS Restart time and Downtime)

You can deploy multiple plug-ins to an OMS instance in graphical interface or command line interface.

Note:

- To view a visual demonstration on how you can deploy a plug-in to the OMS and discover targets, access the following URL and click **Begin Video.**

  https://apex.oracle.com/pls/apex/f?p=44785:24:942581250672901::NO::P24_CONTENT_ID,P24_PREV_PAGE:6000,1

- Plug-ins must be deployed on the OMS prior to being deployed on Management Agents.
- In a multi OMS environment, Plug-in Manager automates plug-in deployment on all the management servers.
- A plug-in upgrade failure could put the Management Repository in an inconsistent state. Oracle recommends that your repository database should be running in archive log mode, and that your backup policies are in place.
- The deployment time varies from one plug-in to another, depending on the volume of data populated in the Management Repository. A page is displayed that allows you to monitor the deployment status, as described in Section 16.6.2.1.
- The deployment of some plug-ins requires the OMS to be stopped, and then restarted. This process occurs automatically as part of the plug-in deployment process.
- While deploying plug-ins to the OMS, OMS plug-in components, discovery plug-in components, and monitoring plug-in components are deployed to the OMS.

To deploy plug-ins to the OMS in graphical mode, follow these steps:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins.**
2. On the Plug-ins page, select the plug-in you want to deploy.

Note: Alternately, you can move to the next step and select the plug-ins after the next step.

---

3. From the **Deploy On** menu, select **Management Servers.**
4. In the Deploy Plug-ins on Management Servers: Plug-ins page, verify that the plug-in details on the lower portion of the screen are correct. Additionally, you can add more plug-ins by clicking **Add.**
5. Select the **Use Last Successful Prerequisite** check box to skip the prerequisite checks.

   The check box is enabled only if the plug-in had successfully cleared the prerequisites checks within the last 24 hours and was not deployed.
6. Click **Next.**
7. In the Deploy Plug-ins on Management Servers: Prerequisite Checks page, wait for the prerequisite checks to complete (if not cleared already) and click **Next.**

8. In the Deploy Plug-ins on Management Servers: Repository page, specify the Management Repository SYS credentials. Click **Named** option to select the saved credentials or click **New** option to enter new credentials.

   The newly entered credentials will be automatically saved for future deployments, after the deployment is successful.

9. Click **Next.**

10. The Deploy Plug-ins on Management Servers: Review page displays the OMSs and the statuses of the OMSs where the plug-ins will be deployed, and the plug-ins. Verify that all the details are correct and click **Deploy.**

To deploy plug-ins to the OMS in silent mode, follow these steps:

1. Log in to `EMCLI` as follows:

   ```
   $ORACLE_HOME/bin/emcli login -username=sysman
   ```

2. Run the following command if the emcli client is an old version, and does not have all required verbs:

   ```
   $ORACLE_HOME/bin/emcli sync
   ```

3. To deploy the plug-ins on the OMS, run the following command:

   ```
   $emcli deploy_plugin_on_server

   -plugin="plug-in_id[:version]

   [-sys_password=sys_password]

   [-prereq_check]"
   ```

   Note: For information on plug-in id, refer to Section 16.5.3.2.

   For example,

   ```
   $emcli deploy_plugin_on_server
   -plugin="oracle.sysman.db:12.1.0.2.0;oracle.sysman.emas:12.1.
   0.2.0"
   ```

   Note: The procedure for plug-in deployment remains the same even in a multi-OMS environment. Enterprise Manager automatically detects whether it is a single-OMS or a multi-OMS environment and in case of a multi-OMS environment, Enterprise Manager automatically deploys the selected plug-in on all OMS instances.

   If the plug-in deployment fails on a primary OMS, where the Administration Server is running, then you must first address the issue, and then resume the deployment or restore the system from backup. If however, the plug-in deployment fails on a non-primary OMS, identify the cause for the failure. If there is a fix or a workaround, fix the problem, and perform the same steps again. The system automatically detects which OMS instances do not have the plug-ins deployed, and deploys them on those servers.

   If the problem persists, contact Oracle Support.

16.6.2.1 Tracking the Deployment Status of Plug-Ins on Oracle Management Service

This section describes the procedure of monitoring the deployment status of plug-ins that do not require down time as well as those that do require down time.

To monitor the status of deployment and undeployment operations of plug-ins that require down time, execute the following command:

```
emctl status oms -details
```

To monitor the status of deployment and undeployment operations for plug-ins that do not require down time, follow these steps:

1. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.**
2. On the Plug-ins page, do one of the following:
   - From the **Actions** menu, select **Deployment Activities.**
   - Select a plug-in, and click the **Recent Deployment Activities** tab at the bottom of the page. Alternatively, you can also run the following command using EMCLI.

     ```
     $emcli get_plugin_deployment_status -plugin_id=<plugin_id>
     ```

16.6.3 Upgrading Plug-Ins Deployed to Oracle Management Service

This section contains the following sections:

- Upgrading Across Plug-In Versions Deployed to Oracle Management Service
- Upgrading Across Plug-In Revisions Within a Plug-In Version Deployed to Oracle Management Service

16.6.3.1 Upgrading Across Plug-In Versions Deployed to Oracle Management Service

You can upgrade across plug-in versions, that is, from one plug-in version to another higher plug-in version or a revision of another higher plug-in version. For example, from Oracle Database plug-in version 12.1.0.1.0 to version 12.1.0.2.0, or from Oracle Database plug-in version 12.1.0.1.0 to version 12.1.0.2.0 [u120427].

To upgrade across plug-in versions deployed to the OMS, follow these steps:

1. Check for the latest available versions and revisions in the Enterprise Manager Store as described in Section 16.5.2.
2. Download them as described in Section 16.6.1.
3. Deploy them to the OMS as described in Section 16.6.2.

16.6.3.2 Upgrading Across Plug-In Revisions Within a Plug-In Version Deployed to Oracle Management Service

This section describes how you can upgrade across plug-in revisions within a plug-in version, that is, from one revision of a plug-in version to another revision of the same plug-in version. For example, from Oracle Database plug-in version 12.1.0.2.0 [u120427] to version 12.1.0.2.0 [u120502].

To upgrade the plug-in revisions deployed to the OMS, follow these steps:

1. Check for the latest available revisions in the Enterprise Manager Store as described in Section 16.5.2.

2. Download them as described in Section 16.6.1.
3. Apply the patches required for the plug-in revision.
   a. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.**
   b. On the Plug-ins page, select the plug-in revision you downloaded, and from the **Actions** menu, select **Information.**
   c. On the Plug-in Information page, in the **General** tab, in the **Dependencies** section, in the **Bug Fixes Required** table, click **View Bug Fixes.**
   d. In the Required Bug Fixes dialog, note the bug numbers listed in the Bug Number column of the Management Server Fixes table.
   e. Download the patches that contain the fixes for the bugs you noted in the previous step.
   f. Apply the downloaded patches on the OMS.
4. Deploy the latest available revisions to the OMS as described in Section 16.6.4.

16.6.4 Deploying Plug-Ins on Oracle Management Agent

While installing a Management Agent using the Add Host Targets Wizard, all the core discovery plug-ins available on the OMS are automatically deployed to the Management Agent.

For information about discovery plug-ins, refer to Section 16.5.3.

If you want to deploy any additional plug-ins after installing the Management Agent, then follow these steps:

1. Set up the Self Update console.
2. Check whether the plug-ins are available on Enterprise Manager store. For instructions refer to Section 16.5.2.
3. Download the available plug-ins. For instructions, refer to Section 16.6.1.
4. Deploy the downloaded plug-ins to the Management Agent.
   a. From the **Setup** menu, select **Extensibility**, then select **Plug-ins.**
   b. On the Plug-ins page, select the plug-in you want to deploy.
   c. From the **Deploy On** menu, select **Management Agent.**
   d. Follow the steps mentioned in the Deploy Plug-ins on Management Agent dialogue box.
   e. Click **Deploy.**

To deploy plug-ins in EM CLI, use the following command:

```
$emcli deploy_plugin_on_agent

-agent_names="agent1[;agent2...]"

-plugin="plug-in_id[:version"]

[-discovery_only]
```

To deploy the latest revision of the plug-in, run the command above with an additional argument: `allow_revision_update.`

16.6.4.1 Tracking the Deployment Status of Plug-Ins on Oracle Management Agent

To track the deployment status of plug-ins on Management Agent, refer to Section 16.6.2.1.

16.6.5 Upgrading Plug-Ins Deployed to Oracle Management Agent

You can upgrade across plug-in versions, that is, from one plug-in version to another, higher plug-in version or a revision of another, higher plug-in version. For example, from Oracle Database plug-in version 12.1.0.1.0 to version 12.1.0.2.0, or from Oracle Database plug-in version 12.1.0.1.0 to version 12.1.0.2.0 [u120427].

> **Note:** You will upgrade the plug-in versions and revisions only on Management Agents that are already installed in your environment.
>
> When a plug-in is deployed explicitly or a target is promoted on new Management Agents, then the latest plug-in version and revision automatically gets included from the OMS.

To upgrade across plug-in versions deployed to the Management Agent, follow these steps:

1. Check for the latest available versions and revisions in the Enterprise Manager Store as described in Section 16.5.2.
2. Download them as described in Section 16.6.1.
3. From the **Setup** menu, select **Extensibility,** then select **Plug-ins.**
4. On the Plug-ins page, select the plug-in you want to upgrade.
5. From the **Deploy On** menu, select **Management Agent.**
6. In the Deploy Plug-in on Management Agent dialog, select the version or revision of the plug-in you want to upgrade to., and click **Continue.**
7. Select the preferred Management Agent to upgrade the plug-in on, and click **Continue.** Then click **Next.** And then click **Deploy.**
8. On the Confirmation dialog, click **Close.**

16.7 Undeploying Plug-Ins

This section explains the following:

- Undeploying Plug-Ins from Oracle Management Service
- Undeploying Plug-Ins from Oracle Management Agent

16.7.1 Undeploying Plug-Ins from Oracle Management Service

To undeploy plug-ins from the OMS, follow the steps:

1. First, undeploy all plug-ins from all Management Agents. To do so, follow the steps mentioned in Section 16.7.2.
2. From the **Setup** menu, select **Extensibility**, then select **Plug-ins.**
3. On the Plug-ins page, select the plug-in you want to undeploy, and from the **Actions** menu, select **Undeploy From,** then select **Management Servers**.

4. In the Undeploy Plug-in From Management Server dialog, enter the Management Repository SYS password, and click **Continue.** Then click **Undeploy.**
5. On the Confirmation dialog, click **Close.**

   To monitor the undeployment operation, click **Show Status.**

To undeploy a plug-in in EM CLI, use the following command:

```
$emcli undeploy_plugin_from_server

 -plugin="plug-inId"

 [-sys_password="sys_password"]
```

> **Note:** When a metadata plug-in is undeployed/redeployed, it is recomended that you run the following command. The command should be run in each OMS environment instance.
>
> ```
> $emcli metric_control -command=flush_metadata_cache
> ```
>
> If you want to undeploy only the plug-ins from the OMS, and not the entire Enterprise Manager system, then use the Plug-ins page within the Enterprise Manager Cloud Control Console. **Do NOT use runInstaller to undeploy only the plug-ins.**

16.7.2 Undeploying Plug-Ins from Oracle Management Agent

To undeploy plug-ins from the Management Agent, follow the steps:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins.**
2. On the Plug-ins page, select the plug-in you want to undeploy, and from the **Actions** menu, select **Undeploy From,** then select **Management Agent**.
3. In the Undeploy Plug-in From Management Agent dialog, click **Add** and add the Management Agents from which you want to undeploy the plug-in. Click **Continue.** Then click **Undeploy.**
4. On the Confirmation dialog, click **Close.**

   To monitor the undeployment operation, click **Show Status.**

> **Note:** Undeploying a plug-in from Management Agent removes all the targets that were monitored by the plug-in.
>
> Undeployment of a plug-in from the Management Agent restarts the Management Agent. The Management Agent does not monitor any target during downtime.

To undeploy a plug-in using EM CLI, use the following command:

```
$emcli undeploy_plugin_from_agent

-plugin="pluginId"

{-agent_names="agent1[;agent2...]" | -all_discovery_only_agents}
```

To undeploy all versions of `oracle.sysman.db2` plug-ins from all Management Agents where only Discovery Plug-ins are deployed, use the following command:

```
$emcli  undeploy_plugin_from_agent -plugin=oracle.sysman.db2
-all_discovery_only_agents
```

16.8 Advanced Operations with Plug-Ins

This section explains the following:

- Re-deploying Plug-Ins on Oracle Management Agent
- Deploying Plug-In Patches While Deploying or Upgrading Management Agent (Create Custom Plug-In Update)

16.8.1 Re-deploying Plug-Ins on Oracle Management Agent

Using re-deploy option, you can re-deploy plug-ins on Oracle Management Agent. The re-deploy plug-in option reconfigures the same plug-in on the Management Agent, and does not change the configuration details.

```
$emcli redeploy_plugin_on_agent

{-agent_names="agent1[;agent2...]" | -group_name="group1"}

-plugin="plug-in_id:version"

[-redeploy_noprompt]
```

Note: While using this option, note that the existing plug-in home will be overwritten, and all applied patches will be lost.

The re-deploy wizard displays the following warning message:

Re-deployment of a plug-in overwrites the existing OracleHome of a plug-in and you will lose any patch(es) that has been applied on plug-in OracleHome.

However, if you have enabled `-redeploy_nopromt` option, then the warning message will not be displayed.

To continue, click **Yes.**

The redeploy command cannot be used on multiple Management Agents without having Custom Plug-in Update for a plug-in.

Note: After a metadata plug-in is redeployed, it is recomended that you run the following command.

```
$emcli metric_control -command=flush_metadata_cache
```

The command should be run on all OMS instances.

16.8.2 Deploying Plug-In Patches While Deploying or Upgrading Management Agent (Create Custom Plug-In Update)

When a new plug-in is released, it can be downloaded using Self-update. If there are defects with the Management Agent plug-ins, Oracle then releases O-patch style patches. While plug-ins get deployed automatically during target discovery on Management Agents, patches for the plug-ins have to be applied on each plug-in manually.

Custom plug-in update is the user copy of the plug-in, along with patches applied to it. Using the Create Custom Plug-In Update command allows you to create a custom copy of plug-in along with the patches applied in self update. Once the patches are applied, you can create a custom plug-in update of the plug-ins on that Management

Agent. The custom plug-in update then becomes a gold image for that plug-in with all the patches applied on that Oracle Home, along with the base plug-in binaries.

After the Custom Plug-in Update is created, any plug-in deployment operation for the plug-in on any Management Agent, using either UI or EMCLI, the new custom copy will be deployed instead of the Oracle supplied version. In this way you don't have to reapply the plug-in patches manually on each plugin home of agent. This custome plug-in image is also used by Agent deployment ot upgrade activity so that the plug-ins getting deployed on these agents are with the patch included.

There are two methods of creating Custom Plug-in Update. The following sections describe the two methods.

- Creating Custom Plug-In Update Using EMCLI*(recommended)*
- Creating Custom Plug-In Update Using EDK

16.8.2.1 Creating Custom Plug-In Update Using EMCLI

To create a custom plug-in update, follow these steps:

1. Select a test Management Agent which is up and running on which the preferred plug-in is already deployed. Apply any patches that you want to apply on this plug-in.
2. Perform the required testing.
3. Create a custom plug-in update using the following command:

   ```
   $emcli create_custom_plugin_update
   ```

   ```
   -agent_name="agent_name"
   ```

   ```
   -plugin_id="plugin_id"
   ```

   > **Note:** To overwrite and update your current custom plug-in update that is stored in a repository, use the `overwrite` option.
   >
   > `$emcli create_custom_plugin_update`
   >
   > -agent_name="agent_name"
   >
   > `-plugin_id="plugin_id"`
   >
   > [-overwrite]
   >
   > This command creates and imports a custom plug-in update from an existing Management Agent where the selected plug-in is deployed. The custom plug-in update will be used for all subsequent plug-in deployments on any Management Agent, in place of Oracle supplied versions.
   >
   > Custom plug-in update is created as per plug-in type. If a custom plug-in update is created, and after three days, a patch is applied, in order to include the patch, the custom plug-in update will have to be created again.

To view a list of all Custom Plug-in Updates created, run the following command.

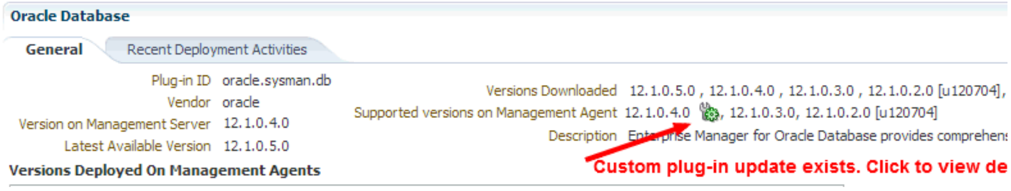
```
$emcli list_custom_plugin_updates
```

To view a a list of patches included in a particular Custom Plug-in Update, run the following command.

```
$emcli list_patches_in_custom_plugin_update -plugin=<plugin_
id>:<version> [-discovery]
```

On the Plug-in Manager console, when you select a plug-in, if a Custom Plug-in Update exists, an icon is displayed beside the version identifier, indicating that that particular plug-in version is customized in the environment, with a list of patches. Figure 16–10 displays the Custom Plug-in Update icon. Once the custom plug-in update exists, it will be used by the Management Agent for deployment and upgrade automatically.

Figure 16–10 Custom Plug-in Update Icon



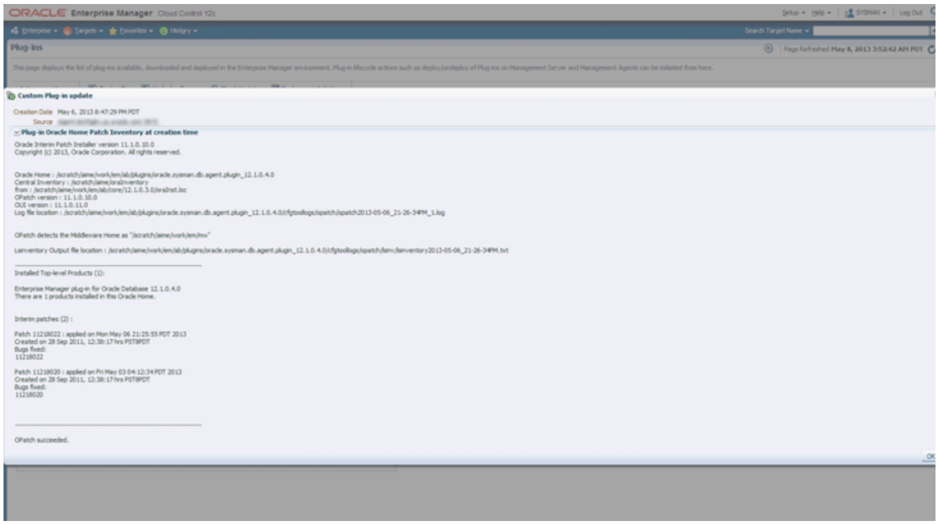
Plug-in ID oracle.sysman.db
Vendor oracle
Version on Management Server 12.1.0.4.0
Latest Available Version 12.1.0.5.0
Versions Deployed On Management Agents

Versions Downloaded 12.1.0.5.0 , 12.1.0.4.0 , 12.1.0.3.0 , 12.1.0.2.0 [u120704],
Supported versions on Management Agent 12.1.0.4.0 ⚙, 12.1.0.3.0, 12.1.0.2.0 [u120704]
Description Enterprise Manager for Oracle Database provides comprehen

Custom plug-in update exists. Click to view de

When you click the Custom Plug-in Update icon, the page that displays the information on Custom Plug-in Update is displayed. Figure 16–11 displays the Custom Plug-in Update information page.

Figure 16–11 Custom Plug-in Update Information Page


ORACLE Enterprise Manager Cloud Control 12c
Setup
Help
SYSMAN
Log Out
Enterprise
Targets
Favorites
History
Search Target Name
Plug-ins
Page Refreshed May 8, 2013 3:52:42 AM PDT
OK

This page displays the list of plug-ins available, downloaded and deployed in the Enterprise Manager environment. Plug-in lifecycle actions such as deploy/undeploy of Plug-ins on Management Server and Management Agents can be initiated from here.

Custom Plug-in update

Creation Date May 6, 2013 8:47:29 PM PDT

Source [redacted]

Plug-in Oracle Home Patch Inventory at creation time

```
Oracle Interim Patch Installer version 11.1.0.10.0
Copyright (c) 2013, Oracle Corporation. All rights reserved.


Oracle Home : /scratch/aime/work/em/ab/plugins/oracle.sysman.db.agent.plugin_12.1.0.4.0
Central Inventory : /scratch/aime/oraInventory
from : /scratch/aime/work/em/ab/core/12.1.0.3.0/oraInst.loc
OPatch version : 11.1.0.10.0
OUI version : 11.1.0.11.0
Log file location : /scratch/aime/work/em/ab/plugins/oracle.sysman.db.agent.plugin_12.1.0.4.0/cfgtoollogs/opatch/opatch2013-05-06_21-26-34PM_1.log


OPatch detects the Middleware Home as "/scratch/aime/work/em/mw"

Lsinventory Output file location : /scratch/aime/work/em/ab/plugins/oracle.sysman.db.agent.plugin_12.1.0.4.0/cfgtoollogs/opatch/lsinv/lsinventory2013-05-06_21-26-34PM.txt

--------------------------------------------------------------------------------
Installed Top-level Products (1):

Enterprise Manager plug-in for Oracle Database 12.1.0.4.0
There are 1 products installed in this Oracle Home.


Interim patches (2) :

Patch 11218022 : applied on Mon May 06 21:25:55 PDT 2013
Created on 28 Sep 2011, 12:38:17 hrs PST8PDT
Bugs fixed:
11218022

Patch 11218020 : applied on Fri May 03 04:12:34 PDT 2013
Created on 28 Sep 2011, 12:38:17 hrs PST8PDT
Bugs fixed:
11218020



--------------------------------------------------------------------------------

OPatch succeeded.
```

16.8.2.2 Creating Custom Plug-In Update Using EDK

To create custom plug-in update using EDK, follow these steps.

1. Download EDK, using the UI or EMCLI, on the Management Agent Host.

   To download EDK using UI, from the **Setup** menu, select **Extensibility,** and then select **Development Kit.**

   To download EDK using EMCLI, run the following command.

   ```
   $emcli get_ext_dev_kit
   ```

2. Run the following command.

   ```
   $empdk create_custom_plugin_update -out_dir <output dir>
   -agent_state_dir <agent_state_dir>
   ```

```
-agent_oracle_home <agent_oracle_home>
```

```
-plug_id <plugin_id>
```

For help with empdk commands, run the following command.

```
$/empdk -help
```

The plug-in update is saved to on a local directory as a .zip file. The .zip file has to be copied to an OMS instance. Once the .zip file is created, from the OMS Home, run the following command to import the custom plug-in update.

```
$emcli import_plugin_update -archive=<archive path>
```

On the Plug-in Manager console, when you select a plug-in, if a Custom Plug-in Update exists, an icon is displayed beside the version identifier, indicating that that particular plug-in version is customized in the environment, with a list of patches. Figure 1-1 displays the Custom Plug-in Update icon.

16.9 Troubleshooting

This section contains information on troubleshooting plug-in related issues. The following sections are covered in this section:

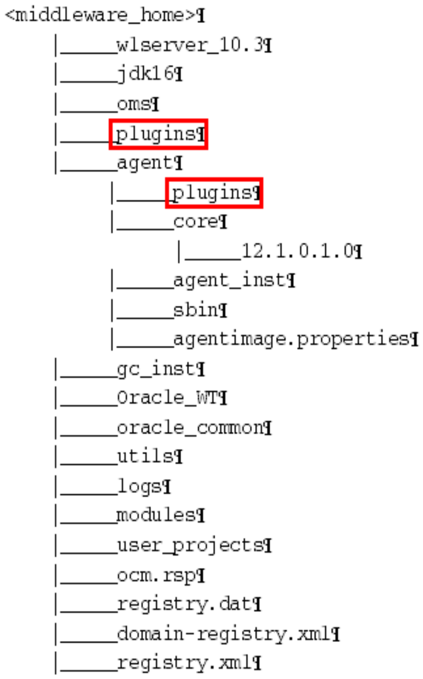
- Understanding Plug-In Homes
- Troubleshooting OMS Plug-In Deployment and Upgrade Issues
  - Troubleshooting OMS Plug-In Deployment Issues
  - Rollback and Resume OMS Plug-In Upgrade
- Troubleshooting Management Agent Plug-In Deployment and Upgrade Issues
  - Troubleshooting Management Agent Plug-In Deployment Issues
  - Troubleshooting Management Agent Plug-In Upgrade Issues

16.9.1 Understanding Plug-In Homes

Plug-in homes are essentially Oracle homes that are dedicated for plug-ins. The plug-in home for plug-ins deployed to the OMS is different from the plug-in home for plug-ins deployed to the Management Agent. Each plug-in home will be its own ORACLE_HOME with a dependency on the OMS. Since plug-in homes are registered in the `oraInventory`, they should not be manually deleted or manipulated.

Figure 16–12 shows the plug-in homes for plug-ins deployed to Enterprise Manager Cloud Control 12*c* Release 1 (12.1.0.1) *(for OMS as well as for central agent).*

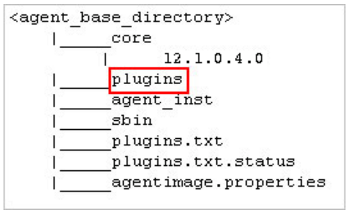
Figure 16–12 Plug-In Homes for Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) (for OMS as well as for Central Agent)



```
<middleware_home>¶
    |_____wlserver_10.3¶
    |_____jdk16¶
    |_____oms¶
    |_____plugins¶
    |_____agent¶
         |_____plugins¶
         |_____core¶
               |_____12.1.0.1.0¶
         |_____agent_inst¶
         |_____sbin¶
         |_____agentimage.properties¶
    |_____gc_inst¶
    |_____Oracle_WT¶
    |_____oracle_common¶
    |_____utils¶
    |_____logs¶
    |_____modules¶
    |_____user_projects¶
    |_____ocm.rsp¶
    |_____registry.dat¶
    |_____domain-registry.xml¶
    |_____registry.xml¶
```

Figure 16–13 indicates the plug-in home for plug-ins deployed to a standalone Management Agent of 12*c* Release 1 (12.1.0.1).

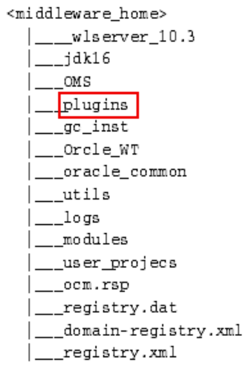
Figure 16–13 Plug-In Home for Standalone Oracle Management Agent 12c Release 4 (12.1.0.4)



```
<agent_base_directory>
    |_____core
          |     12.1.0.4.0
    |_____plugins
    |_____agent_inst
    |_____sbin
    |_____plugins.txt
    |_____plugins.txt.status
    |_____agentimage.properties
```

Figure 16–14 indicates the plug-in home for plug-ins deployed to Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) or later *(only for OMS)*.

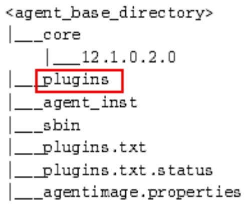
Figure 16–14 Plug-In Homes for Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2) (Only for OMS)



```
<middleware_home>
  |___wlserver_10.3
  |___jdk16
  |___OMS
  |___plugins
  |___gc_inst
  |___Orcle_WT
  |___oracle_common
  |___utils
  |___logs
  |___modules
  |___user_projecs
  |___ocm.rsp
  |___registry.dat
  |___domain-registry.xml
  |___registry.xml
```

Figure 16–15 indicates the plug-in home for plug-ins deployed to a central agent and a standalone Management Agent of 12c Release 2 (12.1.0.2) or later.

Figure 16–15 Plug-In Home for Central Agent and Standalone Oracle Management Agent 12c Release 2 (12.1.0.2)



```
<agent_base_directory>
|___core
    |___12.1.0.2.0
|___plugins
|___agent_inst
|___sbin
|___plugins.txt
|___plugins.txt.status
|___agentimage.properties
```

16.9.2 Troubleshooting OMS Plug-In Deployment and Upgrade Issues

If the deployment of a new plug-in fails, the system automatically recovers. When the automatic recovery is complete, all OMS instances are started. If the upgrade of an existing plug-in fails, manual system recovery is required.

This section provides troubleshooting tips related to the following topics:

- Troubleshooting OMS Plug-In Deployment Issues
- Rollback and Resume OMS Plug-In Upgrade

16.9.2.1 Troubleshooting OMS Plug-In Deployment Issues

If plug-in deployment to the OMS fails, first check the details of the deployment, using the following commands.

- If the OMS is down, use the following command.

  ```
  $emctl status oms -details
  ```

- If the OMS is running, use the following command.

  ```
  $emcli get_plugin_deployment_status
  ```

Note: When the status of the OMS is displayed, review the log files that are displayed in the output.

It is recommended that you take a backup of the Repository in case of a failure in the Recovery.

Review the `pluginca` log file available in the following location. Use them to debug the issue, and if you raise a service request to Oracle Support, then make sure you append these to the service request.

```
$<OMS_HOME>/cfgtoollogs/pluginca/*
```

Note: When you install an additional OMS by cloning an existing, running OMS instance, the plug-in deployed to the source OMS are automatically carried over to the cloned OMS as well. Therefore, you do not have to redeploy the plug-ins on the cloned OMS.

In case of multi OMS environment, the `OMS_HOME` in the log file path indicates the root folder of the OMS where the failure occurs.

For information about installing an additional OMS, refer to the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

16.9.2.2 Rollback and Resume OMS Plug-In Upgrade

If plug-in upgrade fails, then do one of the following:

- Raise a Service Request to find out if there is a possibility of recovering from the current Management Repository.
- Rollback to the latest backup of the Management Repository.
- If you have not taken a backup of the Management Repository, diagnose and resolve the issue that is causing the plug-in upgrade to fail.

  Then, run the following command to resume the plug-in upgrade:

  ```
  $<OMS_HOME>/bin/emctl resume_plugin_upgrade
  ```

  This command automatically detects and resumes the last failed upgrade session. Once the plug-in upgrade succeeds, the OMS restarts automatically. The same deployment ID is updated with the current status of the operation. In case of a multi-OMS environment, the plug-in upgrade happens on the first OMS, and then on all other additional OMS instances.
- If flashback is enabled, the section number will be printed.

16.9.3 Troubleshooting Management Agent Plug-In Deployment and Upgrade Issues

This section provides troubleshooting tips related to the following topics:

- Troubleshooting Management Agent Plug-In Deployment Issues
- Troubleshooting Management Agent Plug-In Upgrade Issues

16.9.3.1 Troubleshooting Management Agent Plug-In Deployment Issues

If plug-in deployment to the Management Agent fails, then review the log file available in the following locations.

```
agent_inst/sysman/log/*
```

```
agent_inst/sysman/registry.xml
```

```
agent_inst/install/logs/*
```

16.9.3.2 Troubleshooting Management Agent Plug-In Upgrade Issues

If plug-in upgrade fails, then review the log file available in the following locations.

- To review the log files using the UI, follow these steps.
  1. From the **Setup** menu, select **Extensibility,** and then select **Plug-ins.**
  2. Select the preferred plug-in, and review the information displayed in the **Recent Deployment Activities** tab.
  3. Click the link in the **Action** column for the preferred Management Agent. From the **Deployment Steps** tab, select the job name. Selecting the job name opens the job details wizard.
- The detailed logs for Management Agent upgrade and deployment are available at the following location.

  ```
  agent_inst/install/logs/agentplugindeploy_N.log
  ```

  In the aforementioned location, N refers to the internal ID. Check the latest log files in the location.
- While filing an SR, upload the following log files.

  ```
  agent_inst/install/logs/*
  ```

  ```
  agent_inst/sysman/log/*
  ```

  ```
  agent_inst/sysman/registry.xml
  ```

17 Patching Oracle Management Service and the Repository

Important: The patching methodology discussed in this chapter can only be used with Enterprise Manager Cloud Control Release 12.1.0.4 and later.

OPatchauto (introduced with version 11.1 of the OPatch utility) automates the patching process by generating custom patching instructions based your particular environment and then automatically applies the patch.

This chapter covers the following topics:

- OPatch Automation
- Required OPatchauto Parameters
- Prerequisites for Running OPatchauto
- Using OPatchauto

17.1 OPatch Automation

With OPatchauto, you can automatically patch a typical OMS configuration (core, plug-in homes) with minimal intervention.

OPatchauto performs many of the pre-patch checks such as:

- Configuration-based prerequisite checks
- Patch-based binary prerequisite checks

OPatchauto performs end-to-end configuration patching. Configuration patching is the process of patching a target based on its configuration. By incorporating the configuration information into the patch process, OPatchauto is able to simplify patching tasks by automating most of the steps.

17.1.1 Supported OMS Configurations and OPatchauto Patchability

- Single OMS – OMS application that runs from a single OMS instance of the system. OPatchauto performs patching and deployment operations
- Multiple OMS – OMS applications that run on two or more machines. The OMSs are connected by the Oracle WebLogic domain and separate managed servers. There is a one-to-one mapping between the managed servers and the separate OMS bits residing on a single machine. OPatchauto provides auto-generated bash

scripts (one per OMS instance) for UNIX based systems. For Windows, it only provides context-sensitive steps (text and HTML). For both cases, administrator needs to follow the steps given by OPatchAuto.

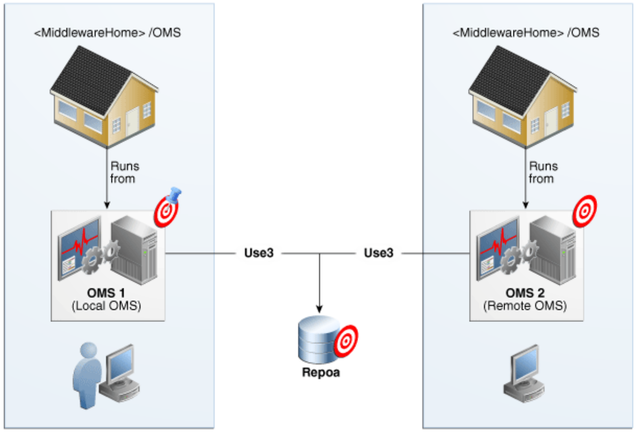
- Standby OMS – A HA (high availability) OMS configuration of Enterprise Manager which permits servicing requests when the primary OMS is down. When configured in this way, the standby OMS is managed by a different domain (managed by Oracle WebLogic Administration Server). OPatchauto provides auto-generated bash scripts (one per OMS instance) for UNIX based systems. For Windows, it only provides context-sensitive steps (text and HTML). For both cases, the administrator needs to follow the steps given by OPatchauto.
- Single Instance Database or Real Application Cluster - shared or Real Application Cluster (RAC)

Example: Multi-OMS System

The following figure illustrates a multi-OMS deployment. The following terms are used:

- *Administrator*: Person installing patches to the OMS core and plug-in homes.
- *Local OMS*: OMS instance on which the administrator runs OPatchauto.
- *Remote OMS*: OMS instances on other machines (within the same OMS domain as the local OMS) where the administrator has not started any patching operations.

Figure 17–1 Simple Multi-OMS System



For a single OMS system (primary), OPatchauto will execute the patching steps. For a multi-OMS UNIX system, OPatchauto generates bash scripts for execution, one per OMS instance; follow the instructions given by OPatchauto to find those scripts. (Requires OPatch 11.1.0.10.4 or later) For Windows multi-OMS systems, OPatchauto will generate customized patching instructions/commands for the environment in text and HTML formats; administrators must execute these instructions to patch the various Oracle Management Services.

17.1.2 OUI Inventory Configurations

Apart from the target (or) instance-based configurations, OPatchauto utilizes installation configuration relationships established in the Oracle Universal Installer (OUI) inventory as core and plug-in Oracle Homes. A typical OMS 12*c* home from the OUI inventory is organized as follows:

```
<Middleware Home>
 |_____platform home
 |_____plugin homes
      |_____oracle.sysman.db.oms.plugin_12.1.0.4.0
      |_____oracle.sysman.emas.oms.plugin_12.1.0.4.0
      |_____oracle.sysman.mos.oms.plugin_12.1.0.4.0
            .
            .
            .
```

17.1.3 Supported Patch Format

Beginning with Enterprise Manager Release 12.1.0.3, Enterprise Manager patches have been converted to a *System patch* format in order to support patch automation.

What is a System Patch?

A System patch contains several sub-patches whose locations are determined by a file called *bundle.xml* in the top level directory of the patch. The sub-patches are intended for different sub-systems of a system that correspond with the OMS core and plug-in home organization.

A typical System patch format is organized as follows:

```
<System patch location - directory>
|_____ Readme.txt (or) Readme.html
       bundle.xml
       automation
       |_____ apply_automation.xml
              rollback_automation.xml
       Sub-patch1
                |_____  etc/config/inventory.xml
                |_____ etc/config/actions.xml
                |_____ files/Subpatch1 'payload'
       Sub-patch2
                |_____  etc/config/inventory.xml
                |_____ etc/config/actions.xml
                |_____ files/Subpatch1 'payload'
```

Notes:

- For Enterprise Manager release 12.1.0.2 or below, OPatchauto is not supported for the released one-off patches. For these older releases, you must use OPatch and follow the patch README instructions.
- OPatchauto and System patches are only supported by Enterprise Manager release 12.1.0.3 and above.

17.1.4 Supported Patching Methodologies

OPatchauto supports rolling mode only for System patches without any automation (binary-only patching through OPatchauto). For all other artifacts (MRS, SQL), OPatchAuto only supports complete system downtime patching operations.

Refer to the patch README for the explicit information on supported patching methodologies.

17.2 Required OPatchauto Parameters

OPatchauto for the Enterprise Manager OMS will prompt for the following input parameters when performing patching operations. These parameters were determined at the time of Enterprise Manager installation.

- Oracle WebLogic Admin Sever URL & port number
- Oracle WebLogic Administration Server username
- Oracle WebLogic Administration Server password

Because OPatchauto requires this input for each patching operation, OPatchauto provides the ability to encrypt the username and password via WebLogic encryption APIs and pass this information using a property file when running OPatchauto *apply* and *rollback* operations. The next section discusses how to create a property file.

17.2.1 Creating a Property File

The automated patching functionality achieved using opatchauto expects WebLogic Administration Server URL and credentials as an input for patching and configuration detection operations. Primarily, the WebLogic Administration server is the host that manages the Managed Server where the OMS instance is deployed. If you do not want to set the credentials every time you are prompted while patching the OMS, you can update the property file. OPatch allows you to repeatedly provide the inputs using property file option.

> **Note:** Property file for a Primary OMS and Standby OMS are different, as they are in different domains.

To create an OPatch property file:

1. Run the following script to create the WebLogic encrypted configuration and key files.

   On UNIX:

   ```
   $ OPatch/wlskeys/createkeys.sh -oh <full path of platform home> -location
   <location to put the encrypted files>
   ```

   On Windows:

   ```
   $ OPatch\wlskeys\createkeys.cmd -oh <full path of platform home> -location
   <location to put the encrypted files>
   ```

   When prompted, enter the credentials of the Oracle WebLogic Administration Server that manages the Managed Server on which OMS instance is deployed. Two files are generated with the file names: `config` and `key`.

2. Create the property file with the following entries:

   ```
   AdminServerURL=t3s://<host address from where admin server is running>:<port of
   the admin server>
   AdminConfigFile=<'config' file location>
   AdminKeyFile=<'key' file location>

   The values for host address and port of admin server can be located by running
   the following 'emctl command' on a Oracle Home.

   $ORACLE_HOME/bin/emctl status oms -details
   Oracle Enterprise Manager Cloud Control 12c Release 4
   ```

```
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
Enter Enterprise Manager Root (SYSMAN) Password :
Console Server Host        : my_console_server.oracle.com
HTTP Console Port          : 7788
HTTPS Console Port         : 7799
HTTP Upload Port           : 4889
HTTPS Upload Port          : 4900
EM Instance Home           : /scratch/hkumars/oms_install_dir/gc_inst/em/EMGC_
OMS2
OMS Log Directory Location : /scratch/hkumars/oms_install_dir/gc_inst/em/EMGC_
OMS2/sysman/log
OMS is not configured with SLB or virtual hostname
Agent Upload is locked.
OMS Console is locked.
Active CA ID: 1
Console URL: https://my_console_server.oracle.com:7799/em
Upload URL: https://my_console_server.oracle.com:4900/empbs/upload

WLS Domain Information
Domain Name            : GCDomain
Admin Server Host      : my_admin_server.oracle.com
Admin Server HTTPS Port: 7101

Oracle Management Server Information
Managed Server Instance Name: EMGC_OMS2
Oracle Management Server Instance Host: my_console_server.oracle.com
WebTier is Up
Oracle Management Server is Up

BI Publisher Server is not functioning because of the following reason:
Unexpected error occurred. Check error and log files.
Check the following log files:
EM log files: /scratch/hkumars/oms_install_dir/gc_inst/em/EMGC_
OMS2/sysman/log/emctl.log, emoms.trc, emoms_pbs.trc
BI Publisher Server Logs: /scratch/hkumars/oms_install_dir/gc_inst/user_
projects/domains/GCDomain/servers/BIP2/logs/
BI Publisher Log        : /scratch/hkumars/oms_install_dir/gc_inst/user_
projects/domains/GCDomain/servers/BIP2/logs/bipublisher/bipublisher.log

Following is the example of how a property file (constructed by the above
mentioned guidelines) should appear:

AdminServerURL=t3s://my_admin_server.oracle.com:7101
AdminConfigFile=/scratch/hkumars/oms_install_dir/middleware/oms/config/config
AdminKeyFile=/scratch/hkumars/oms_install_dir/middleware/oms/config/key
```

Note: To retrieve the WebLogic Administration Server URL details, run the following commands on the OMS home that you are patching:

On Unix:

```
$ORACLE_HOME/bin/emctl status oms -details
```

On Windows:

```
%ORACLE_HOME%\bin\emctl.bat status oms -details
```

The command output contains the WebLogic Administration Server details. Here is an example on how to construct the URL with these output details.

Example:

```
WLS Domain Information

Domain Name : GCDomain
Admin Server Host : my_wls.oracle.com
Admin Server HTTPS Port: 7103
```

To construct the Administrator Server URL, use the following syntax:

```
t3s://<admin server host>:<port>
```

In this example, the URL translates as follows:

```
t3s://my_wls.oracle.com:7103
```

17.3 Prerequisites for Running OPatchauto

Before running an OPatchauto patching session, you must ensure the following configuration and inventory-based prerequisites are satisfied: Configuration-based conditions that have to be honored for OMS automation is given below.

- The Enterprise Manager Software library must be configured.
- The Oracle WebLogic Administration Server that controls the OMS instance (currently to be patched) through a managed server must be up and running.
- Ensure that the Oracle Database, which houses the OMS Management Repository, and its listener are up and running.
- Ensure that you have the latest version of OPatch in the OMS platform home of each host. The latest version of OPatch is available from My Oracle Support: OPatch release version 11.1.0.0.0 and Patch 6880880

  If you do not have the latest OPatch version, follow the instructions outlined in the My Oracle Support note 224346.1 available at:

  ```
  https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=224346.1
  ```

- Check your patch README to determine whether there are any specific prerequisites to be executed based on patch and patching methodologies.

Checking System Prerequisites

To make sure all prerequisite checks pass and no errors occur during the OPatchauto patching session, Oracle recommends running the following commands on each OMS instance (in your OMS system).

```
$<Platform Home>/OPatch/opatchauto apply -analyze
```

Must be run from the System patch location (for *apply* operations)

Note: OMS systems need not be shut down when running `opatchauto apply -analyze`.

Note: Check the Patch README and the instructions given for chosen patching methodologies.

OR

```
$<Platform Home>/OPatch/opatchauto rollback -analyze -id  <list of sub-patches to
be rolled back for System patch>
```

Example 17–1 `opatchauto apply -analyze` ***Output***

```
$opatchauto apply /scratch/patches/targetPatchingImplRegistration/1111118
-property_file property_file -analyze
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.

OPatchauto version : 11.1.0.10.4
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime/work/midnew270/oms
Log file location  :
 /scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-01_21-26-49PM_
1.log

OPatchauto log file:
 /scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-01_21-26-51PM_analyze.log

Configuration Validation: Success

Running apply prerequisite checks for sub-patch(es) "1111118" and Oracle Home
"/scratch/aime/work/midnew270/oms"...
Please monitor OPatch log file:
 /scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/1111118_May_01_2014_21_26_
49/ApplyPrereq2014-05-01_21-27-05PM_2.log
Sub-patch(es) "1111118" are successfully analyzed for Oracle Home
 "/scratch/aime/work/midnew270/oms"


Complete Summary
================

All log file names referenced below can be accessed from the directory
"/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/2014-05-01_21-26-49PM_
SystemPatch_1111118_1"

Prerequisites analysis summary:
-------------------------------

The following sub-patch(es) are applicable:

  Oracle Home Name   Sub-patches                                          Log file
  ----------------   -----------                                          --------
```

```
           oms12c1       1111118   1111118_ApplyPrereq2014-05-01_21-27-05PM_2.log

Log file location:
 /scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-01_21-26-51PM_analyze.log

OPatchauto succeeded.
```

Example 17–2 `opatchauto rollback -analyze` ***output***

```
$opatchauto rollback -id 1111113,17712920,1111111 -property_file property_file
-analyze
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.

OPatchauto version : 11.1.0.10.4
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime/work/midnew270/oms
Log file location  : /scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/May_02_
2014_01_05_58/rollback2014-05-02_01-05-58AM_1.log

OPatchauto log file:
 /scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/SystemPatch/opatch_oms_
2014-05-02_01-06-00AM_analyze.log

Configuration Validation: Success

Running rollback prerequisite checks for patch(es) "1111111" and Oracle Home
"/scratch/aime/work/midnew270/plugins/oracle.sysman.emas.oms.plugin_12.1.0.6.0"...
Please monitor OPatch log file:
 /scratch/aime/work/midnew270/plugins/oracle.sysman.emas.oms.plugin_
12.1.0.6.0/cfgtoollogs/opatch/1111111_May_02_2014_01_05_
59/RollbackPrereq2014-05-02_01-06-07AM_2.log
Sub-patch(es) "1111111" are successfully analyzed for Oracle Home
"/scratch/aime/work/midnew270/plugins/oracle.sysman.emas.oms.plugin_12.1.0.6.0"

Running rollback prerequisite checks for patch(es) "17712920" and Oracle Home
"/scratch/aime/work/midnew270/plugins/oracle.sysman.db.oms.plugin_12.1.0.6.0"...
Please monitor OPatch log file:
 /scratch/aime/work/midnew270/plugins/oracle.sysman.db.oms.plugin_
12.1.0.6.0/cfgtoollogs/opatch/17712920_May_02_2014_01_05_
59/RollbackPrereq2014-05-02_01-06-10AM_2.log
Sub-patch(es) "17712920" are successfully analyzed for Oracle Home
 "/scratch/aime/work/midnew270/plugins/oracle.sysman.db.oms.plugin_12.1.0.6.0"

Running rollback prerequisite checks for patch(es) "1111113" and Oracle Home
 "/scratch/aime/work/midnew270/oms"...
Please monitor OPatch log file:
 /scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/1111113_May_02_2014_01_05_
59/RollbackPrereq2014-05-02_01-06-12AM_2.log
Sub-patch(es) "1111113" are successfully analyzed for Oracle Home
 "/scratch/aime/work/midnew270/oms"

Complete Summary
================

All log file names referenced below can be accessed from the directory
 "/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/2014-05-02_01-05-58AM_
```

```
SystemPatch_2111111_1"

Prerequisites analysis summary:
-------------------------------

The following sub-patch(es) are rollbackable:

Oracle Home Name   Sub-patches                      Log file
----------------   -----------                        --------
  oracle_sysman_db11      17712920   17712920_RollbackPrereq2014-05-02_01-06-10AM_
2.log
  oracle_sysman_emas11       1111111    1111111_RollbackPrereq2014-05-02_
01-06-07AM_2.log
 oms12c1       1111113    1111113_RollbackPrereq2014-05-02_01-06-12AM_2.log

Log file location:
 /scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/SystemPatch/opatch_oms_
2014-05-02_01-06-00AM_analyze.log

OPatchauto succeeded.
```

Note

- Once the analysis finishes, you can refer to the OPatchauto log to see what steps would be executed by OPatchauto in non –analyze mode. The log file contains references to the HTML and text output file HTML containing detailed steps.
- If you are analyzing a standby OMS system, you must include the *-standby* option.

17.4 Using OPatchauto

OPatchauto must be run from the platform home of the OMS being patched. The ORACLE_HOME environment variable must be set as the platform home or provided using the OPatchauto "–oh" option. For example:

```
<Platform Home>/OPatch/opatchauto apply <patch>
```

Minimum Required OPatchauto Version: 11.1.0.10.4

Ensuring You Have the Latest Version of OPatch

OPatchauto uses the OPatch utility to apply the patch. For this reason, you must ensure that you have the latest version of OPatch 11.1 on all OMS instance platform homes. If you not sure which version of OPatch resides on your system, run the following command:

<Platform Home>/OPatch/opatchauto version

To download the latest version of OPatch, follow the instructions outlined in the My Oracle Support note 224346.1 available at the following location:

https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=224346.1

Patching Quickstart

Using OPatchauto typically involves the following phases:

1. Determining Whether Your System Meets OPatchauto System Requirements

Run `opatchauto apply -analyze`

The `apply -analyze` command simulates an OPatchauto apply session by running all prerequisite checks, when possible, without making changes to the system (either bits or configurations). This command does not apply the patch.

See "Prerequisites for Running OPatchauto" on page 17-6 for additional information.

2. Determining What System Patches Currently Exist on Your System

Run `opatchauto lspatches`

See "lspatches" on page 17-25   for more information.

3. Obtaining Patches from My Oracle Support (MOS)

OPatchauto requires that the required platform or plug-in System patches be obtained from My Oracle Support and downloaded to the OMS instance on which OPatchauto is to be run.

See "My Oracle Support: Searching for Patches" on page 17-10 for more information.

4. Applying a Patch

Run `$opatchauto apply` <patch>

The apply command applies all patches within a specified System patch to the platform home from which OPatchauto is command is run.

See "Running `opatchauto apply`" on page 17-14 for more information.

5. Deinstalling Individual Sub-patches of a System Patch

Run `$opatchauto rollback -id <list of comma separated sub-patches of System patch>`

Note: For a complete list of sub-patches of the System patch, refer to the patch README.

If, after applying the patch, the system is not stable, the most likely cause is the patch itself. Contact Oracle Support. They will recommend that you remove the patch using the `opatchauto rollback` command.

See "Running `opatchauto rollback`" on page 17-15 for more information.

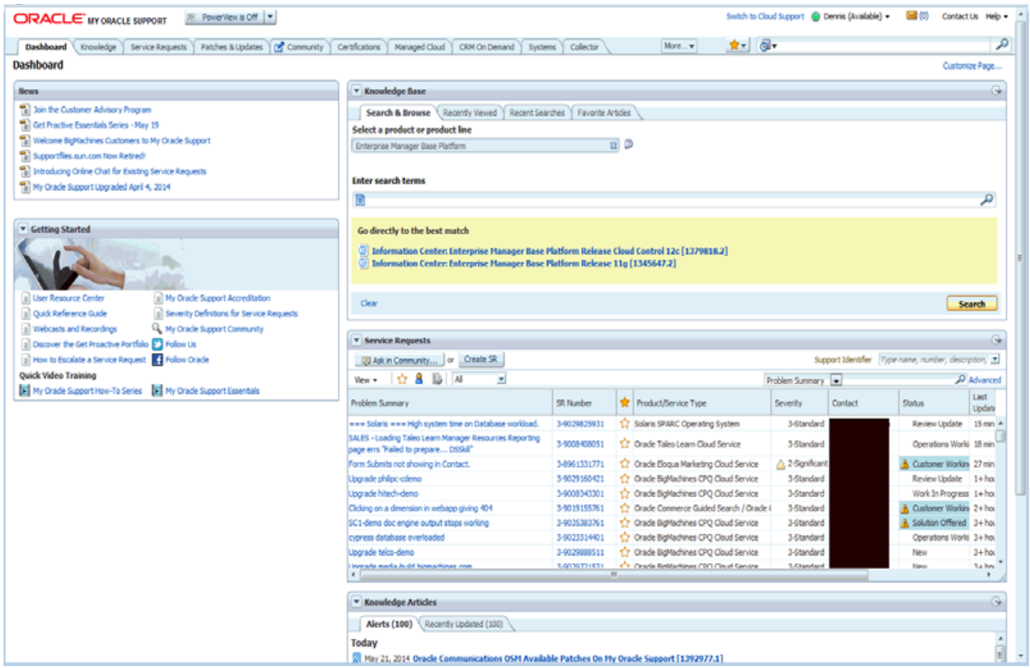
17.4.1 My Oracle Support: Searching for Patches

The first step in the patching process is to determine what patches you need from My Oracle Support (MOS). MOS is the single source of truth for patching. You can access MOS at the following location:

https://support.oracle.com

Once you have logged in, you have access to interactive support tools and information that simplify searching for and obtaining the requisite patches for your Oracle environment. The following figure shows the MOS home page.

Figure 17–2 My Oracle Support Main Page



ORACLE MY ORACLE SUPPORT PowerView is Off

Switch to Cloud Support Dennis (Available) (0) Contact Us Help

Dashboard

News

- Join the Customer Advisory Program
- Get Proactive Essentials Series - May 19
- Welcome BigMachines Customers to My Oracle Support
- Supportfiles.sun.com Now Retired!
- Introducing Online Chat for Existing Service Requests
- My Oracle Support Upgraded April 4, 2014

Getting Started

- User Resource Center
- Quick Reference Guide
- Webcasts and Recordings
- Discover the Get Proactive Portfolio
- How to Escalate a Service Request
- My Oracle Support Accreditation
- Severity Definitions for Service Requests
- My Oracle Support Community
- Follow Us
- Follow Oracle

Quick Video Training

- My Oracle Support How-To Series
- My Oracle Support Essentials

Knowledge Base

Select a product or product line: Enterprise Manager Base Platform

Enter search terms

Go directly to the best match

- Information Center: Enterprise Manager Base Platform Release Cloud Control 12c [1379818.2]
- Information Center: Enterprise Manager Base Platform Release 11g [1345647.2]

Service Requests

Problem Summary	SR Number	★	Product/Service Type	Severity	Contact	Status	Last Updat
=== Solaris === High system time on Database workload.	3-9029825931	☆	Solaris SPARC Operating System	3-Standard	[redacted]	Review Update	15 min
SALES - Loading Taleo Learn Manager Resources Reporting page errs "Failed to prepare... DSSkill"	3-9008408051	☆	Oracle Taleo Learn Cloud Service	3-Standard	[redacted]	Operations Worki	18 min
Form Submits not showing in Contact.	3-8961331771	☆	Oracle Eloqua Marketing Cloud Service	△ 2-Significant	[redacted]	Customer Workin	27 min
Upgrade philipc-cdemo	3-9029160421	☆	Oracle BigMachines CPQ Cloud Service	3-Standard	[redacted]	Review Update	1+ hou
Upgrade hitech-demo	3-9008343301	☆	Oracle BigMachines CPQ Cloud Service	3-Standard	[redacted]	Work In Progress	1+ hou
Clicking on a dimension in webapp giving 404	3-9019155761	☆	Oracle Commerce Guided Search / Oracle (	3-Standard	[redacted]	Customer Workin	2+ hou
SC1-demo doc engine output stops working	3-9035383761	☆	Oracle BigMachines CPQ Cloud Service	3-Standard	[redacted]	Solution Offered	3+ hou
cypress database overloaded	3-9023314401	☆	Oracle BigMachines CPQ Cloud Service	3-Standard	[redacted]	Operations Worki	3+ hou
Upgrade telco-demo	3-9029888511	☆	Oracle BigMachines CPQ Cloud Service	3-Standard	[redacted]	New	3+ hou
Upgrade media-build bigmachines.com	3-9029721531	☆	Oracle BigMachines CPQ Cloud Service	3-Standard	[redacted]	New	3+ hou

Knowledge Articles

Today

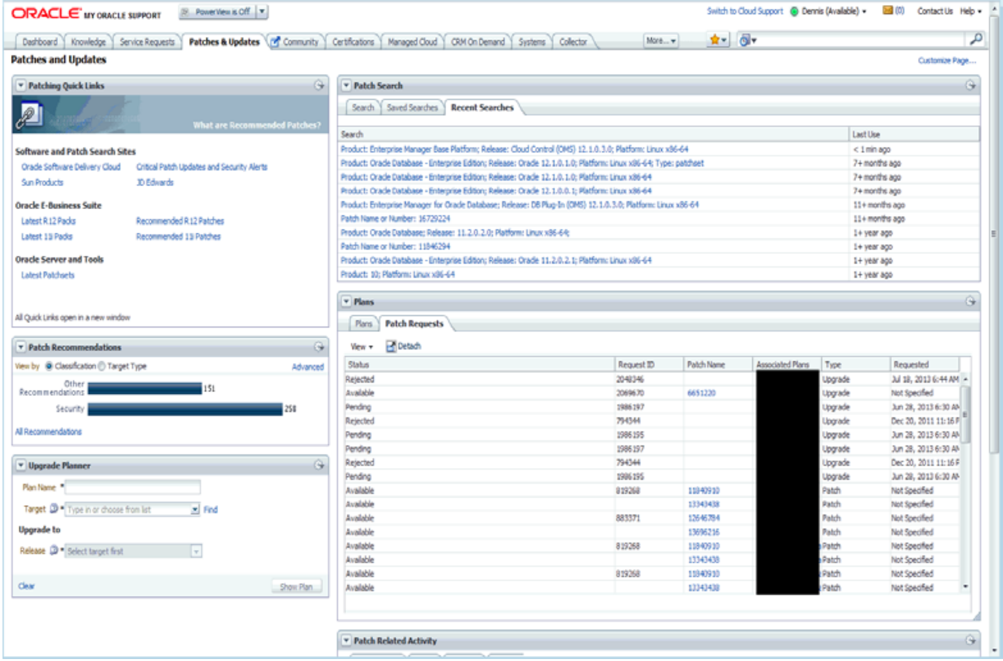
May 21, 2014 Oracle Communications OSM Available Patches On My Oracle Support [1392977.1]

Note: You can find complete documentation about MOS at the following location:

http://docs.oracle.com/cd/E25290_01/index.htm

My Oracle Support contains many features and capabilities that are grouped under tabs across the top of the application. Of primary interest is the *Patches and Updates* tab shown in the following figure.

Figure 17–3 MOS Patches and Updates



Patches and Updates

Patching Quick Links

Software and Patch Search Sites
Oracle Software Delivery Cloud
Critical Patch Updates and Security Alerts
Sun Products
JD Edwards

Oracle E-Business Suite
Latest R12 Packs
Recommended R12 Patches
Latest 11i Packs
Recommended 11i Patches

Oracle Server and Tools
Latest Patchsets

All Quick Links open in a new window

Patch Recommendations

View by ● Classification ○ Target Type Advanced

Other Recommendations 151
Security 258

All Recommendations

Upgrade Planner

Plan Name *
Target * Type in or choose from list Find
Upgrade to
Release * Select target first
Clear Show Plan

Patch Search

Search | Saved Searches | Recent Searches

Search	Last Use
Product: Enterprise Manager Base Platform; Release: Cloud Control (OMS) 12.1.0.3.0; Platform: Linux x86-64	< 1 min ago
Product: Oracle Database - Enterprise Edition; Release: Oracle 12.1.0.1.0; Platform: Linux x86-64; Type: patchset	7+ months ago
Product: Oracle Database - Enterprise Edition; Release: Oracle 12.1.0.1.0; Platform: Linux x86-64	7+ months ago
Product: Oracle Database - Enterprise Edition; Release: Oracle 12.1.0.0.1; Platform: Linux x86-64	7+ months ago
Product: Enterprise Manager for Oracle Database; Release: DB Plug-In (OMS) 12.1.0.3.0; Platform: Linux x86-64	11+ months ago
Patch Name or Number: 16729224	11+ months ago
Product: Oracle Database; Release: 11.2.0.2.0; Platform: Linux x86-64;	1+ year ago
Patch Name or Number: 11846294	1+ year ago
Product: Oracle Database - Enterprise Edition; Release: Oracle 11.2.0.2.1; Platform: Linux x86-64	1+ year ago
Product: 10; Platform: Linux x86-64	1+ year ago

Plans

Plans | Patch Requests

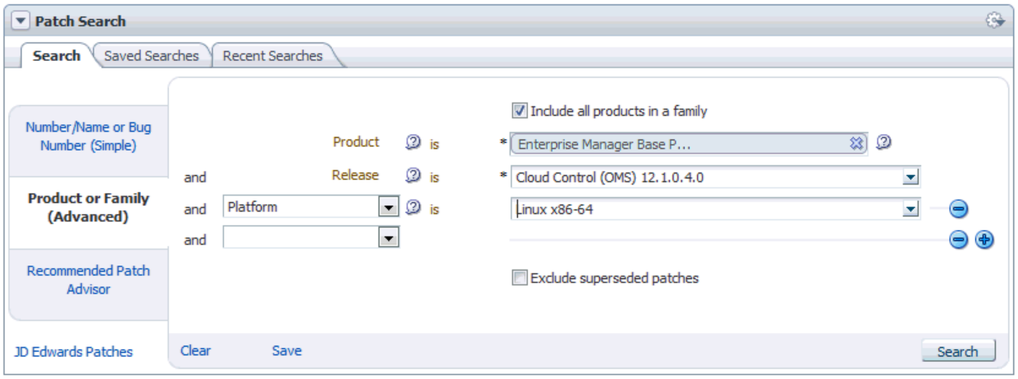
View ▾ Detach

Status	Request ID	Patch Name	Associated Plans	Type	Requested
Rejected	2048346		[redacted]	Upgrade	Jul 18, 2013 6:44 AM
Available	2069670	6651220	[redacted]	Upgrade	Not Specified
Pending	1986197		[redacted]	Upgrade	Jun 28, 2013 6:30 AM
Rejected	794344		[redacted]	Upgrade	Dec 20, 2011 11:16 F
Pending	1986195		[redacted]	Upgrade	Jun 28, 2013 6:30 AM
Pending	1986197		[redacted]	Upgrade	Jun 28, 2013 6:30 AM
Rejected	794344		[redacted]	Upgrade	Dec 20, 2011 11:16 F
Pending	1986195		[redacted]	Upgrade	Jun 28, 2013 6:30 AM
Available	819268	11840910	[redacted]	Patch	Not Specified
Available		13343438	[redacted]	Patch	Not Specified
Available	883371	12646784	[redacted]	Patch	Not Specified
Available		13696216	[redacted]	Patch	Not Specified
Available	819268	11840910	[redacted]	Patch	Not Specified
Available		13343438	[redacted]	Patch	Not Specified
Available	819268	11840910	[redacted]	Patch	Not Specified
Available		13343438	[redacted]	Patch	Not Specified

Click on the tab to access the *Patches and Updates* page. From here, you can search for the patches based on the OMS patch area (core, plug-in, or combination). The following examples illustrate OMS patch searches for the various patch areas.

From the Search tab, click **Product or Family (Advanced)**.

Figure 17–4 Searching by Product or Family


Patch Search
Search
Saved Searches
Recent Searches
Number/Name or Bug Number (Simple)
Product or Family (Advanced)
Recommended Patch Advisor
JD Edwards Patches
Clear
Save
Search

☑ Include all products in a family

Product is * Enterprise Manager Base P...

and Release is * Cloud Control (OMS) 12.1.0.4.0

and Platform is Linux x86-64

and

☐ Exclude superseded patches

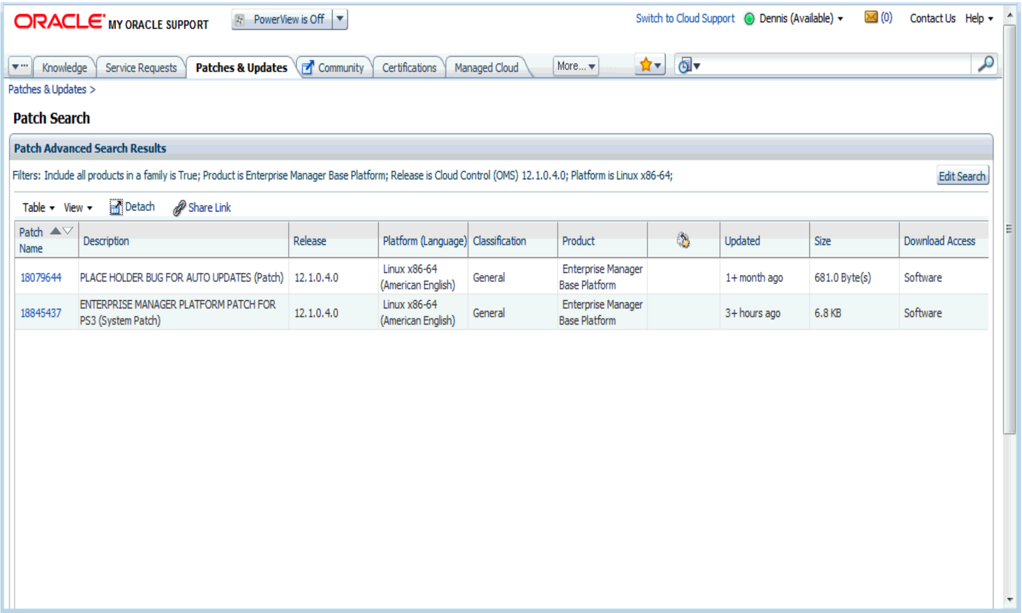
Example: Searching for a Platform Patch

To search for Enterprise Manager OMS core patches, enter the following search parameters:

- **Product**: Enterprise Manager Base Platform
- **Release**: Cloud Control (OMS) 12.1.0.4.0
- **Platform**: Linux x86-64

Clicking **Search** displays the following results.

Figure 17–5 OMS Core Patch Search Results



Patch Search

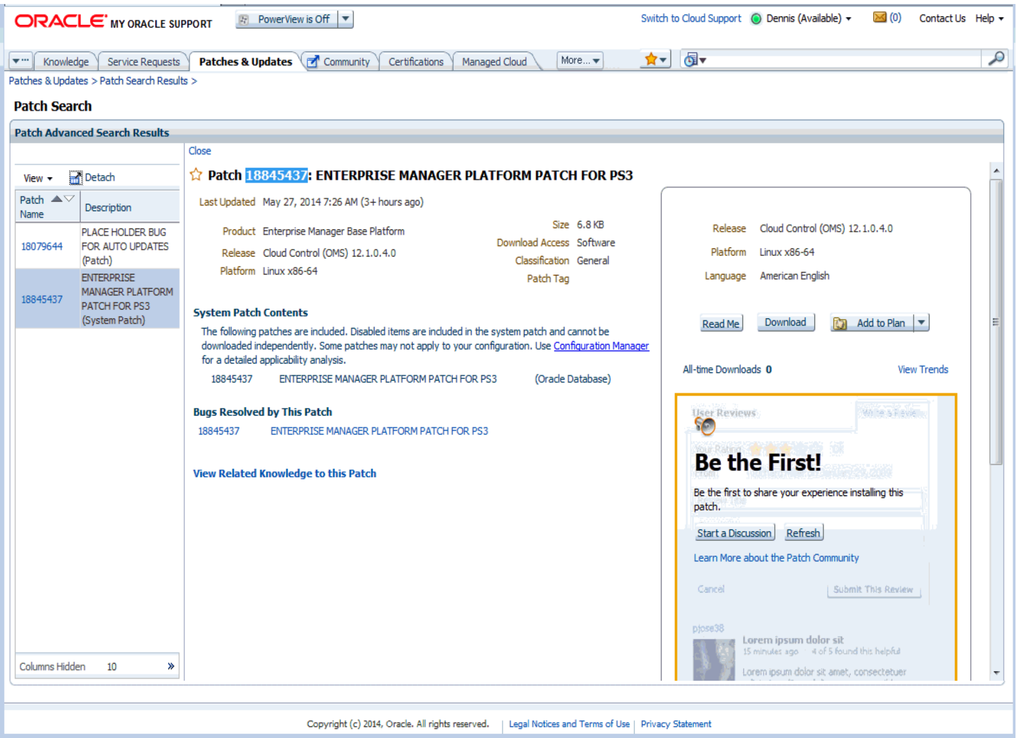
Patch Advanced Search Results

Filters: Include all products in a family is True; Product is Enterprise Manager Base Platform; Release is Cloud Control (OMS) 12.1.0.4.0; Platform is Linux x86-64;

Patch Name	Description	Release	Platform (Language)	Classification	Product		Updated	Size	Download Access
18079644	PLACE HOLDER BUG FOR AUTO UPDATES (Patch)	12.1.0.4.0	Linux x86-64 (American English)	General	Enterprise Manager Base Platform		1+ month ago	681.0 Byte(s)	Software
18845437	ENTERPRISE MANAGER PLATFORM PATCH FOR PS3 (System Patch)	12.1.0.4.0	Linux x86-64 (American English)	General	Enterprise Manager Base Platform		3+ hours ago	6.8 KB	Software

By clicking on patch 18845437 you are taken to the patch page where you can view bugs resolved by this patch, related Knowledge Articles, or view a generic patch README.

Figure 17–6 OMS Core Patch Page



Patch Search

Patch Advanced Search Results

Patch Name	Description
18079644	PLACE HOLDER BUG FOR AUTO UPDATES (Patch)
18845437	ENTERPRISE MANAGER PLATFORM PATCH FOR PS3 (System Patch)

Patch 18845437: ENTERPRISE MANAGER PLATFORM PATCH FOR PS3

Last Updated May 27, 2014 7:26 AM (3+ hours ago)

Product Enterprise Manager Base Platform
Release Cloud Control (OMS) 12.1.0.4.0
Platform Linux x86-64

Size 6.8 KB
Download Access Software
Classification General
Patch Tag

Release Cloud Control (OMS) 12.1.0.4.0
Platform Linux x86-64
Language American English

All-time Downloads 0

System Patch Contents

The following patches are included. Disabled items are included in the system patch and cannot be downloaded independently. Some patches may not apply to your configuration. Use Configuration Manager for a detailed applicability analysis.

18845437 ENTERPRISE MANAGER PLATFORM PATCH FOR PS3 (Oracle Database)

Bugs Resolved by This Patch

18845437 ENTERPRISE MANAGER PLATFORM PATCH FOR PS3

View Related Knowledge to this Patch

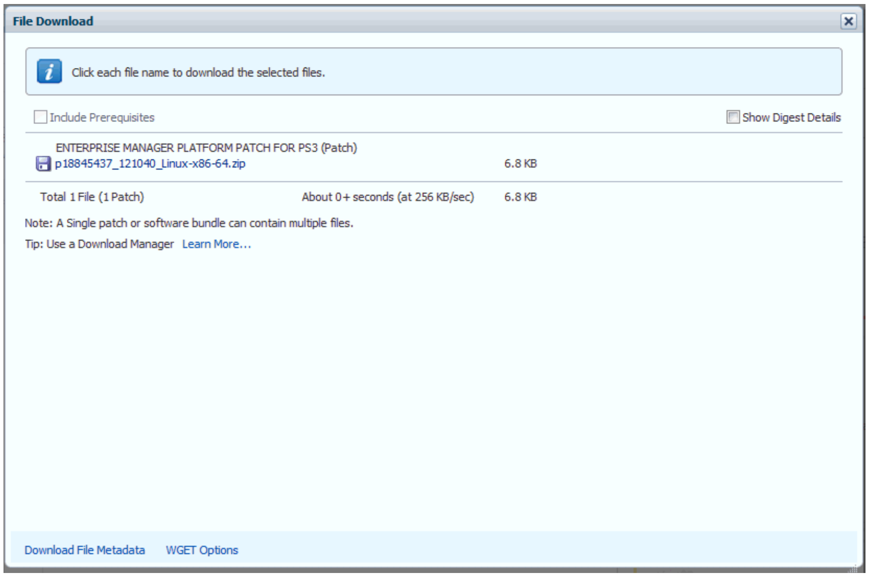
Be the First!

Be the first to share your experience installing this patch.

Copyright (c) 2014, Oracle. All rights reserved. | Legal Notices and Terms of Use | Privacy Statement

Click **Download** to save the patch .ZIP file to your local system.

Figure 17–7 Patch Download Dialog



File Download

Click each file name to download the selected files.

□ Include Prerequisites □ Show Digest Details

ENTERPRISE MANAGER PLATFORM PATCH FOR PS3 (Patch)
p18845437_121040_Linux-x86-64.zip 6.8 KB

Total 1 File (1 Patch) About 0+ seconds (at 256 KB/sec) 6.8 KB

Note: A Single patch or software bundle can contain multiple files.

Tip: Use a Download Manager Learn More...

17.4.2 Running `opatchauto apply`

Once you have downloaded the patch, see the patch README for explicit patch details and instructions on applying the patch. You can find the README at the following location

```
<System patch location>/README.txt (or) README.html
```

As you step through the patching operations in the README, running `opatchauto apply` (depending on the configuration that is patched, primary or standby) will generate a custom, environment-specific version of the README for patching operations for the primary site multi-OMS or standby site OMS systems. For a primary site single OMS system, running `opatchauto apply` will perform patching and deployment operations.

On your local OMS instance, run the following command from the top level System patch directory:

```
$<Platform home>/OPatch/opatchauto apply <patch>
```

Note: Unlike `opatchauto analyze`, you should not run `opatchauto apply` on every OMS instance. OPatchauto will either execute all patching and deployment operations, or will generate environment-specific steps that include complete configuration aspects of the System.

For a multi-OMS UNIX system, OPatchauto generates bash scripts for execution, one per OMS instance; follow the instructions given by opatchauto to find those scripts. (Requires OPatch 11.1.0.10.2 or later.) For Windows multi-OMS systems, OPatchauto will generate customized patching instructions/commands for the environment in text and HTML formats; administrators must execute these instructions to patch the various OMSs.

17.4.3 Running `opatchauto rollback`

See the patch README for explicit patch details and instructions on deinstalling the patch. You can find the README at the following location

```
<System patch location>/README.txt (or) README.html
```

As you step through the patch deinstallation operations in the README, running `opatchauto rollback` (depending on the configuration that is patched, primary or standby) will generate a custom, environment-specific version of the README for patching operations for the primary site multi-OMS or standby site OMS systems. For a primary site single OMS system, running `opatchauto rollback` will perform the deinstallation operations.

On your local OMS instance, run the following command from the top level System patch directory:

```
$<Platform home>/OPatch/opatchauto rollback -id <list of comma separated
sub-patches of System patch>
```

Note:

- Unlike `opatchauto analyze`, you should not execute the opatchauto rollback command on every OMS instance. OPatchauto will either execute all patching and deployment operations, or will generate environment-specific steps that include complete configuration aspects of the System.
- The list of sub-patches within the System patch can be retrieved from patch README.

  The list of sub-patches listed in System patch README may differ from the patches that are actually installed. During System patch installation, some sub-patches may be skipped (not installed).

For a multi-OMS UNIX system, Opatchauto generates bash scripts for execution, one per OMS instance; follow the instructions given by opatchauto to find those scripts. (Requires OPatch 11.1.0.10.2 or later) For Windows multi-OMS systems, OPatchauto will generate customized patching instructions/commands for the environment in text and HTML formats; administrators must execute these instructions to patch the various OMSs.

17.4.4 Running `opatchauto lspatches`

After the patch is applied or rolled back, you can run the `opatchauto lspatches` command to generate a comprehensive Oracle home – patches map of the OMS instance homes and installed patches.

Example 17–3 Sample `opatchauto lspatches` ***Output***

```
$opatchauto lspatches
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.

Oracle Home:/scratch/aime/work/midnew270/oms
1111113
1111111
1111115
```

```
Oracle Home:/scratch/aime/work/midnew270/plugins/oracle.sysman.db.oms.plugin_
12.1.0.6.0
17712920;EM DB PLUGIN BUNDLE PATCH 12.1.0.4.4

Oracle Home:/scratch/aime/work/midnew270/plugins/oracle.sysman.emas.oms.plugin_
12.1.0.6.0
1111111

The following groups of patch(es) are applied as System Patch bundle(s):
1111111
1111115
1111113,17712920,1111111

For more details on installed patch(es) in platform, plugin homes, Please do
'$ORACLE_HOME/OPatch/opatch lsinventory -details -oh <desired home path>'
```

17.4.5 Running `opatchauto version`

To determine the version numbers of the various OPatchauto utilities (Opatch, OPlan, OsysModel) that reside on your system, you can run `opatchauto version`.

Example 17–4 `opatchauto version` ***Output***

```
OPatchauto Version: 11.1.0.4.0
OPlan Version: 12.1.0.2.0
OsysModel build: Fri May 23 19:23:33 PDT 2014
```

17.4.6 Patching a Standby OMS System

If you have configured a standby OMS for High Availability, refer to the chapter on "Enterprise Manager Disaster Recovery" and the appendix on Standby OMSs Using Standby WebLogic Domain" both of which can be found in the Enterprise Manager Advanced Installation and Configuration Guide.

OPatchauto Command Syntax

This section provides a comprehensive listing and description of all OPatchauto commands used to patch an OMS.

> **Important:** OPatchauto commands must be run from the OMS Platform home.

OPatchauto Commands

The OPatchauto commands are run from the OMS Platform home out of the standard OPatch directory. The Platform home must be set as $ORACLE_HOME. In the following generic example, an OPatchauto command is run from a Platform home

```
<Platform home>/OPatch/opatchauto apply <PATH_TO_PATCH_
DIRECTORY>
```

where <PATH_TO_PATCH_DIRECTORY> is the full path to the System patch top level directory.

OPatchauto consists of four primary commands.

- apply
- rollback
- checkapplicable
- saveConfigurationSnapshot
- lspatches
- version

OPatchauto help

You can view online help for any command (except *version*) by specifying the -help option.

```
<Platform home>/OPatch/opatchauto -help
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.


 Usage: opatchauto [ -help ] [ -analyze ] [ command ]

            command := apply
                       rollback
                       checkApplicable
                       query
                       lspatches
                       version
                       saveConfigurationSnapshot

 <global_arguments> := -help       Displays the help message for the command.
                       -analyze    Print the actions, steps to be performed
without any execution.

 example:
   'opatchauto -help'
```

```
'opatchauto apply -help'
'opatchauto rollback -help'
'opatchauto checkApplicable -help'
'opatchauto query -help'
'opatchauto lspatches -help'
'opatchauto saveConfigurationSnapshot -help'
```

Apply

Apply a System patch to OMS instance homes. You must specify the patch location or the current directory will be used as the patch location.

> **Important:** OPatchauto must be run from the platform home. ORACLE_HOME environment variable must be set as the platform home or provided using the –oh option.

You must run the *Apply* command directly from the System patch location.

When running `opatchauto apply`, you will be prompted the following:

- WebLogic Admin Server URL of the primary OMS (or standby OMS)
- Username and Password

Silent interaction is supported by using the *silent* and *property_file* options.

The *standby* option should be used if a stand by OMS system is patched.

OPatchauto can pass 'x=y' properties through the command line. See "Apply Command Properties" on page 17-20.

Syntax

```
<Platform home>/OPatch/opatchauto apply <System patch location>
                  [-jre <Path to JRE>]
                  [-nonrolling]
                  [-invPtrLoc <Path to oraInst.loc>]
                  [-property_file <Path to property file>]
                  [-analyze]
                  [-silent]
                  [-oh <Platform home path>]
                  [-standby]
```

Parameters

<System patch location>

Path to the location of the patch. If the patch location is not specified, then the current directory is taken as the patch location. The patch can only be a System patch.

Apply Command Options

Table 17–1 Apply

Option	Description
jre	This option tells opatchauto to use JRE (java) from the specified location instead of the default location under Oracle Home.
nonrolling	Apply and deploy the patch in non-rolling fashion, provided it is supported by the patch.
invPtrLoc	Used to locate the oraInst.loc file. Needed when the installation used the -invPtrLoc flag. This should be the path to the oraInst.loc file.

Table 17–1 (Cont.) Apply

Option	Description
property_file	The administrator defined property file for OPatchauto to use. The path to the property file should be absolute. The keys for OPatchauto are: 'AdminConfigFile' - Encrypted file for Administration Server administrator of the OMS instance domain. 'AdminKeyFile' - Encrypted file for Administration Server password of the OMS instance domain. 'AdminServerURL' - Administration Server URL of OMS instance domain. (Example: t3s://<host address>:<port number>) The Key, value pair is of the format 'x=y' where 'x' is opatchauto understood key and each pair is separated by newline in the property file. This option is typically used for silent operations. This option is very useful for silent mode of 'opatchauto' invocation. In order to create encrypted files for a WebLogic Admin Server username & password, run $ORACLE_HOME/OPatch/wlskeys/createKeys.sh (.cmd for Windows) to get the files and load it thorough a custom file via the 'property_file' option. NOTE: For Windows, ensure that directories, files in the path are separated by "\\" in the property file.
analyze	Prints out the actions without any configuration/binary change through 'opatchauto'. This option performs prerequisite checks that includes both configuration and binary prerequisite checks. It simulates an apply operation (does not apply the patch). The command 'opatchauto apply' with this option must be run on each OMS instance to make sure all prerequisites pass for patching operations.
silent	Suppresses any user interaction.
oh	The parameter passed through this option will override ORACLE_HOME environment variable. This parameter (if this option is used) must be the core platform home.
standby	This option should be used when patching a standby OMS infrastructure.

Apply Command Properties

Table 17–2 Apply Properties

Option	Description
OPatchAuto.OMS_DISABLE_HOST_CHECK=true	Used to disable host verification check for WebLogic Admin Server. Set this property to true if your OMS configuration is based on virtual host.

Table 17–2 (Cont.) Apply Properties

Option	Description
OPatchAuto.OMS_USER=<installed OMS user>	Used when OPatchauto is not able to obtain the installed OMS administrator name. This switch is applicable only for Microsoft Windows environments.
OPatchAuto.OMS_SCRIPTS_DIR=<existing directory>	Used to specify a single, existing directory where bash scripts (generated by OPatchauto for multi-OMS configurations) are copied. By providing an existing directory, the bash scripts are copied to a newly created, timestamped sub-directory under the directory specified by this property. This allows an OMS administrator to execute the scripts from pre-determined, shared location rather than manually copying scripts to individual OMS machines. This switch is applicable only for UNIX systems.

Rollback

Roll back sub-patches of a System patch from OMS instance home. Administrator specifies the sub-patch IDs of the System patch. You can obtain the sub-patch IDs by running the `opatchauto lspatches` command. See "Running `opatchauto lspatches`" on page 17-15.

Important: OPatchauto must be run from the platform home. ORACLE_HOME environment variable must be set as platform home or provided via the `-oh` option.

When running *opatchauto rollback*, you will be prompted the following:

- WebLogic Admin Server URL of the primary OMS (or standby OMS)
- Username and Password

Silent interaction is supported by using the *silent* and *property_file* options.

The *standby* option should be used if a stand by OMS system is patched.

OPatchauto can pass 'x=y' properties through the command line. See "Rollback Command Properties" on page 17-23.

Syntax

```
opatchauto rollback -id <sub patches ID of System patch>
                    [-idFile <file contains list of sub-patch IDs
                      of System patch> ]
                    [-invPtrLoc <Path to oraInst.loc>]
                    [-jre <LOC>]
                    [-silent]
                    [-nonrolling]
                    [-property_file <path to property file>]
                    [-analyze]
                    [-oh <Platform home path>]
                    [-standby ]
```

Parameters

Sub-patch IDs for the System patch to be rolled back. If you want to roll back an entire System patch, the patch IDs for all sub-patches of the System patch (to be rolled back) must be specified.

Rollback Options

Table 17–3 Rollback

Option	Description
id	List of sub-patches of a System patch. For a complete list of sub-patches, see the System patch README. Use 'opatchauto lspatches' option to display all patch ids for both core home and plug-in homes with relation to the System patch bundles. The patch ids can be only from one bundle in a session. The list is separated by commas.
idfile	File that contains the list of sub-patch IDs of a System patch.
invPtrLoc	The `invPtrLoc` option is used to locate the Central Inventory Pointer File (`oraInst.loc)`. Input for this option is the path to the `oraInst.loc` file.

Table 17–3 (Cont.) Rollback

Option	Description
jre	This jre option instructs OPatchauto to use the JRE (java) from the specified location instead of the default location under Oracle Home.
silent	This option refers to silent mode of invocation.
nonrolling	The `nonrolling` option instructs OPatchauto to run the patching session run in 'nonrolling' mode. Before the patching session can start, the following prerequisites must be met: ■ The stack on the local node must be running ■ All remote nodes must be down.
property_file	The administrator defined property file for opatchauto to use. The path to the property file should be absolute. The keys for 'opatchauto' are: 'AdminConfigFile' - Encrypted file for Administration Server administrator of OMS instance domain. 'AdminKeyFile' - Encrypted file for Administration Server password of OMS instance domain. 'AdminServerURL' - Administration Server URL of OMS instance domain. (Example: t3s://<host address>:<port number>) The Key, value pair is of the format 'x=y' where 'x' is opatchauto/opatch understood key and each pair is separated by newline in the property file. In order to create encrypted files for Oracle WebLogic Administration Server username & password, Use $ORACLE_HOME/OPatch/wlskeys/createkeys.sh (.cmd for Windows) to get the files and load it thorough a custom file by 'property_file' option. NOTE: For Windows, ensure that directories, files in the path are separated by "\\" in the property file.
analyze	This option helps us to do dry-run prerequisite checks that includes both configuration and binary prerequisite checks. The command 'opatchauto rollback' with this option must be run on each OMS instance to make sure all prerequisites pass for patching operations.
oh	The parameter passed through this option will override ORACLE_HOME environment variable. This parameter (if this option is used) must be the core platform home.
standby	This option should be used when patching a standby OMS infrastructure.

Rollback Command Properties

Table 17–4 Rollback Properties

Option	Description
OPatchAuto.OMS_DISABLE_HOST_CHECK=true	Used to disable host verification check for WebLogic Admin Server. Set this property to true if your OMS configuration is based on virtual host.

Table 17–4 (Cont.) Rollback Properties

Option	Description
OPatchAuto.OMS_USER=<installed OMS user>	Used when OPatchauto is not able to obtain the installed OMS administrator name. This switch is applicable only for Microsoft Windows environments.
OPatchAuto.OMS_SCRIPTS_DIR=<existing directory>	Used to specify a single, existing directory where bash scripts (generated by OPatchauto for multi-OMS configurations) are copied. By providing an existing directory, the bash scripts are copied to a newly created, timestamped sub-directory under the directory specified by this property. This allows an OMS administrator to execute the scripts from pre-determined, shared location rather than manually copying scripts to individual OMS machines. This switch is applicable only for UNIX systems.

lspatches

Display patches and their Oracle home relationships with reference to OMS platform and plug-in homes. Set ORACLE_HOME as the platform home or override the it using *-oh* option. This command also displays sub-patches of the System patch bundles. Each System patch bundle is separated by a new line.

Syntax

```
opatchauto lspatches   [ -invPtrLoc <Path to oraInst.loc> ]
                       [-jre <LOC> ]
                       [-oh <Platform Oracle home> ]
```

Options

Table 17–5 lspatches

Option	Description
jre	This `jre` option instructs OPatchauto to use the JRE (java) from the specified location instead of the default location under Oracle Home.
invPtrLoc	The `invPtrLoc` option is used to locate the Central Inventory Pointer File (`oraInst.loc.` Input for this option is the path to the `oraInst.loc` file.
oh	The location of Enterprise Manager platform home. This overrides the ORACLE_HOME environment variable.

version

The version command shows the current version number of the OPatch utility, dependent OPlan version, and the osysmodel version.

Important: OPatchauto must be run from the platform home.

Syntax

```
<GI_HOME>/OPatch/opatchauto version [-invPtrLoc <Path to oraInst.loc>]
               [-jre <LOC>]
               [-oh <ORACLE_HOME>]
               [-help] [-h]
```

Options

The following table describes the options available for the version command.

Table 17–6 version ***Command Options***

Option	Description
-invPtrLoc	The invPtrLoc option is used to locate the Central Inventory Pointer File (oraInst.loc). Input for this option is the path to the oraInst.loc file.
-jre	This jre option instructs OPatchauto to use the JRE (java) from the specified location instead of the default location under Oracle Home.
-oh	The oh option specifies the Oracle Home to work on. This takes precedence over the environment variable ORACLE_HOME.

checkApplicable

The `checkApplicable` command performs prerequisite binary checks on the OMS platform home and plug-in homes to determine the applicability of a System patch and/or the whether sub-patches of the System patch can be rolled back.

Syntax

```
opatchauto checkApplicable
     [-id <singleton or System Patch ID to be rolled back>]
     [-invPtrLoc <Path to oraInst.loc>]
     [-jre <LOC>]
     [-ph <System patch that is to be installed>]
     [-silent]
```

Options

The following table describes the options available for the `checkApplicable` command.

Table 17–7 `checkApplicable` ***Command Options***

Option	Description
id	Used to specify the sub-patch IDs that are to be rolled back from the OMS platform home or plug-in homes.
invPtrLoc	Used to locate the oraInst.loc file. Needed when the installation used the -invPtrLoc flag. This should be the path to the oraInst.loc file.
jre	Instructs OPatch to use the JRE (java) from the specified location instead of the default location under Oracle Home.
ph	Used to specify the path to the patch location. The input must be a System patch location.
silent	Suppresses any user interaction

saveConfigurationSnapshot

The `saveConfigurationSnapshot` command generates configuration a snapshot for the primary OMS (along with OMS repository and standby OMS) and saves it to an XML file that can be read by OPatch.

If file is not specified, it will be saved to a default file (configData.xml) at the following location

`ORACLE_HOME/cfgtoollogs/opatch/sysconfig/configData.xml`

When running the `saveConfigurationSnapshot` command, you will be prompted for the following:

- WebLogic Admin Server URL of the primary OMS
- Username and password

You can run the command in silent mode (suppress user interaction) via the *silent* and *property_file* options.

This command must be run from an OMS instance belonging to the primary OMS system. If the OMS configuration is running on a virtual host, you must set the `OPatchAuto.OMS_DISABLE_HOST_CHECK=true` option from the command line.

Syntax

```
opatchauto saveConfigurationSnapshot
     [-configFile <File to save configuration snapshot> ]
     [-oh <ORACLE_HOME> ]
     [-invPtrLoc <Path to oraInst.loc> ]
     [-jre <LOC> ]
     [-silent ]
     [-property_file <path to file> ]
```

Options

The following table describes the options available for the `version` command.

Table 17–8 `saveConfigurationSnapshot` ***Command Options***

Option	Description
configFile	Enables OPatch to write the configuration for the specified product to an XML file. The XML file can only be recognized by Oracle System Model APIs and accessed through via the Enterprise Manager SDK.
oh	Specifies the Oracle home to be worked on. The Oracle Home specified takes precedence over the environment variable ORACLE_HOME.
invPtrLoc	Used to locate the oraInst.loc file. Needed when the installation used the -invPtrLoc flag. This should be the path to the oraInst.loc file.
jre	Instructs OPatch to use JRE (java) from the specified location instead of the default location under Oracle Home.
silent	Suppresses any user-interaction.

Table 17–8 (Cont.) `saveConfigurationSnapshot` ***Command Options***

Option	Description
property_file	The user-defined property file for OPatchauto to use. The path to the property file must be absolute. The keys for 'opatchauto' are: ■ AdminConfigFile - Encrypted file for Admin Server user of the GC Domain. ■ AdminServerURL' - Admin Server URL of GC Domain (Example: t3s://<host address>:<port number>) ■ AdminKeyFile - Encrypted file for Admin Server password of the GC Domain. The Key, value pair is of the format 'x=y' where 'x' is an OPatchauto understood key and each pair is separated by newline in the property file. The `property_file` option is typically used when running OPatchauto in silent mode operation (suppress user interaction) In order to create encrypted files for a WebLogic Admin Server username & password, run the following script: `$ORACLE_HOME/OPatch/wlskeys/createKeys.sh` (createKeys.cmd for Windows) to obtain the files and load them through a custom file using the *property_file* option. NOTE: For Windows, maker sure that directories, files in the path are separated by "\\" in the property file.

Standby OMS Patching

There are two methods used to implement a standby OMS:

1. Standby OMS - Replicating OMS, Software library and Repository Components

If a standby site is set up through file system replication (Enterprise Manager 12.1.0.3 and later), there is no need to patch the standby site to keep it in sync with the primary site. When you apply patches to the primary OMS, the changes are automatically replicated at the standby site either manually or via automatic storage replication. For more details on this approach, see the chapter on "Enterprise Manager Disaster Recovery" in the Enterprise Manager Advance Installation and Configuration Guide..

Using the data and storage replication, the standby site does not need to be patched.

2. Standby OMS Configured in Parallel with the Primary OMS System

When patches are applied on the primary site OMS, they must also be applied on the standby site Management Services. Note that patches typically update the Oracle Homes (via the OPatch `apply` command) and may require scripts to be run against the Management Repository. On the standby site, it is sufficient to update the Oracle Homes (using OPatchauto) and skip the running of scripts on the Management Repository because database changes are automatically propagated to the standby site using Data Guard.

To patch the standby site, run `opatchauto apply` and `opatchauto rollback` with the standby option.

Troubleshooting

This chapter describes common OPatchauto problems that may occur during patching operations or the analyze phase.

This chapter covers the following:

- OPatchauto Troubleshooting Architecture
- OPatchauto Log Management Architecture
- Logs for Oracle Support
- OPatchauto: Cases Analysis, Error Codes, and Remedies/Suggestions
- OPatchauto: External Utilities Error Codes
- Special Error Cases for OPatchauto OMS Automation

OPatchauto Troubleshooting Architecture

In order for OPatchauto to fully automate the patching process, it accesses various tools/utilities to carry out different patching tasks in their respective phases. The primary tools/utilities outside of OPatch and OPatchauto are:

- `emctl stop oms` - Life cycle
- `emctl start oms` - Life cycle
- `emctl applypatch`, `emctl rollbackpatch` – Apply, rollback SQL changes in the OMS repository SYSMAN schema respectively
- `emctl register`, `emctl deregister` – Register, de-register metadata services with the right XMLs for MRS artifacts as per patch metadata instructions respectively

These tools/utilities are accessed during the patching process. Note that failure during invocation of these utilities can also happen and the errors & remedies for those commands are not handled in this document. They need to be followed up with Oracle Support for details. However, OPatchauto will trap errors from these commands output, push it to appropriate logs and announce it to the administrator and finally to support.

Apart from the above external tools/utilities, OPatchauto uses the following internal utilities to do binary patching operations. They have separated log files generated by OPatchauto. The internal utilities are patch binary prerequisite checks and patch binary apply, rollback operations.

OPatchauto Log Management Architecture

This section refers to the information through logs published by OPatchauto as part of its patching operations. This knowledge is needed for the administrator to obtain the appropriate logs from right area to troubleshoot and inform Oracle Support for further analysis. The following annotated example shows opatchauto apply output that displays the various log files that are created when running OPatchauto.

Sample OPatchauto Apply Output

```
$ OPatch/opatchauto apply /scratch/patches/targetPatchingImplRegistration/1111118
-silent -property_file property_file
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.

OPatchauto version : 11.1.0.10.4
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime/work/midnew270/oms
Log file location  :
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-15_03-24-24AM_
1.log

OPatchauto log file:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-15_03-24-25AM_deploy.log

Configuration Validation: Success

Running apply prerequisite checks for sub-patch(es) "1111118" and Oracle Home
"/scratch/aime/work/midnew270/oms"...
Please monitor OPatch log file:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/1111118_May_15_2014_03_24_
24/ApplyPrereq2014-05-15_03-24-41AM_2.log
Sub-patch(es) "1111118" are successfully analyzed for Oracle Home
"/scratch/aime/work/midnew270/oms"

To continue, OPatchauto will do the following:
[Patch and deploy artifacts]   : Apply sub-patch(es) [ 1111118 ] to Oracle Home
"/scratch/aime/work/midnew270/oms";
                                 Register MRS artifact
"TargetPatchingImplRegistration"

Do you want to proceed? [y|n]
Y (auto-answered by -silent)
User Responded with: Y

Applying sub-patch "1111118" to Oracle Home "/scratch/aime/work/midnew270/oms"...
Please monitor OPatch log file:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/1111118_May_15_2014_03_24_
24/apply2014-05-15_03-24-48AM_4.log

Registering service "TargetPatchingImplRegistration" with register file
"/scratch/aime/work/midnew270/oms/sysman/metadata/targetpatchingregister/RegisterA
gentTarget.xml"...

Complete Summary
================

All log file names referenced below can be accessed from the directory
```

```
"/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/2014-05-15_03-24-24AM_
SystemPatch_1111118_1"

Patching summary:
-----------------

Binaries of the following sub-patch(es) have been applied successfully:

Oracle Home Name   Sub-patches                                   Log file
----------------   -----------                                   --------
       oms12c1       1111118   1111118_apply2014-05-15_03-24-48AM_4.log

Deployment summary:
-------------------

The following artifact(s) have been successfully deployed:

Artifacts            Log file
---------             --------
MRS-TargetPatchingImplRegistration   emctl_register_
TargetPatchingImplRegistration_2014-05-15_03-24-58AM.log


Log file location:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-15_03-24-25AM_deploy.log

OPatchauto succeeded.
```

Log output to a consolidated directory

As shown in the example above, there is a reference to pushing of all logs to consolidated log directory. The following line in the trace example shows this consolidation log directory.

```
...

All log file names referenced below can be accessed from the directory
"/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/2014-05-15_03-24-24AM_
SystemPatch_1111118_1"

...
```

This consolidated log directory would contain the following files (here with reference to the example for *apply*).

```
$ ls -l /scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/2014-05-15_03-24-24AM_
SystemPatch_1111118_1
total 64
-rw-rw-r-- 1 aime svrtech  5335 May 15 03:25 1111118_ApplyPrereq2014-05-15_
03-24-41AM_2.log
-rw-rw-r-- 1 aime svrtech 19665 May 15 03:25 1111118_apply2014-05-15_03-24-48AM_
4.log
-rw-rw-r-- 1 aime svrtech   120 May 15 03:24 AdminServerStatusPrerequisites_
2014-05-15_03-24-40AM.log
-rw-rw-r-- 1 aime svrtech    66 May 15 03:24 RepositoryStatusPrerequisites_
2014-05-15_03-24-41AM.log
-rw-rw-r-- 1 aime svrtech    71 May 15 03:24 Swlib_Prerequisite_2014-05-15_
03-24-41AM.log
```

```
-rw-rw-r-- 1 aime svrtech   497 May 15 03:25 emctl_register_
TargetPatchingImplRegistration_2014-05-15_03-24-58AM.log
-rw-rw-r-- 1 aime svrtech  9588 May 15 03:25 opatch2014-05-15_03-24-24AM_1.log
-rw-rw-r-- 1 aime svrtech  2708 May 15 03:25 temp_apply_automation.xml
-rw-rw-r-- 1 aime svrtech  2124 May 15 03:25 temp_rollback_automation.xml
$
```

All the individual log files of each invocation, commands are finally copied to a consolidated place as highlighted above. Each command naming convention is self-explanatory and it indicates the actual operations being performed in automation. The 'opatchauto' log file will refer the individual log files so that administrator can easily connect to individual files to refer to any failure.

Logs for Oracle Support

If the administrator wants to contact Oracle Support, the administrator must provide the following references to Support.

- Administrator interface trace(s).
- Consolidated log directory as zip
- OPatch log file
- OPatchauto log file
- Output of **opatchauto lspatches** command on all OMS instance homes.

OPatchauto: Cases Analysis, Error Codes, and Remedies/Suggestions

Refer to the following table for common OPatchauto error codes.

Table 17–9 OPatchauto Error Codes

Error Code	Description	Remedy/Suggestion
231	Wrong Oracle WebLogic Administration Server URL and/or invalid credentials	Correct the interview inputs and run OPatchauto again.
234	Malformed Oracle WebLogic Administration Server URL	If the Oracle WebLogic Administration Server URL is already defaulted (value given), type <enter>. If it is not given, construct the Oracle WebLogic Administration Server URL as t3s://<WebLogic Administration Server host address>:<WebLogic Administration Server port> .of the domain that controls the managed server on which the OMS is deployed.
235	Unable to connect to OMS repository	Check the OMS repository connectivity for SYSMAN administrator and run OPatchauto again.
236	OUI central inventory read issue	Check if the OUI inventory is locked by some other processes. Check if OUI inventory is readable.
238	Patch binary prerequisite checks failure	Check OPatchauto, OPatch, patch binary prerequisite log files for more details on the errors. If not resolved, contact Oracle Support.

Table 17–9 (Cont.) OPatchauto Error Codes

Error Code	Description	Remedy/Suggestion
240 - 251	Binary updates (or) deployment failure	■ This is a case for single OMS system. Patching steps are decided by OPatchauto but it failed to execute steps. OPatchauto will print the failed executed step and the remaining steps to be executed for completion of patching operations. Administrator need to contact Oracle support with logs, resolve why it failed and then must execute manually the failed step and steps referred by OPatchauto (in OPatchauto log file) to complete operations. ■ In case of multi OMS (or) stand by OMS patching operations, failure of individual commands that got executed through text/html output must be brought to support notice for further diagnosis. After the failure condition is resolved, administrator need to execute the failed steps and further steps mentioned in HTML (or) text output to complete the patching operations.
233	Software library not configured OMS repository connectivity not achieved. (post successful check of the same during credential inputs Oracle WebLogic Administration Server not reachable (post successful check of the same during credential inputs)	Check the OPatchauto log file for the failure.

OPatchauto: External Utilities Error Codes

The following table lists exit codes for external utilities that OPatchauto uses for life cycle and deployment. If the deployment (or) life cycle fails through OPatchauto, the administrator can search individual log files for the error messages shown in the *Error Message/Recommendation* column.

Table 17–10 OPatchauto External Utilities Error Codes

Exit Code	Error Message / Recommendation
34	Displays the usage of the command.
35	Unable to read password! Exiting...
36	Unable to get a connection to the repository! Exiting...
37	The Plug-in is not deployed on this Management Server. The plug-in has to be deployed first to register metadata for that plug-in.
38	Input file does not exist
39	This operation is not supported by service.
40	Metadata operation is skipped.
41	Error occurred during Metadata registration.
42	Error occurred during Metadata de-registration.

Special Error Cases for OPatchauto OMS Automation

This section provides issue resolution information for special cases when using OPatchauto. This information will allow the administrator to handle these issues easily with less need for support team intervention.

Windows patching failure due to lock of files by Oracle WebLogic Administration Server

In Windows operating systems, it has been noticed that some of the Enterprise Manager related files (used for patching) are locked by running of Oracle WebLogic Administration Server. As OPatchauto required Oracle WebLogic Administration Server to be RUNNING for the configuration detection, we need to perform the following steps to make sure that this conflict with respect to environment and patching is removed.

1. Go to ORACLE_HOME
2. Run OPatchauto in non-analyze mode. For further instructions, refer to the patch README and Administrator guide.

   Once the OPatchauto is run in non-analyze mode, it will check if active files are locked by Oracle WebLogic administration server and will provide a prompt as shown below (in silent mode it will be auto-yes):

   ```
   Running prerequisite checks to verify if any files or services are locked by
   admin server process...
   Please monitor OPatch log file: c:\MW_130518\oms\cfgtoollogs\opatch\1111112_
   Jun_
   26_2014_08_16_19\ApplyPrereq2014-06-26_08-16-57AM_8.log

   The details are:

   Following files are active :
   c:\MW_130518\oms\sysman\jlib\emCoreConsole.jar

   Due to active files to be patched, opatchauto will stop all OMS processes so
   tha
   t lock on active files may be released...
   Do you want to proceed? [y|n]
   y
   User Responded with: Y
   opatchauto has stopped all OMS processes successfully.
   ```

   If there is a failure while stopping OMS processes, OPatchauto will accordingly error out. Refer to the OPatchauto log file for details.
3. OPatchauto will stop the stack and then ask for a confirmation from the administrator on whether to proceed with prerequisite checks of patch binaries (in silent mode it will be auto-yes):

   ```
   opatchauto has stopped all OMS processes successfully. Please make sure the
   above listed active files are unlocked by all windows processes.
   Do you want to proceed? [y|n] y

   User Responded with: Y
   ```

Note: Administrators are requested to use some open source utilities like process explorer and search for file strings given as output in (2) to check if any files are still active. If so, kill the process tree of those files so that OPatch will run the checks, patch, and deploy the automation elements.

---

4. OPatchauto will not attempt to re-start the stack. The administrator must restart the stack as needed.

   A complete sample trace of this case is shown below:

```
C:\MW_130518\oms\OPatch_June26>opatchauto apply ..\patches\cmdRcu\1111112
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.


OPatchauto version : 11.1.0.10.4
OUI version        : 11.1.0.12.0
Running from       : c:\MW_130518\oms
Log file location  : c:\MW_130518\oms\cfgtoollogs\opatch\opatch2014-06-26_
08-16-19AM_1.log

opatchauto log file: c:\MW_130518\oms\cfgtoollogs\opatchauto\1111112\opatch_
oms_2014-06-26_08-16-23AM_deploy.log

Please enter the WebLogic Admin Server URL for primary OMS:> t3s://example.o
racle.com:7101
Please enter the WebLogic Admin Server username for primary OMS:> weblogic
Please enter the WebLogic Admin Server password for primary OMS:>

Configuration Validation: Success


Running prerequisite checks to verify if any files or services are locked by
admin server process...
Please monitor OPatch log file: c:\MW_130518\oms\cfgtoollogs\opatch\1111112_
Jun_26_2014_08_16_19\ApplyPrereq2014-06-26_08-16-57AM_8.log

The details are:

Following files are active :
c:\MW_130518\oms\sysman\jlib\emCoreConsole.jar

Due to active files to be patched, opatchauto will stop all OMS processes so
that lock on active files may be released...
Do you want to proceed? [y|n]
y
User Responded with: Y
opatchauto has stopped all OMS processes successfully.


opatchauto has stopped all OMS processes successfully. Please make sure the
above listed active files are unlocked by all windows processes.
Do you want to proceed? [y|n]
y
User Responded with: Y

Running apply prerequisite checks for patch(es) "1111112" and Oracle Home
"c:\MW
```

```
_130518\oms"...
Please monitor OPatch log file: c:\MW_130518\oms\cfgtoollogs\opatch\1111112_
Jun_26_2014_09_01_33\ApplyPrereq2014-06-26_09-03-41AM_10.log
Patches "1111112" are successfully analyzed for Oracle Home "c:\MW_130518\oms"

To continue, OPatch will do the following:
[Patch and deploy patch(es) binaries]   : Apply patch(es) [ 1111112 ] to Oracle
Home "c:\MW_130518\oms";
                                          Apply RCU artifact with patch "c:\MW_
130518\oms\.patch_storage\1111112_Feb_21_2014_06_30_38\original_patch"


Do you want to proceed? [y|n]
y
User Responded with: Y

Applying patch "1111112" to Oracle Home "c:\MW_130518\oms"...
Please monitor OPatch log file: c:\MW_130518\oms\cfgtoollogs\opatch\1111112_
Jun_26_2014_09_01_33\apply2014-06-26_09-04-17AM_12.log

Updating repository with RCU reference file "c:\MW_130518\oms\.patch_
storage\1111112_Feb_21_2014_06_30_38\original_patch"

Copying all logs to: c:\MW_130518\oms\cfgtoollogs\opatch\2014-06-26_09-01-32AM_
SystemPatch_1111112_1

Patching summary:
Following patch(es) are successfully applied (Oracle home:patch list):
c:\MW_130518\oms:1111112


Log file location: c:\MW_130518\oms\cfgtoollogs\opatchauto\1111112\opatch_oms_
2013-06-26_09-01-36AM_deploy.log

opatchauto succeeded.
```

Multi-OMS Execution for UNIX based Systems

This section deals with possible issues you may encounter when running bash scripts generated by OPatchauto in multi-OMS (UNIX-based systems) environment. The following OPatchauto-generated output illustrates various script-based issues.

Example 17–5 OPatchauto Output: Multi-OMS, UNIX-based Environment

```
$ OPatch/opatchauto apply /scratch/aime/patches/ComparisonTemplate/1111136
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.

OPatchauto version : 11.1.0.10.4
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime/work/midnew6898/oms
Log file location  :
 /scratch/aime/work/midnew6898/oms/cfgtoollogs/opatch/opatch2014-05-28_11-39-39AM_
1.log

OPatchauto log file:
/scratch/aime/work/midnew6898/oms/cfgtoollogs/opatchauto/1111136/opatch_oms_
2014-05-28_11-39-40AM_deploy.log

Please enter OMS weblogic admin server URL(t3s://linux07jif.myco.com:7101):>
Please enter OMS weblogic admin server username:> weblogic
Please enter OMS weblogic admin server password:>

Configuration Validation: Success

WARNING: OPatchauto cannot run patching steps in multi-OMS environment.

Please perform the following steps to complete patching operations.
-------------------------------------------------------------------
1. Please copy the script "/scratch/aime/work/midnew6898/oms/.patch_
storage/oms/scripts_2014-05-28_11-40-01/run_script#1_on_host_linux06xlv_us_oracle_
com_as_user_aime.sh" to "linux06xlv.myco.com" and execute the script.

2. Please execute the script "/scratch/aime/work/midnew6898/oms/.patch_
storage/oms/scripts_2014-05-28_11-40-01/run_script#2_on_host_linux07jif_us_oracle_
com_as_user_aime.sh" on local host.

--------------------------------------------------------------------------------
The following warnings have occurred during OPatchauto execution:
1)  OPatchauto cannot run patching steps in multi-OMS environment.

--------------------------------------------------------------------------------
OPatchauto Session completed with warnings.
Log file location:
/scratch/aime/work/midnew6898/oms/cfgtoollogs/opatchauto/1111136/opatch_oms_
2014-05-28_11-39-40AM_deploy.log

OPatchauto completed with warnings.
```

Note 1: Generation of bash scripts is only available for UNIX based systems running OPatchauto 11.1.0.10.2 and above.

Note 2: OPatchAuto completes with *warnings* with *clear* messages For example:

```
WARNING: OPatchauto cannot automate patching steps
in multi-OMS environment.
```

This means that patching and deployment **are not** complete until the administrator performs the bash script execution instructions generated by OPatchatuo.

Troubleshooting Bash Script Execution

The following section covers the most common issues you may encounter while executing OPatchauto-generated bash scripts in multi-OMS (UNIX-based) environments.

No Windows Support

Microsoft Windows does not support bash script execution. So, this optimization (steps reduction) is not applicable for Windows OMS PS2 environments. The older context sensitive individual steps output through OPatchAuto remains in Windows.

Bash script program availability

The scripts assume that bash is located at `/bin/bash`. However, if this is not true, make sure the first line of the scripts are updated with the output of `whereis bash`.

In-between command failure in bash script

If there is a failure in between execution of commands in the bash script, the script stops running. The OMS administrator must triage the failure and comment out (inserting a hash "#" character at the beginning of a line) the already executed portions of the script and restart the bash script execution. Make sure you do not to comment out prompts and prompt-related code in the script.

Complete execution needed for all bash scripts

ALL bash script steps must be executed. No script and no step within any script can be omitted, even in the event of failures. Patching is correct and complete if and only if all steps of all bash scripts are executed correctly as per the order specification.

Patch location (if mounted)

The patch location input may exist on a mounted location. The bash scripts try to perform a secure copy (SCP) from the local OMS (where the OPatchauto Perl script was invoked). The SCP attempt could fail if the location is mounted. The bash script will ignore the SCP failure.

OMS repository SYSMAN password and prompts

The bash script prompts for OMS repository SYSMAN password only at the point where a command requires this information. The script does not prompt for the SYSMAN password at the beginning of the script. For this reason, pay special attention to prompts at all places of the script execution. Bash script execution is not a silent execution.

The bash script prompt will appear as follows:

Please provide credential for OMS repository SYSMAN user:

Patch Transfer/Download

The script will provide an option to download patch from local OMS to remote nodes (for the scripts that involve remote nodes). If the patch is on shared location (or) already downloaded to a specified location mentioned by the script, a user can choose to input *n* when prompted, and ignore this transfer.

Features in OPatchauto Release 11.1.0.11.0 and Above

OPatchauto Release 11.1.0.11.0 and above supports resume upon failure capability for both single-OMS and multi-OMS configurations.

This section covers the following topics:

- Resume capability in Single-OMS Configuration
- Resume Capability in Multi-OMS Configuration

Resume capability in Single-OMS Configuration

On a single OMS System, OPatchauto executes end-to-end automation of patching steps. Beginning with release 11.1.0.11.0, once a failure has occurred, OPatchauto can generate a bash script containing list of all incomplete (or) failed steps. The OMS administrator must refer to the master log file created by OPatchauto to ascertain and resolve the root cause of the failure, and then run the bash script given by OPatchauto. The bash script runs the steps from the point of failure.

Example

1. OPatchauto, while applying an auto system patch. fails due to file permission issue.

```
OPatch/opatchauto apply /net/adc2100679/scratch/opack_system_
patch/ps2Convertedps3/targetPatchingImplRegistration/1111118
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.


OPatchauto version : 11.1.0.11.0
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime/work/midnew270/oms
Log file location  :
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-05_
04-56-44AM_1.log

OPatchauto log file:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-05_04-56-48AM_deploy.log

Please enter OMS weblogic admin server URL(t3s://linux01moa.myco.com:7101):>
Please enter OMS weblogic admin server username:> weblogic
Please enter OMS weblogic admin server password:>


Configuration Validation: Success


Running apply prerequisite checks for sub-patch(es) "1111118" and Oracle Home
"/scratch/aime/work/midnew270/oms"...
Please monitor OPatch log file:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/1111118_May_05_2014_04_56_
44/ApplyPrereq2014-05-05_04-57-42AM_2.log
Sub-patch(es) "1111118" are successfully analyzed for Oracle Home
"/scratch/aime/work/midnew270/oms"

To continue, OPatchauto will do the following:
[Patch and deploy artifacts]   : Apply sub-patch(es) [ 1111118 ] to Oracle Home
"/scratch/aime/work/midnew270/oms";
                                 Register MRS artifact
"TargetPatchingImplRegistration"


Do you want to proceed? [y|n]
y
User Responded with: Y

Applying sub-patch "1111118" to Oracle Home
```

```
"/scratch/aime/work/midnew270/oms"...
Please monitor OPatch log file:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/1111118_May_05_2014_04_56_
44/apply2014-05-05_05-02-45AM_4.log


OPatchauto failed to apply following patch(es) "1111118"  to core/plugin Oracle
home(s).

Complete Summary
================

All log file names referenced below can be accessed from the directory
"/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/2014-05-05_04-56-44AM_
SystemPatch_1111118_1"

Patching summary:
-----------------

The following sub-patch(es) are applicable:

Oracle Home Name   Sub-patches                 Log file
----------------   -----------                 --------
      oms12c1       1111118   1111118_ApplyPrereq2014-05-05_04-57-42AM_2.log


Binaries of the following sub-patch(es) failed to get applied:

  Oracle Home Name   Sub-patches                Log file
  ----------------   -----------                --------
        ms12c1       1111118   1111118_apply2014-05-05_05-02-45AM_4.log



OPatchauto failed to execute some of the patching steps. Please check the
Patching summary,individual logs and
try to resolve the issue. Once the issue is resolved,Please execute below
script to complete patching session:
"/scratch/aime/work/midnew270/oms/.opatchauto_patch_storage/oms_
session/scripts_2014-05-05_04-56-44AM/run_script_singleoms_resume.sh"

--------------------------------------------------------------------------------
OPatchauto wont allow any other patching operations unless the script is
executed successfully
--------------------------------------------------------------------------------

[ Error during Patch and deploy artifacts Phase]. Detail: opatchauto failed to
apply some of the patches to the OMS instance home(s).
OPatchauto failed: OPatchauto failed to execute some of the OMS operations.
Please refer log file(s) for details.
Log file location:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-05_04-56-48AM_deploy.log

Recommended actions: Please refer log file(s) for more details on the errors.
Please contact Oracle Support.

OPatchauto failed with error code 241
```

2. OMS Administrator cannot start a new patching session when there are remnants of an incomplete patching session. OPatchauto clearly errors out with the detailed information regarding the failure and what action need to be taken to fix this issue.

```
$opatchauto apply /net/adc2100679/scratch/opack_system_
patch/ps2Convertedps3/Probanal/9111111
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.

OPatchauto version : 11.1.0.11.0
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime/work/midnew270/oms
Log file location  :
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-05_
05-20-49AM_1.log

OPatchauto failed:

OPatchauto finds that previous patching session is not yet completed. Please
refer log file
"/scratch/aime/work/midnew270/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-05_04-56-48AM_deploy.log"
for the previous session and execute the script
"/scratch/aime/work/midnew270/oms/.opatchauto_patch_storage/oms_
session/scripts_2014-05-05_04-56-44AM/run_script_singleoms_resume.sh"
to complete the previous session. OPatchauto can proceed to execute new
operations only if previous session is completed successfully.

Log file location:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-05_
05-20-49AM_1.log

OPatchauto failed with error code 73
```

3. Now OMS Administrator can run the single-OMS Resume script to finish the failed patching session

```
$ /scratch/aime/work/midnew270/oms/.opatchauto_patch_storage/oms_
session/scripts_2014-05-05_04-56-44AM/run_script_singleoms_resume.sh

Please provide credential for OMS repository SYSMAN user:
Command to execute (Step 1): echo /net/adc2100679/scratch/opack_system_
patch/ps2Convertedps3/targetPatchingImplRegistration/1111118/1111118 >>
/scratch/aime/work/midnew270/oms/.phBaseFile2014-05-05_04-56-44AM.txt
Command to execute (Step 1): /scratch/aime/work/midnew270/oms/OPatch/opatch
napply -phBaseFile /scratch/aime/work/midnew270/oms/.phBaseFile2014-05-05_
04-56-44AM.txt -invPtrLoc /scratch/aime/work/midnew270/oms/oraInst.loc -oh
/scratch/aime/work/midnew270/oms -silent
Command to execute (Step 1): rm
/scratch/aime/work/midnew270/oms/.phBaseFile2014-05-05_04-56-44AM.txt
Oracle Interim Patch Installer version 11.1.0.11.0
Copyright (c) 2014, Oracle Corporation.  All rights reserved.


Oracle Home       : /scratch/aime/work/midnew270/oms
Central Inventory : /ade/aime_emgcview/oracle/work/DB112/oraInventory
   from           : /scratch/aime/work/midnew270/oms/oraInst.loc
OPatch version    : 11.1.0.11.0
OUI version       : 11.1.0.12.0
Log file location :
```

```
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-05_
05-28-53AM_1.log


OPatch detects the Middleware Home as "/scratch/aime/work/midnew270"

Verifying environment and performing prerequisite checks...
OPatch continues with these patches:   1111118

Do you want to proceed? [y|n]
Y (auto-answered by -silent)
User Responded with: Y
All checks passed.
Backing up files...
Applying interim patch '1111118' to OH '/scratch/aime/work/midnew270/oms'

Patching component oracle.sysman.oms.core, 12.1.0.4.0...

Verifying the update...
Patch 1111118 successfully applied.
Log file location:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-05_
05-28-53AM_1.log

OPatch succeeded.
Command to execute (Step 2): /scratch/aime/work/midnew270/oms/bin/emctl
register oms metadata -service TargetPatchingImplRegistration -debug -file
/scratch/aime/work/midnew270/oms/sysman/metadata/targetpatchingregister/Registe
rAgentTarget.xml -core -sysman_pwd %EM_REPOS_PASSWORD%
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
Starting output for debug mode.
 Debug logs will be written to /scratch/aime/work/insthome270/em/EMGC_
OMS1/sysman/log/emctl.log
Metadata registration successful
Command to execute (Step 3): /scratch/aime/work/midnew270/oms/OPatch/opatchauto
commit -id 1111118 -oh /scratch/aime/work/midnew270/oms -invPtrLoc
/scratch/aime/work/midnew270/oms/oraInst.loc
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.


OPatchauto version : 11.1.0.11.0
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime/work/midnew270/oms
Log file location  :
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-05_
05-29-21AM_1.log


OPatchauto will now mark the patch "1111118" as auto-executed.
Log file location:
/scratch/aime/work/midnew270/oms/cfgtoollogs/opatch/opatch2014-05-05_
05-29-21AM_1.log

OPatchauto succeeded.

OPatchauto rollback is also supported for resume feature and it works in the
same way how apply works.
```

Resume Capability in Multi-OMS Configuration

The 11.1.0.11.0 version of OPatchauto prompts for the SYSMAN password at the start of the script unlike in previous release of OPatchauto where the SYSMAN password must be entered only at the time deploy commands are executed. OPatchauto cannot execute patching steps on a multi-OMS configuration, It generates a bash script containing all the patching steps specific to each host for all the nodes. The name of the script contains hostname, username. OMS administrator can run a specific script for each host on all nodes to complete patching session.

1. OPatchauto apply executes successfully as it generates only patching instructions without executing bash scripts.

```
$ OPatch/opatchauto apply
/scratch/opatchdev/targetPatchingImplRegistration/1111118
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.


OPatchauto version : 11.1.0.11.0
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime1/work/midnew9693/oms
Log file location  :
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatch/opatch2014-05-05_
22-43-08PM_1.log

OPatchauto log file:
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-05_22-43-14PM_deploy.log

Please enter OMS weblogic admin server URL(t3s://linux01amd.myco.com:7101):>
Please enter OMS weblogic admin server username:> weblogic
Please enter OMS weblogic admin server password:>


Configuration Validation: Success

WARNING: OPatchauto cannot run patching steps in multi-OMS environment.


Please perform the following steps to complete patching operations.
-------------------------------------------------------------------
        1. Please copy the script
"/scratch/aime1/work/midnew9693/oms/.opatchauto_patch_storage/oms_
session/scripts_2014-05-05_22-43-51/run_script#1_on_host_linux07jdx_us_oracle_
com_as_user_aime1.sh" to "linux07jdx.myco.com" and execute the script.
        2. Please execute the script
"/scratch/aime1/work/midnew9693/oms/.opatchauto_patch_storage/oms_
session/scripts_2014-05-05_22-43-51/run_script#2_on_host_linux01amd_us_oracle_
com_as_user_aime1.sh" on local host.

-------------------------------------------------------------------------------
-
The following warnings have occurred during OPatchauto execution:
1)  OPatchauto cannot run patching steps in multi-OMS environment.

-------------------------------------------------------------------------------
-
OPatchauto Session completed with warnings.
```

```
Log file location:
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-05_22-43-14PM_deploy.log

OPatchauto completed with warnings.
```

2. Run the bash script corresponding to the local host(primary host on a Multi-OMS configuration). Script execution has failed because of issue in connecting to database repository because of incorrect sysman password.

```
[aime1@linux01amd oms]$ /scratch/aime1/work/midnew9693/oms/.opatchauto_patch_
storage/oms_session/scripts_2014-05-05_22-43-51/run_script#2_on_host_
linux01amd_us_oracle_com_as_user_aime1.sh
Creating  master log file /scratch/aime1/work/midnew9693/oms/.opatchauto_patch_
storage/oms_session/oms_session_log_2014-05-05_22-43-08PM...
Creating  session file /scratch/aime1/work/midnew9693/oms/.opatchauto_patch_
storage/oms_session/oms_session_2014-05-05_22-43-08PM...

Please provide credential for OMS repository SYSMAN user:
Command to execute (Step 2):
/scratch/aime1/work/midnew9693/oms/OPatch/opatchauto checkApplicable -ph
/scratch/opatchdev/targetPatchingImplRegistration/1111118 -oh
/scratch/aime1/work/midnew9693/oms -invPtrLoc
/scratch/aime1/work/midnew9693/oms/oraInst.loc
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.


OPatchauto version : 11.1.0.11.0
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime1/work/midnew9693/oms
Log file location  :
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatch/opatch2014-05-05_
22-45-52PM_1.log

OPatchauto log file:
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-05_22-45-53PM_analyze.log



Running apply prerequisite checks for sub-patch(es) "1111118" and Oracle Home
"/scratch/aime1/work/midnew9693/oms"...
Please monitor OPatch log file:
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatch/1111118_May_05_2014_22_
45_52/ApplyPrereq2014-05-05_22-45-57PM_2.log
Sub-patch(es) "1111118" are successfully analyzed for Oracle Home
"/scratch/aime1/work/midnew9693/oms"

Complete Summary
================

All log file names referenced below can be accessed from the directory
"/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatch/2014-05-05_22-45-52PM_
SystemPatch_1111118_1"

Prerequisites analysis summary:
-------------------------------

The following sub-patch(es) are applicable:
```

```
Oracle Home Name   Sub-patches             Log file
----------------   -----------             --------
     oms12c1       1111118   1111118_ApplyPrereq2014-05-05_22-45-57PM_2.log



Log file location:
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatchauto/1111118/opatch_oms_
2014-05-05_22-45-53PM_analyze.log

OPatchauto succeeded.
Command to execute (Step 4): echo
/scratch/opatchdev/targetPatchingImplRegistration/1111118/1111118 >>
/scratch/aime1/work/midnew9693/oms/.phBaseFile2014-05-05_22-43-08PM.txt
Command to execute (Step 4): /scratch/aime1/work/midnew9693/oms/OPatch/opatch
napply -phBaseFile /scratch/aime1/work/midnew9693/oms/.phBaseFile2014-05-05_
22-43-08PM.txt -invPtrLoc /scratch/aime1/work/midnew9693/oms/oraInst.loc -oh
/scratch/aime1/work/midnew9693/oms -silent
Command to execute (Step 4): rm
/scratch/aime1/work/midnew9693/oms/.phBaseFile2014-05-05_22-43-08PM.txt
Oracle Interim Patch Installer version 11.1.0.11.0
Copyright (c) 2014, Oracle Corporation.  All rights reserved.


Oracle Home       : /scratch/aime1/work/midnew9693/oms
Central Inventory : /ade/aime1_opatchauto_fix_
lat/oracle/work/DB112/oraInventory
   from           : /scratch/aime1/work/midnew9693/oms/oraInst.loc
OPatch version    : 11.1.0.11.0
OUI version       : 11.1.0.12.0
Log file location :
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatch/opatch2014-05-05_
22-46-00PM_1.log


OPatch detects the Middleware Home as "/scratch/aime1/work/midnew9693"

Verifying environment and performing prerequisite checks...
OPatch continues with these patches:   1111118

Do you want to proceed? [y|n]
Y (auto-answered by -silent)
User Responded with: Y
All checks passed.
Backing up files...
Applying interim patch '1111118' to OH '/scratch/aime1/work/midnew9693/oms'

Patching component oracle.sysman.oms.core, 12.1.0.4.0...

Verifying the update...
Patch 1111118 successfully applied.
Log file location:
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatch/opatch2014-05-05_
22-46-00PM_1.log

OPatch succeeded.
Command to execute (Step 6): /scratch/aime1/work/midnew9693/oms/bin/emctl
register oms metadata -service TargetPatchingImplRegistration -debug -file
/scratch/aime1/work/midnew9693/oms/sysman/metadata/targetpatchingregister/Regis
```

```
terAgentTarget.xml -core -sysman_pwd %EM_REPOS_PASSWORD%
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
Starting output for debug mode.
 Debug logs will be written to /scratch/aime1/work/insthome9693/em/EMGC_
OMS1/sysman/log/emctl.log
EM-04036: Unable to get a connection to the repository!  Exiting...
The command failed with error code 36


Script execution has failed. Please refer to log file:
/scratch/aime1/work/midnew9693/oms/.opatchauto_patch_storage/oms_session/oms_
session_log_2014-05-05_22-43-08PM for more details

Please fix the failures and re-run the same script to complete the patching
session.
```

3. OMS Administrator can re-run the script by fixing the issue (provide correct sysman password to connect to database repository.). Script resumes execution from the failure point and executes successfully.

```
[aime1@linux01amd oms]$ /scratch/aime1/work/midnew9693/oms/.opatchauto_patch_
storage/oms_session/scripts_2014-05-05_22-43-51/run_script#2_on_host_
linux01amd_us_oracle_com_as_user_aime1.sh

Please provide credential for OMS repository SYSMAN user:
Command to execute (Step 2):
/scratch/aime1/work/midnew9693/oms/OPatch/opatchauto checkApplicable -ph
/scratch/opatchdev/targetPatchingImplRegistration/1111118 -oh
/scratch/aime1/work/midnew9693/oms -invPtrLoc
/scratch/aime1/work/midnew9693/oms/oraInst.loc
SKIP command for step 2...
Command to execute (Step 4): echo
/scratch/opatchdev/targetPatchingImplRegistration/1111118/1111118 >>
/scratch/aime1/work/midnew9693/oms/.phBaseFile2014-05-05_22-43-08PM.txt
Command to execute (Step 4): /scratch/aime1/work/midnew9693/oms/OPatch/opatch
napply -phBaseFile /scratch/aime1/work/midnew9693/oms/.phBaseFile2014-05-05_
22-43-08PM.txt -invPtrLoc /scratch/aime1/work/midnew9693/oms/oraInst.loc -oh
/scratch/aime1/work/midnew9693/oms -silent
Command to execute (Step 4): rm
/scratch/aime1/work/midnew9693/oms/.phBaseFile2014-05-05_22-43-08PM.txt
SKIP command for step 4...
Command to execute (Step 6): /scratch/aime1/work/midnew9693/oms/bin/emctl
register oms metadata -service TargetPatchingImplRegistration -debug -file
/scratch/aime1/work/midnew9693/oms/sysman/metadata/targetpatchingregister/Regis
terAgentTarget.xml -core -sysman_pwd %EM_REPOS_PASSWORD%
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
Starting output for debug mode.
 Debug logs will be written to /scratch/aime1/work/insthome9693/em/EMGC_
OMS1/sysman/log/emctl.log
Metadata registration successful
Command to execute (Step 7):
/scratch/aime1/work/midnew9693/oms/OPatch/opatchauto commit -id 1111118 -oh
/scratch/aime1/work/midnew9693/oms -invPtrLoc
/scratch/aime1/work/midnew9693/oms/oraInst.loc
OPatch Automation Tool
Copyright (c) 2014, Oracle Corporation.  All rights reserved.
```

```
OPatchauto version : 11.1.0.11.0
OUI version        : 11.1.0.12.0
Running from       : /scratch/aime1/work/midnew9693/oms
Log file location  :
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatch/opatch2014-05-05_
22-49-34PM_1.log


OPatchauto will now mark the patch "1111118" as auto-executed.
Log file location:
/scratch/aime1/work/midnew9693/oms/cfgtoollogs/opatch/opatch2014-05-05_
22-49-34PM_1.log

OPatchauto succeeded.


All operations for this script are appended to log file:
/scratch/aime1/work/midnew9693/oms/.opatchauto_patch_storage/oms_session/oms_
session_log_2014-05-05_22-43-08PM
```

18

Patching Oracle Management Agents

This chapter describes how to patch Oracle Management Agents (Management Agents) in Enterprise Manager Cloud Control (Cloud Control).

This chapter consists of the following sections:

- Overview
- Automated Management Agent Patching Using Patch Plans (Recommended)
- Manual Management Agent Patching

18.1 Overview

Management Agent patches are released to fix one or more errors related to Management Agent targets. You can patch Management Agents that are deployed on OMS hosts, as well as remote hosts. In Cloud Control, separate Management Agent patches exist for core components of Management Agents and Management Agent plug-ins.

You can apply Management Agent patches using the automated approach (that is, using patch plans) or the manual approach. Oracle recommends using the automated approach to carry out your patching operations. This approach not only saves time and effort while mass-deploying patches, but also reduces human intervention, thereby minimizing the errors involved while patching. For more information about this approach, see Section 18.2.

If you are unable to patch your Management Agent targets using patch plans, you can use the manual patching approach. However, this approach is not recommended. For more information about this approach, see Section 18.3.

18.2 Automated Management Agent Patching Using Patch Plans (Recommended)

Automated patching is a quick, easy, and reliable patching mechanism that is facilitated using patch plans in Cloud Control. Patch plans can be created, accessed, and deployed using the Cloud Control console, or EM CLI. For large scale deployments, you can use EM CLI to create, access, and deploy patch plans. This section only describes how to patch your Management Agent targets using the Cloud Control console. For information about patching targets using EM CLI, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

Automated patching can be performed while Cloud Control is running in the Online mode, as well as the Offline mode. When Cloud Control is running in the Online mode, you can connect to *My Oracle Support* to download the patches that you want to apply. However, if Cloud Control is running in the Offline mode, you must ensure that the patches that you want to apply are already available in Oracle Software Library (Software Library).

This section consists of the following:

- Advantages of Automated Management Agent Patching
- Accessing the Patches and Updates Page
- Viewing Patch Recommendations
- Searching for Patches
- Applying Management Agent Patches
- Verifying the Applied Management Agent Patches
- Management Agent Patching Errors

18.2.1 Advantages of Automated Management Agent Patching

The advantages of patching your Management Agent targets using the automated approach (as compared to the manual approach) are:

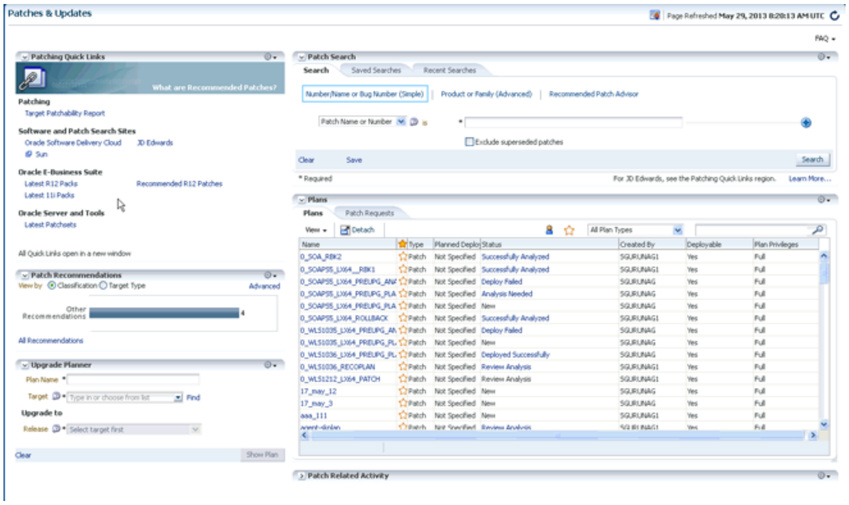
- Patching operations are more organized, done through a single window, and are always initiated only from the OMS.
- This approach allows you to schedule periodic patching jobs that connect to *My Oracle Support,* check for the latest patches, and automatically download them. This saves the effort involved in searching for the latest patches and patch sets, and downloading them whenever they are available.
- Multiple patches and multiple sets of homogeneous targets can be added to a single patch plan. For example, both core and plug-in component Management Agent patches can be patched by adding them to the same patch plan.

18.2.2 Accessing the Patches and Updates Page

To access the Patches and Updates page in Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching,** then select **Patches & Updates**.

Figure 18–1 displays the Patches and Updates page.

Figure 18–1 Patches and Updates Page



Name	☆	Type	Planned Deplo	Status	Created By	Deployable	Plan Privileges
0_SOA_RBK2	☆	Patch	Not Specified	Successfully Analyzed	SGURUNAG1	Yes	Full
0_SOAPS5_LX64__RBK1	☆	Patch	Not Specified	Successfully Analyzed	SGURUNAG1	Yes	Full
0_SOAPS5_LX64_PREUPG_ANA	☆	Patch	Not Specified	Deploy Failed	SGURUNAG	Yes	Full
0_SOAPS5_LX64_PREUPG_PLA	☆	Patch	Not Specified	Analysis Needed	SGURUNAG	Yes	Full
0_SOAPS5_LX64_PREUPG_PLA	☆	Patch	Not Specified	New	SGURUNAG	Yes	Full
0_SOAPS5_LX64_ROLLBACK	☆	Patch	Not Specified	Successfully Analyzed	SGURUNAG1	Yes	Full
0_WLS1035_LX64_PREUPG_AN	☆	Patch	Not Specified	Deploy Failed	SGURUNAG	Yes	Full
0_WLS1035_LX64_PREUPG_PL	☆	Patch	Not Specified	New	SGURUNAG	Yes	Full
0_WLS1036_LX64_PREUPG_PL	☆	Patch	Not Specified	Deployed Successfully	SGURUNAG	Yes	Full
0_WLS1036_RECOPLAN	☆	Patch	Not Specified	Review Analysis	SGURUNAG1	Yes	Full
0_WLS1212_LX64_PATCH	☆	Patch	Not Specified	Review Analysis	SGURUNAG1	Yes	Full
17_may_12	☆	Patch	Not Specified	New	SGURUNAG	Yes	Full
17_may_3	☆	Patch	Not Specified	New	SGURUNAG	Yes	Full
aaa_111	☆	Patch	Not Specified	New	SGURUNAG1	Yes	Full
agent-dinlan	☆	Patch	Not Specified	Review Analysis	SGURUNAG1	Yes	Full

18.2.3 Viewing Patch Recommendations

Patch recommendations are proactive notifications of potential system problems and recommendations that help you improve system performance and avert outages. Patch recommendations minimize the effort required to search for the critical patches that must be applied on your targets.

The Patch Recommendations section is available on the Patches and Updates page. The patches in this section are classified as security patches, and other recommended patches.

For more information about patch recommendations, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

Note:

- Patch recommendations are available only if Oracle Configuration Manager Release 10.3.2 or higher is deployed in your enterprise.
- Patch recommendations are not available for custom plug-ins. They available only for the default plug-ins that are released with Cloud Control.

18.2.4 Searching for Patches

This section consists of the following:

- Searching for Patches On My Oracle Support
- Searching for Patches in Software Library

18.2.4.1 Searching for Patches On My Oracle Support

If you already know about the existence of a patch from external sources such as blogs, Oracle technology forums, or from colleagues, then use the search functionality to search for those patches. The search functionality enables you to perform more flexible and advanced searches, and offers capabilities such as saving a search that is used routinely, and searching based on existing saved searches. All of this enables you to perform searches quickly and efficiently.

To search for a patch on My Oracle Support, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. To perform a simple search, in the Patch Search region, select **Number/Name or Bug Number (Simple),** then specify the patch name, patch number, or the bug number. Click **Search**.

   To perform an advanced search, select **Product or Family (Advanced),** then specify the product, release, and any other criteria you wish to use for the patch search.

   Alternatively, you can use the **Saved** tab to search for previously saved searches. You can also use the **Recent** tab to access any recently performed searches.

   Once the patch search is complete, the results appear in the **Patch Search Results** page. On this page, you can select a patch and download it either to the local host or to Software Library.

18.2.4.2 Searching for Patches in Software Library

By default, when you search for a patch on the Patches & Updates page, Cloud Control connects to My Oracle Support using the Internet connectivity available on that host, and searches for the requested patch on My Oracle Support. This is because the search functionality is set to perform in online mode by default.

However, if your host does not have Internet connectivity, then you must switch over to offline mode so that the search can be performed in Software Library.

To switch over to offline mode, follow these steps:

1. From the **Setup** menu, select **Provisioning and Patching,** then select **Offline Patching.**
2. For **Connection,** select **Offline**.

Note: In offline mode, you cannot:

- Search and download patches from My Oracle Support
- Resolve patch conflicts with merge patches
- View the Related Activity region
- Access Quicklinks
- View or create upgrade plans

To search for a patch in Software Library, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. To perform a simple search, in the Software Library Patch Search region, select **Number/Name or Bug Number (Simple),** then specify the patch name, patch number, or the bug number. Click **Search**.

   To perform an advanced search, select **Product or Family (Advanced),** then specify the product, release, and any other criteria you wish to use for the patch search.

   Alternatively, you can use the **Saved** tab to search for previously saved searches. You can also use the **Recent** tab to access any recently performed searches.

Once the patch search is complete, the results appear in the **Patch Search Results** page.

18.2.5 Applying Management Agent Patches

To apply Management Agent patches using patch plans, follow these steps:

Note:

- Using patch plans, you can apply patches on the core components of Management Agents, as well as on Management Agent plug-ins. The patching process that must be used for both actions is the same, and is described in this section.
- For a large scale deployments, you can use EM CLI. For information about patching using EM CLI, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

---

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches and Updates**.
2. On the Patches and Updates page, select the Management Agent patches that you want to apply from the Patch Recommendations section, or the Patch Search section.

   For more information on the Patch Recommendation section, see Section 18.2.3. For more information on how to search for patches, see Section 18.2.4.
3. From the context menu that appears, select one of the following options:
   - **Add to New:** Select this option if you want to create a new patch plan that has the selected patch.

     Specify a plan name, the targets that you want to patch, then click **Create Plan.**

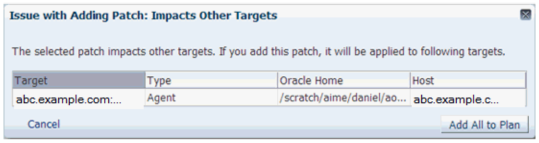
     The patch and the associated targets are added to the patch plan.
   - **Add to Existing Plan:** Select this option if you want to add the selected patch to an existing patch plan.

     Select the existing patch plan that you want to add the required patch to, specify the patch targets, then click **Add Patch to Plan.**

   Note: Ensure that the patches you select have the same platform as the targets that you want to patch. For example, Linux x86 patches can be applied only on Linux x86 targets. Any mismatch will result in a patching error.

   ---
4. If the selected patches are applied on homogeneous targets, then the patch plan is created successfully with a link to view the patch plan. Click the link to view the patch plan details.

   If any of the Management Agent targets added to the patch plan are shared agents or cluster Management Agents, then you may see a warning message mentioning that there are issues with adding the patch to the patch plan.



Issue with Adding Patch: Impacts Other Targets

The selected patch impacts other targets. If you add this patch, it will be applied to following targets.

Target	Type	Oracle Home	Host
abc.example.com:...	Agent	/scratch/aime/daniel/ao...	abc.example.c...

As a solution to this problem, click **Add All To Plan** to add all the affected targets to the patch plan.

However, if the platform of the selected patch does not match the platform of the selected target, you may see one of the following errors or warnings:

- A null platform error occurs when the selected target appears with a null platform. The patch plan validation fails as platform of the patch and the platform of the target do not match. This may occur when a target is down. In this case, the patch plan is not created until the error is fixed.
- A platform mismatch warning appears when the platform of the patch and the platform of a target do not match. This target is ignored, and the patch plan is created without this target. The other homogeneous targets are added to the plan.

> **Note:** Oracle recommends that you fix the warnings before proceeding, as they may result in an error during patch plan validation. However, if you want to proceed regardless, you can select **Ignore Warnings and Add.**

5. Navigate to the Patches & Updates page. In the Plans region, click the name of the patch plan that you want to view.

   The Create Plan wizard is displayed.

6. On the Plan Information page, do the following:

   a. In the Overview section, validate the patch plan name. You can choose to edit it if you want.

   b. *(Optional)* Enter a short description for the patch plan.

   c. *(Optional)* In the Allow Access For section, click **Add** to grant patch plan access permissions to administrators or roles for the current patch plan.

      In the Add Privileges to Administrators window, select an administrator or a role, the access permission that you want to grant, then click **Add Privilege**.

   d. Click **Next**.

7. On the Patches page, review the patches added to the patch plan.

   To add new patches to the patch plan or add additional targets to a patch that has already been added to the patch plan, click **Add Patch**. In the Edit Search dialog box, enter the patch number, then click **Search**. Select the required patch, then click **Add to This Plan**. Select the targets that you want to add to the patch, then click **Add to This Plan.**

   Click **Next**.

8. On the Deployment Options page, do the following:

   1. In the Where to Stage section, select one of the following options:

      Yes, if you want the wizard to stage the patches from Software Library to a temporary location accessible to the target host, before the patch is applied on the target. By default, the wizard stages the patches to a default location on the target host, but if you want to change the location, you can enter a location where the patch can be staged.

No, if you have already manually staged the patches to a temporary location accessible to the target host. This can even be a shared, NFS-mounted location. In this case, ensure that you download the patch you want to apply, navigate to the location (parent directory) where you want to stage the patch, create a subdirectory with the same name as the patch ZIP file, then extract the contents of the patch ZIP file in this subdirectory. In the Where to Stage section, enter the absolute path to the parent directory where you have manually staged the patches.

For example, if you downloaded patch `699099.zip,` and the stage location, which is the parent directory, is `/u01/app/oracle/em/stagepatch,` then in this parent directory, create a subdirectory titled `699099` and extract the contents of the zip file. Enter `/u01/app/oracle/em/stagepatch` as the stage path.

2. In the Credential Information section, provide the required credentials for patching. You can choose to use preferred credentials, or override the preferred credentials with different credentials.

   In Enterprise Manager Cloud Control 12*c* Release 4 (12.1.0.4), normal Oracle home credentials are not required for patching secure Management Agent targets. If the patches that you want to apply on the Management Agent targets require *root* user access to perform certain tasks, then you must provide the privileged Oracle home credentials for the Management Agent targets.

   If the Management Agent targets that you want to patch are not secure, then you must set the preferred Management Agent host credentials for all the Management Agent targets that you want to patch. To set the preferred host credentials for Management Agent targets, from the **Setup** menu, select **Security,** then select **Preferred Credentials.** Select the **Agent** target type, then click **Manage Preferred Credentials.** Set the preferred host credentials for the required Management Agent targets.

   For more information about setting preferred credentials, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

   Note: The named credentials of type *SSH Key Credentials* cannot be set as the normal host preferred credentials or the privileged host preferred credentials for Oracle home targets.

   Click **Validate Credentials** to verify the accuracy of the provided credentials.

3. In the Notification section, specify whether or not you want to enable email notifications when the patch plan is scheduled, starts, requires action, is suspended, succeeds, and fails.

   To enable email notifications, select **Receive notification emails when the patching process,** then select the required options. If a warning message, mentioning that the sender or the receiver email address is not set up, is displayed, perform the action mentioned in the warning.

4. In the Rollback section, select **Rollback patches in the plan** to roll back the patches listed in the plan, rather than deploy them.

5. In the OPatch Upgrade section, select **OPatch Upgrade** to upgrade the OPatch component before the patching operation begins.

   For the OPatch component to be upgraded, ensure that it is downloaded and unzipped to the same location where the patches that you want to apply are staged.

6. In the Conflict Check section, specify whether you want to enable or disable ARU Conflict Check, a check that uses Oracle Automated Release Updates (ARU) to search for patch conflicts within the patch plan during the analysis stage. Also, specify the action that the patching procedure must take when a patch conflict is encountered during deployment.

   For **Conflicts,** select **Stop at Conflicts** if you want the patching procedure to stop the deployment of the plan when a conflict is encountered, select **Force Apply** if you want the patching procedure to roll back the conflicting patches and apply the incoming patches when a conflict is encountered, or select **Skip conflicts** if you want the patching procedure to apply only the non-conflicting patches, and skip the application of the conflicting patches, when a conflict is encountered.

7. Click **Next**.

9. On the Validation page, click **Analyze** to validate the patch before deploying it. A validation job is submitted, which checks for patch conflicts, checks for the latest OPatch version, checks if the version and platform of the targets and the patch are the same, and so on. To track the progress of the validation job, click **Show Detailed Results.**

   Alternatively, you can navigate directly to the Review and Deploy page to deploy the Management Agent patches without analyzing the plan. If you do so, a deploy job is submitted which analyzes the plan, and deploys it on successful analysis.

   > **Important:** If any problems are encountered during the analysis phase, then the split plan feature is enabled, in which the patch plan is split into two patch plans, one having the targets for which the analysis failed, and another having the targets for which the analysis was successful. The patch plan having the targets for which the analysis was successful is available for deployment, while the other patch plan must be reanalyzed and deployed separately.
   >
   > Figure 18–5 illustrates the split plan feature.

   Upon validation, if there are conflicts between two patches, then it is recommended that you request for replacement patches. In this case, click **Request Replacement Patches**. If there is a merge patch already available for the conflicting patches, you can choose to directly replace the conflicting patches with the merge patch. To do this, click **Replace Conflicting Patches**.

   For information about the errors that may occur during the validation phase, see Section 18.2.7.

   Click **Next.**

10. On the Review & Deploy page, review the details that you have provided for the patch plan, then click **Deploy**.

    Once you click **Deploy,** a Deploy Confirmation dialog box appears, which enables you to schedule the Deploy operation. Select **Deploy.** If you want to begin the

Deploy operation immediately, select **Immediately.** If you want to schedule the Deploy operation such that it begins at a later time, select **Later,** then specify the time. Click **Submit.**

After scheduling a deploy operation, the **Deploy** button on the Review and Deploy page is renamed to **Reschedule.** If you want to reschedule the Prepare or Deploy operation, click **Reschedule,** specify the time, then click **Submit.** If you want to discard the schedule and bring the patch plan back to its last valid state, click **Stop Schedule.** Note that the deploy operation schedule is discarded if you edit a patch plan deployment option or a patch target. In this case, you must validate the patch plan again.

A deploy job is submitted. To track the progress of the job, click **Show Detailed Results.**

18.2.6 Verifying the Applied Management Agent Patches

To verify the applied Management Agent patches, perform the following steps:

1. In Cloud Control, from the **Targets** menu, select **All Targets**.
2. On the All Targets page, for the **Search Target Name** field, enter the name of the Management Agent target that you just patched, then click the search icon. Click the name of the required target.
3. On the Management Agent target home page, under the Summary section and the Configuration sub-section, click **Oracle Home and Patch Details** to view all the jobs that have run on the Oracle home target of the Management Agent.
4. Under the Patch Advisories section, select the **Patches Applied** tab to verify all the patches that have been applied successfully on the Management Agent target.

18.2.7 Management Agent Patching Errors

The following are some of the errors that you may encounter while patching Management Agent targets:

- Oracle Home Credentials Are Not Set
- Management Agent Target Is Down
- Patch Conflicts Are Detected
- User Is Not a Super User
- Patch Is Not Staged or Found

18.2.7.1 Oracle Home Credentials Are Not Set

Error Description

This error occurs when the preferred Management Agent host credentials (for patching Management Agents that are not secure), or the privileged Oracle home credentials (for patches that require *root* user access) are not set.

Workaround

If the Management Agent targets that you want to patch are not secure, set the preferred Management Agent host credentials for all these targets. To set the preferred host credentials for a Management Agent target, from the **Setup** menu, select **Security,** then select **Preferred Credentials.** Select the **Agent** target type, then click **Manage**

Preferred Credentials. Set the preferred host credentials for the Management Agent target. Analyze and deploy the patch plan.

If the patches that you want to apply (on the Management Agent targets) require *root* user access, set the privileged Oracle home credentials for the Management Agent targets. Analyze and deploy the patch plan.

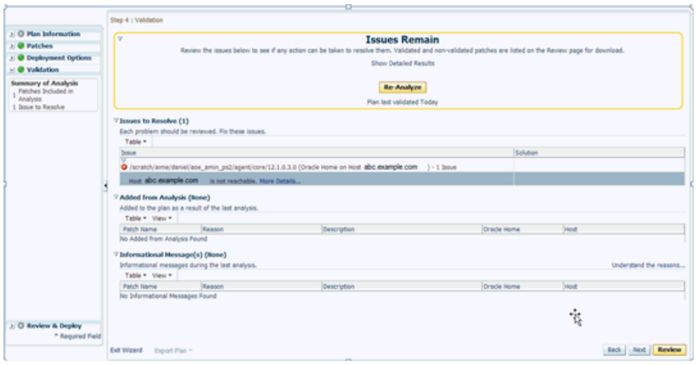
18.2.7.2 Management Agent Target Is Down

Error Description

This error occurs when the Management Agent target added for patching is not up and running.

Figure 18–2 displays an example of this error.

Figure 18–2 Patching Error: Management Agent Target Is Down



Summary of Analysis
1 Patches Included in Analysis
1 Issue to Resolve

* Required Field

Issues Remain

Review the issues below to see if any action can be taken to resolve them. Validated and non-validated patches are listed on the Review page for download.

Plan last validated Today

Issues to Resolve (1)

Each problem should be reviewed. Fix these issues.

Issue	Solution
/scratch/aime/daniel/aoe_amin_ps2/agent/core/12.1.0.3.0 (Oracle Home on Host abc.example.com) - 1 Issue	
Host abc.example.com is not reachable. More Details...	

Added from Analysis (None)

Added to the plan as a result of the last analysis.

Patch Name	Reason	Description	Oracle Home	Host
No Added from Analysis Found				

Informational Message(s) (None)

Informational messages during the last analysis.

Patch Name	Reason	Description	Oracle Home	Host
No Informational Messages Found				

Workaround

Start the Management Agent target, then analyze and deploy the patch plan.

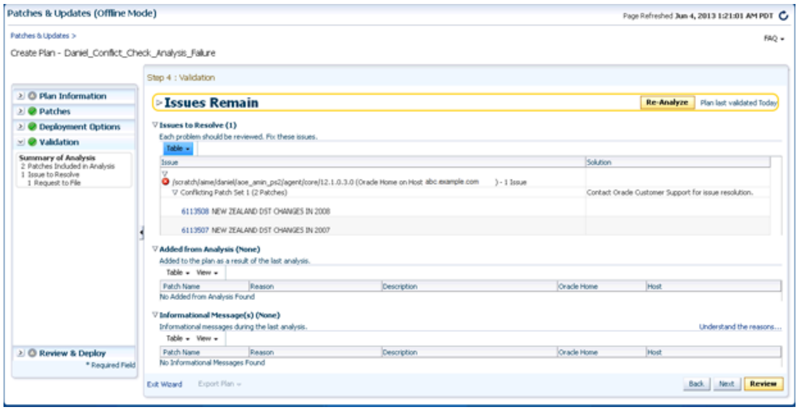
18.2.7.3 Patch Conflicts Are Detected

Error Description

This error occurs when there is a conflict between two added patches.

Figure 18–3 displays an example of this error.

Figure 18–3 Patching Error: Patch Conflicts



Patches & Updates (Offline Mode)

Page Refreshed Jun 4, 2013 1:21:01 AM PDT

Create Plan - Daniel_Conflict_Check_Analysis_Failure

Step 4 : Validation

Issues Remain

Plan last validated Today

Summary of Analysis
2 Patches Included in Analysis
1 Issue to Resolve
1 Request to File

Issues to Resolve (1)

Each problem should be reviewed. Fix these issues.

Issue	Solution
/scratch/aime/daniel/aoe_amin_ps2/agent/core/12.1.0.3.0 (Oracle Home on Host abc.example.com) - 1 Issue	
Conflicting Patch Set 1 (2 Patches)	Contact Oracle Customer Support for issue resolution.
6113508 NEW ZEALAND DST CHANGES IN 2008	
6113507 NEW ZEALAND DST CHANGES IN 2007	

Added from Analysis (None)

Added to the plan as a result of the last analysis.

Patch Name	Reason	Description	Oracle Home	Host
No Added from Analysis Found				

Informational Message(s) (None)

Informational messages during the last analysis.

Patch Name	Reason	Description	Oracle Home	Host
No Informational Messages Found				

Workaround

Do one of the following:

- Contact Support to obtain a merged patch.
- Choose the advanced OPatch options to force apply the patch. However, choosing this option and applying the patch will result in the loss of earlier patch changes.

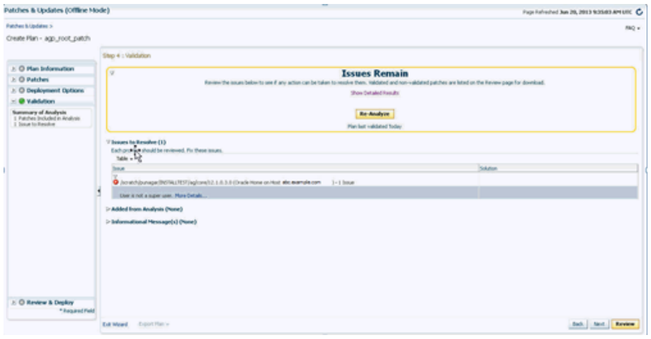
18.2.7.4 User Is Not a Super User

Error Description

This error occurs when the user that runs the patch plan does not have *root* access.

Figure 18–4 displays an example of this error.

Figure 18–4 Patching Error: User Is Not a Super User



Patches & Updates (Offline Mode)

Page Refreshed Jun 20, 2013 9:35:03 AM UTC

Create Plan - agp_root_patch

Step 4 : Validation

Issues Remain

Review the issues below to see if any action can be taken to resolve them. Validated and non-validated patches are listed on the Review page for download.

Plan last validated Today

Summary of Analysis
1 Patches Included in Analysis
1 Issue to Resolve

Issues to Resolve (1)

Each problem should be reviewed. Fix these issues.

Issue	Solution
/scratch/punagar/INSTALLTEST/ag/core/12.1.0.3.0 (Oracle Home on Host abc.example.com) - 1 Issue	
User is not a super user. More Details...	

Added from Analysis (None)

Informational Message(s) (None)

Workaround

Follow these steps:

1. Create a new credential that has *root* access.
2. Ensure that privilege delegation settings have been configured on the target Management Agent host. For more information about privilege delegation, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.
3. Analyze and deploy the patch plan.

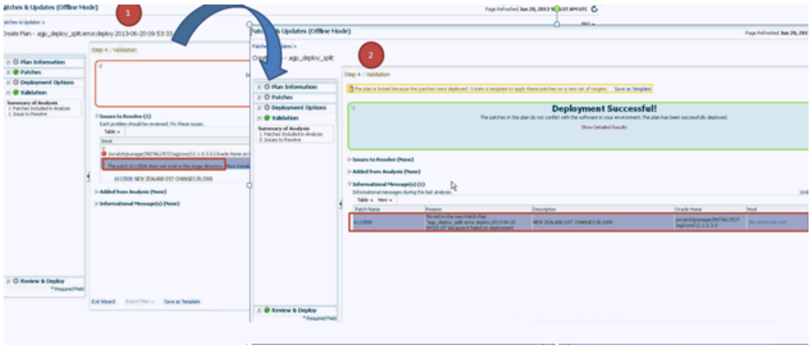
18.2.7.5 Patch Is Not Staged or Found

Error Description

This error occurs when the patch is not present in the stage location.

Figure 18–5 displays an example of this error. This figure also illustrates the split plan feature.

Figure 18–5 Patching Error: Patch Is Not Staged or Found



Workaround

Ensure that the patch is available in the stage location. Analyze and deploy the patch plan.

18.3 Manual Management Agent Patching

Manual patching is a patching mechanism that requires you to follow step-by-step instructions to patch a Management Agent manually. This mechanism of patching requires you to ensure certain prerequisites, manually validate the patch for applicability and conflicts, and can be used to patch only a single Management Agent at a time.

Note: Oracle recommends that you use the automated patching mechanism as it not only saves time and effort in mass-deploying patches, but also reduces human intervention, thereby minimizing the errors involved during the patching process.

To patch a Management Agent target manually, perform the following steps:

1. Log into My Oracle Support (`https://support.oracle.com`).

   Note: Ensure that you check the Patch Recommendation section to view the patches that are recommended for your environment.

   ---

2. On the My Oracle Support home page, click **Patches and Updates.**
3. Enter the required patch number in the Patch Search section, then click **Search.**
4. Select the patch, and from the context menu that appears, select **Download**.

5. Extract the patch zip file and follow the instructions available in `Readme.html` or `Readme.txt` to install the patch.

> **Note:** In Cloud Control, separate Management Agent patches exist for core components of Management Agents and Management Agent plug-ins. Ensure that you navigate to the correct directory location under `<installation_base_directory>` while manually patching a Management Agent core component or a Management Agent plug-in. For example, to patch a Management Agent core component manually, you must navigate to `<installation_base_directory>/core/`, and to patch a Management Agent plug-in, you must navigate to `<installation_base_directory>/plugins`. The following is the structure of the Management Agent installation base directory:

```
<installation_base_directory>
    |_____core
         |_____12.1.0.4.0
    |_____plugins
    |_____plugins.txt
    |_____plugins.txt.status
    |_____agent_inst
    |_____sbin
    |_____agentimage.properties
```

19 Personalizing Cloud Control

You can personalize the page layout and data displayed in certain Cloud Control pages, including target home pages such as the Oracle WebLogic Server target home page. The changes you make are persisted for the currently logged in user, enabling you to create customized consoles for monitoring various target types.

Personalization support provided in the current release allows you to:

- Customize the layout of regions on a page
- Add a region to, or remove a region, from a page
- Specify what data should be displayed within each region
- Set your own homepage

Note that not all pages in Cloud Control can be personalized. The page edit mode will only be enabled for those pages or page regions that can be modified.

This chapter contains the following sections:

19.1 Personalizing a Cloud Control Page

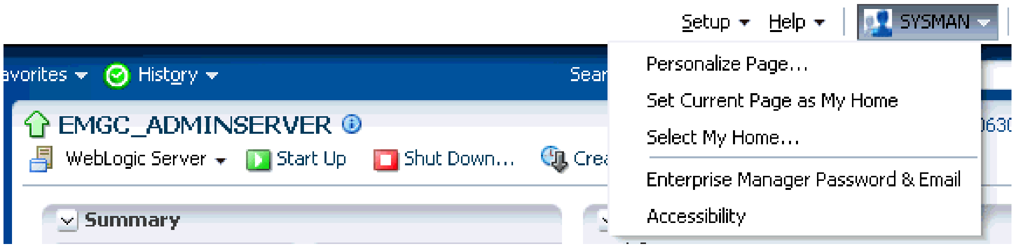
Pages in Cloud Control are laid out in a columnar format. Each column contains one or more *regions*, each of which contains data rendered as a bar chart, graph or other visual component.

You can modify the layout of columns within a page, as well as select the regions to display within each column, enabling you to personalize how the data on a page is arranged and displayed.

To personalize a page:

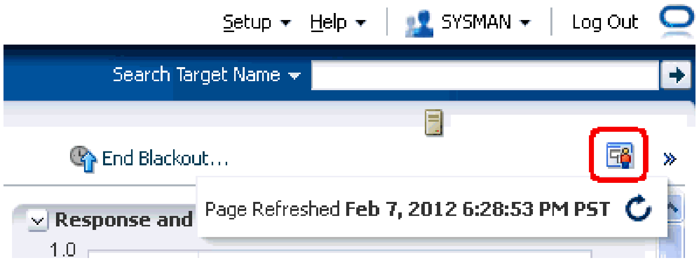
1. Navigate to the page you want to personalize.
2. Do one of the following:
   - Select **Personalize Page** from the menu item that displays the username of the currently logged-in user, just to the left of the Log Out menu item. In Figure 19–1, the menu item displays the SYSMAN user name.

Figure 19–1 Personalize Page Menu



- Or, click the "Personalize Page" icon on the right-hand side of the page, shown just above the "Page Refreshed" time stamp, as shown in Figure 19–2.

Figure 19–2 Personalize Page Icon



Note that the menu item or icon will only be enabled if the page you are currently on can be personalized.

3. You are now in page edit mode. Click the **Change Layout** button. A graphical menu of column layout options opens.
4. Select the column layout you want to use.
5. Next, add a region to each column. Click the **Add Content** button for a specific column. The Resource Catalog, which contains available components used to display data, opens.
6. Select a region, then click **Add** to add it to the column. Note that you can "stack" regions on top of one another.
7. Once a region has been added to a column, you can:
   - Customize the region. See Section 19.2, "Customizing a Region" for details.
   - Click the **View Actions** menu in the upper right corner of the region to move the region up or down within the column.
   - Drag the region from one column to another.
8. Click **Close** to save your changes.

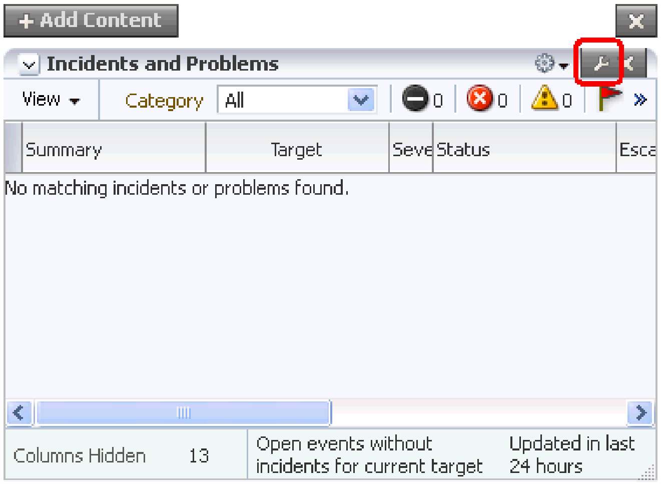
19.2 Customizing a Region

A *region* contains business data rendered as a bar chart, graph or other visual component. You can select the component to display within a specific region.

To customize a region within a page column:

1. Navigate to the page containing the region you want to customize and enable the page editing mode as described in Section 19.1, "Personalizing a Cloud Control Page".
2. Click the “ratchet” icon next to the “X” icon within a region, as shown in Figure 19–3. Note that the icon will only be enabled if the region can be customized.

Figure 19–3 Customize Region Icon



No matching incidents or problems found.

For most resources, you will specify the target host from which to collect data.

Other configurable parameters and customization options vary between regions. When you click the icon, a dialog opens to enable you to specify parameters, such as target type, target name and metric name.

3. If at a later time you want to remove the region from the page, click the “X” icon in the region.
4. Click **Close** to save your changes.

19.3 Setting Your Homepage

Cloud Control allows you to choose the page that will serve as your homepage - the first page you see after logging in to Cloud Control. You can either:

- Choose your own page, such as a target homepage that you view frequently or have customized to suit your specific needs
- Select from a pre-designed homepage templates created for specific types of Cloud Control users

Choosing Your Own Homepage

1. Navigate to the page you want to set as your homepage.
2. Select **Set Current Page As My Home** from the menu item that displays the username of the currently logged-in user, just to the left of the Log Out menu item, as shown in Figure 19–1.

Selecting a Pre-Designed Homepage

1. Select **Select My Home** from the menu item that displays the username of the currently logged-in user, just to the left of the Log Out menu item, as shown in Figure 19–1.
2. Click the **Preview** button to preview a page design template you are interested in.
3. Click the **Select As My Home** button to select a template as your homepage. Once you have selected a page, you can customize it to suit your needs.

De-selecting Your Homepage

Your homepage is saved as a "favorite" page. To de-select your current homepage:

1. From the **Favorites** menu, select **Manage Favorites**.
2. Select your homepage from the list, then click the **Remove Selected** button.
3. Click **OK** when finished.

20 Starting and Stopping Enterprise Manager Components

This chapter explains how to use the Enterprise Manager command line utility (emctl) to start and stop the Management Services, the Management Agent, and Cloud Control.

This chapter also explains the various emctl commands for Management Service and Management Agent and how to use log information to troubleshoot emctl.

Following are the sections in this chapter:

- Controlling the Oracle Management Agent
- Controlling the Oracle Management Service
- Setting Java Memory Arguments for Oracle Management Service
- Controlling JVMD and ADP Engines
- Guidelines for Starting Multiple Enterprise Manager Components on a Single Host
- Starting and Stopping Oracle Enterprise Manager 12c Cloud Control
- Additional Management Agent Commands

20.1 Controlling the Oracle Management Agent

The following sections describe how to use the Enterprise Manager command line utility (`emctl`) to control the Oracle Management Agent:

- Starting, Stopping, and Checking the Status of the Management Agent on UNIX
- Starting and Stopping the Management Agent on Windows
- Checking the Status of the Management Agent on Windows
- Troubleshooting Management Agent Startup Errors

20.1.1 Starting, Stopping, and Checking the Status of the Management Agent on UNIX

When you start the agent on UNIX systems, it starts the parent watchdog process and the child Java process for the agent. The watchdog monitors the agent Java process and attempts to start it if it fails abnormally.

To start, stop, or check the status of the Management Agent on UNIX systems:

1. Change directory to the `AGENT_INSTANCE_HOME/bin` directory.
2. Use the appropriate command described in Table 20–1.

For example, to stop the Management Agent, enter the following commands:

```
$PROMPT> cd AGENT_INSTANCE_HOME/bin
$PROMPT> emctl stop agent
```

Table 20–1 Starting, Stopping, and Checking the Status of the Management Agent

Command	Purpose
emctl start agent	Starts the Management Agent
emctl stop agent	Stops the Management Agent
emctl status agent	If the Management Agent is running, this command displays status information about the Management Agent, including the Agent Home, the process ID, and the time and date of the last successful upload to the Management Repository (Example 20–1).

Example 20–1 Checking the Status of the Management Agent

```
$ ./emctl status agent
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation. All rights reserved.
---------------------------------------------------------------
Agent Version          : 12.1.0.4.0
OMS Version            : 12.1.0.4.0
Protocol Version       : 12.1.0.1.0
Agent Home             : /scratch/agtRC2/agent_inst
Agent Log Directory    : /scratch/agtRC2/agent_inst/sysman/log
Agent Binaries         : /scratch/agtRC2/core/12.1.0.4.0
Agent Process ID       : 3104
Parent Process ID      : 3040
Agent URL              : https://linuxserver03.myco.com:3872/emd/main/
Local Agent URL in NAT : https://linuxserver03.myco.com:3872/emd/main/
Repository URL         : https://linuxserver03.myco.com:4902/empbs/upload
Started at             : 2014-03-17 13:57:24
Started by user        : aime
Operating System       : Linux version 2.6.18-308.0.0.0.1.el5xen (amd64)
LLast Reload           : (none)
Last successful upload                       : 2014-04-08 21:48:35
Last attempted upload                        : 2014-04-08 21:48:35
Total Megabytes of XML files uploaded so far : 28.79
Number of XML files pending upload           : 0
Size of XML files pending upload(MB)         : 0
Available disk space on upload filesystem    : 19.01%
Collection Status                            : Collections enabled
Heartbeat Status                             : Ok
Last attempted heartbeat to OMS              : 2014-04-08 21:50:28
Last successful heartbeat to OMS             : 2014-04-08 21:50:28
Next scheduled heartbeat to OMS              : 2014-04-08 21:51:28
---------------------------------------------------------------
Agent is Running and Ready
```

Example 20–2

```
$. /emctl status agent
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
---------------------------------------------------------------
Agent Version          : 12.1.0.4.0
OMS Version            : 12.1.0.4.0
```

```
Protocol Version       : 12.1.0.1.0
Agent Home             : /scratch/agtR05/agent_inst
Agent Log Directory    : /scratch/agtR05/agent_inst/sysman/log
Agent Binaries         : /scratch/agtR05/core/12.1.0.4.0
Agent Process ID       : 11802
Parent Process ID      : 11740
Agent URL              : https://example.com:3872/emd/main/
Local Agent URL in NAT : https://example.com:3872/emd/main/
Repository URL         : https://example.com:4901/empbs/upload
Started at             : 2014-03-06 11:10:57
Started by user        : user1
Operating System       : Linux version 2.6.18-308.0.0.0.1.el5xen (amd64)
Last Reload            : (none)
Last successful upload                       : 2014-03-10 21:56:02
Last attempted upload                        : 2014-03-10 21:56:02
Total Megabytes of XML files uploaded so far : 6.8
Number of XML files pending upload           : 0
Size of XML files pending upload(MB)         : 0
Available disk space on upload filesystem    : 25.40%
Collection Status                            : Collections enabled
Heartbeat Status                             : Ok
Last attempted heartbeat to OMS              : 2014-03-10 22:00:15
Last successful heartbeat to OMS             : 2014-03-10 22:00:15
Next scheduled heartbeat to OMS              : 2014-03-10 22:01:15

---------------------------------------------------------------
Agent is Running and Ready
```

On IBM AIX environment with a large memory configuration where the Management Agent is monitoring a large number of targets, the Agent may not start. To prevent this issue, prior to starting the Management Agent, add the following parameters to the common environment file:

```
LDR_CNTRL="MAXDATA=0x80000000"@NOKRTL
AIX_THREADSCOPE=S
```

The LDR_CNTRL variable sets the data segment size and disables loading of run time libraries in kernel space. The AIX_THREADSCOPE parameter changes AIX Threadscope context from the default Processwide 'P' to Systemwide 'S'. This causes less mutex contention.

20.1.2 Starting and Stopping the Management Agent on Windows

When you install the Oracle Management Agent on a Windows system, the installation procedure creates one new service in the Services control panel.

The procedure for accessing the Services control panel varies, depending upon the version of Microsoft Windows you are using. For example, on Windows 2000, locate the Services Control panel by selecting **Settings** and then **Administrative Tools** from the **Start** menu.

> **Note:** The `emctl` utility described in Section 20.2.1 is available in the `bin` subdirectory of the Oracle home where you installed the Management Agent; however, Oracle recommends that you use the Services control panel to start and stop the Management Agent on Windows systems.

Table 20–2 describes the Windows service that you use to control the Management Agent.

Table 20–2 Service Installed and Configured When You Install the Management Agent on Windows

Component	Service Name Format	Description

Oracle Management Agent	`Oracle<agent_home>Agent`
	For example:
	`OracleOraHome1Agent`
		Use this to start and stop the Management Agent.

20.1.3 Checking the Status of the Management Agent on Windows

To check the status of the Management Agent on Windows systems:

1. Change directory to the following location in the `AGENT_INSTANCE_HOME` directory:

   ```
   <install directory of agent>\core\12.1.0.x.0\bin
   ```

   For example, `d:\12cagent\core\12.1.0.3.0\bin`.

2. Enter the following emctl command to check status of the Management Agent:

   ```
   $PROMPT> emctl status agent
   ```

   If the Management Agent is running, this command displays status information about the Management Agent, including the Agent Home, the process ID, and the time and date of the last successful upload to the Management Repository (Example 20–1).

20.1.4 Troubleshooting Management Agent Startup Errors

If the agent fails to start, see the `emctl.log` and `emagent.nohup` log files for details. The log files are saved in the `$AGENT_INSTANCE_HOME/sysman/logs` directory. Following are common issues and troubleshooting suggestions:

20.1.4.1 Management Agent starts up but is not ready

The Management Agent goes through the following process when it starts up:

1. Starting up (the Management Agent has just received the request to start up and is going to start the initialization sequence)
2. Initializing (the Management Agent is iterating over each of its components and is initializing them)
3. Ready (All components have been initialized and the Management Agent is ready to accept requests)

The command to start the Management Agent (`emctl start agent`) has a default timeout of 120 seconds. At the end of that timeout, it will return control to the caller and will indicate what the last state of the Management Agent was when it returns control. Depending on the number of targets being monitored by the Management Agent, step 2 listed above could take a long time and it is possible that when the command exits, the state of the agent is "Initializing" and the command reports that the "agent is running but is not ready".

You can increase the timeout by setting an environment variable "EMAGENT_TIME_FOR_START_STOP". The value should indicate the number of seconds to wait before returning control to the caller.

20.1.4.2 Management Agent fails to start due to time zone mismatch between agent and OMS

The Management Agent uses the time zone set in emd.properties file. During the install process of the Management Agent, the agent and the host target are registered with the OMS along with the time zone. If the Management Agent’s time zone is modified at any point after the installation, the OMS will signal the Management Agent to shut down as soon as it detects this mismatch.

To reset the Management Agent's time zone, run the following command:

```
emctl resettz agent
```

For more information about setting the time zone for the agent, see Section 20.7.4.

20.1.4.3 Management Agent fails to start due to possible port conflict

If the Management Agent cannot start and emctl reports that there is a possible port conflict, check the Management Agent's port (based on emd.properties:EMD_URL) and see if there is another application, such as another agent, running on the machine that is already bound to the port.

To resolve this issue, stop the application currently bound to the Management Agent's port.

20.1.4.4 Management Agent fails to start due to failure of securing or unsecuring

Securing or unsecuring of the Management Agent can fail if the password to secure the agent against the OMS is incorrect or if the OMS is locked or down. You can find the reason for the failure in the `<agent state directory>/sysman/log/secure.log` file.

20.2 Controlling the Oracle Management Service

> **Note:** The user who can start or stop the OMS is the Oracle Software Owner.

When you start the Management Service, the following services are started:

1. OPMN process. This is the watchdog for the Apache process. The OPMN process starts the Apache process if it crashes.
2. Apache processes to start the HTTP server.
3. Node Manager Java process. This is the watchdog for the Managed Server and Admin Server processes. It restarts the Managed Server and Admin Server processes if they crash.
4. Admin Server Java process (if the command to start OMS is executed on the first OMS machine). This is the WebLogic Server instance that maintains configuration data for configured Enterprise Manager domain.
5. Managed Server Java process. This is the Managed WebLogic Server on which Enterprise Manager application is deployed.

6. (On Windows only) Node Manager service process. This is the Windows service for starting and stopping the Node Manager (equivalent to the Node Manager process on Linux).
7. (On Windows only) OMS service process. This is the Windows service for starting and stopping the OMS.
8. BI Publisher Server Java process, if it has been configured on the system. This is the Managed WebLogic Server on which the Oracle BI Publisher application is deployed.

The following sections describe how to control the Oracle Management Service:

- Controlling the Management Service on UNIX
- Controlling the Management Service on Windows

20.2.1 Controlling the Management Service on UNIX

To start, stop, or check the status of the Management Service with the Enterprise Manager command-line utility, follow these steps:

1. Change directory to the `ORACLE_HOME/bin` directory in the Management Service home.
2. Use the appropriate command described in Table 20–3.

   For example, to stop the Management Service, enter the following commands:

   ```
   $PROMPT> cd bin
   $PROMPT> ./emctl stop oms
   ```

Table 20–3 Starting, Stopping, and Checking the Status of the Management Service

Command	Purpose
emctl start oms	Starts the Fusion Middleware components required to run the Management Service. Specifically, this command starts HTTP Server, the Node Manager, OPMN process, and the managed server on which the Management Service is deployed. In addition, if this command is run on the host that has the Administration Server, then the Administration Server is also started. Similarly, if this command is run on a host that has Oracle BI Publisher configured, then Oracle BI Publisher is also started.
emctl stop oms	Stops the OMS managed server and HTTP server but leaves Node Manager and Administration Server running. **Note:** The `emctl stop oms` command does not stop Fusion Middleware. Use `emctl stop oms -all` to stop all processes including Administration Server, HTTP Server, Node Manager, management server, and Oracle BI Publisher (if it is configured on the host).
emctl status oms	Displays a message indicating whether or not the Management Service is running. Run `emctl status oms -details` to view information about the configuration of the management service such as ports being used and the URLs for console and upload.

Table 20–3 (Cont.) Starting, Stopping, and Checking the Status of the Management

Command	Purpose
emctl config oms -set_startup_mode [pbs_only | console_only | normal]	Configures the startup mode of the OMS. This command cannot be executed on the primary OMS. The three startup modes are as below: ■ `pbs_only`: If the startup mode is configured to `pbs_only`, then the command `emctl start oms` starts only the PBS application. ■ `console_only`: If the startup mode is configured to `console_only`, then the command `emctl start oms` starts only the console application. ■ `normal`: If the startup mode is configured to `normal`, then the command `emctl start oms` starts both the PBS application and the console application.

20.2.2 Controlling the Management Service on Windows

When you install the Oracle Management Service on a Windows system, the installation procedure creates a new service in the Services control panel.

The procedure for accessing the Services control panel varies, depending upon the version of Microsoft Windows you are using. For example, on Windows 2000, locate the Services control panel by selecting **Settings,** then **Administrative Tools** from the **Start** menu.

> **Note:** The `emctl` utility described in Section 20.2.1 is available in the `bin` subdirectory of the Oracle home where you installed the Management Service; however, Oracle recommends that you use the Services control panel to start and stop the Management Service on Windows systems.

Table 20–4 describes the Windows service that you use to control the Oracle Management Service.

Table 20–4 Service Installed and Configured When Installing the Oracle Management Service on Windows

Component	Service Name Format	Description
Oracle Management Server	`OracleManagementServer_EMGC_OMS1_1`	Use this service to start and stop all components that were installed and configured as part of the Management Service J2EE application.

20.2.3 Troubleshooting Oracle Management Service Startup Errors

Following are the log files you can check if the OMS fails to start:

Management Service Fails to Start

Check the logs located as indicated in Table 20–5. The INSTANCE_HOME mentioned in the table is the OMS instance home and n is the index of the OMS server.

Table 20–5 OMS Log Files Location

OMS Log File	Log File Location
emctl log file	$INSTANCE_HOME/sysman/log/emctl.log file
Managed Server log files	$INSTANCE_HOME/user_projects/domains/<DOMAIN_NAME>/servers/EMGC_OMS<n>/logs/EMGC_OMS<n>.log $INSTANCE_HOME/user_projects/domains/<DOMAIN_NAME>/servers/EMGC_OMS<n>/logs/EMGC_OMS<n>.out
OMS log files	$INSTANCE_HOME/sysman/log/emoms_pbs.log $INSTANCE_HOME/sysman/log/emoms_pbs.trc $INSTANCE_HOME/sysman/log/emoms.trc $INSTANCE_HOME/sysman/log/emoms.log
Node Manager log files	$INSTANCE_HOME/NodeManager/emnodemanager/nodemanager.log

WebTier Service Fails to Start

Check logs under `<WebTier Instance Home>/diagnostics` folder in case WebTier start fails.

20.3 Setting Java Memory Arguments for Oracle Management Service

If you have changed the default, out-of-box memory settings for an OMS, then before upgrading the OMS, perform the following steps to preserve the changes. Otherwise, the changes will be lost during upgrade.

1. Run the following command on all the OMS instances:

```
$<OMS_HOME>/bin/emctl set property -name 'JAVA_EM_MEM_ARGS'
-value '<java_memory_arguments>'
```

   For example,

```
$<OMS_HOME>/bin/emctl set property -name 'JAVA_EM_MEM_ARGS'
-value '-Xms256m -Xmx1740m'
```

2. Stop all the OMS instances and all the Oracle WebLogic-related services, and then start them again.

```
$<OMS_HOME>/bin/emctl stop oms -all
```

```
$<OMS_HOME>/bin/emctl start oms
```

20.4 Controlling JVMD and ADP Engines

This section contains the following:

- Controlling JVMD Engines
- Controlling ADP Engines

20.4.1 Controlling JVMD Engines

Table 20–6 lists the commands used to control JVMD Engines.

Table 20–6 Commands Used to Control JVMD Engines

Command	Purpose
emctl extended oms jvmd list	Lists all the JVMD Engines.
emctl extended oms jvmd start -server=<server_name1>,<server_name2>...	Starts specified JVMD Engines. Accepts the engine names as a comma separated list.
emctl extended oms jvmd start -all	Starts all JVMD Engines.
emctl extended oms jvmd stop -server=<server_name1>,<server_name2>...	Stops specified JVMD Engines. Accepts the engine names as a comma separated list.
emctl extended oms jvmd stop -all	Stops all JVMD Engines.
emctl extended oms jvmd status -server=<server_name1>,<server_name2>...	Displays the status of specified JVMD Engines. Accepts the engine names as a comma separated list.
emctl extended oms jvmd status -all	Displays the status of all JVMD Engines.
emctl extended oms jvmd -help	Displays the list of available commands for the JVMD verb.

20.4.2 Controlling ADP Engines

Table 20–7 lists the commands used to control ADP Engines.

Table 20–7 Commands Used to Control ADP Engines

Command	Purpose
emctl extended oms adp list	Lists all ADP Engines.
emctl extended oms adp start -server=<server_name1>,<server_name2>...	Starts specified ADP Engines. Accepts the engine names as a comma separated list.
emctl extended oms adp start -all	Starts all ADP Engines.
emctl extended oms adp stop -server=<server_name1>,<server_name2>...	Stops specified ADP Engines. Accepts the engine names as a comma separated list.
emctl extended oms adp stop -all	Stops all ADP Engines.
emctl extended oms adp status -server=<server_name1>,<server_name2>...	Displays the status of specified ADP Engines. Accepts the engine names as a comma separated list.
emctl extended oms adp status -all	Displays the status of all ADP Engines.
emctl extended oms adp -help	Displays the list of available commands for the ADP verb.

20.5 Guidelines for Starting Multiple Enterprise Manager Components on a Single Host

Oracle Enterprise Manager components are used to manage a variety of Oracle software products. In most cases, in a production environment, you will want to distribute your database and WebLogic Server instances among multiple hosts to improve performance and availability of your software resources. However, in cases where you must install multiple WebLogic Servers or databases on the same host, consider the following guidelines.

When you start Fusion Middleware Control, the Management Agent, or Database Control, Enterprise Manager immediately begins gathering important monitoring data about the host and its managed targets. Keep this in mind when you develop a process for starting the components on the host.

Specifically, consider staggering the startup process so that each Enterprise Manager process has a chance to start before the next process begins its startup procedure. Using a staggered startup procedure ensures that the processes are not in contention for resources during the CPU-intensive startup phase for each component. However, in the case of a system restart, `/etc/init.d/gcstartup` script which is registered during the EM deployment ensures that the OMS and the Management Agent are started automatically in a staggered manner.

20.6 Starting and Stopping Oracle Enterprise Manager 12c Cloud Control

As described in the previous sections, you use separate commands to control the Oracle Management Service and Management Agents.

The following sections describe how to stop and start all the Cloud Control components that are installed by the Oracle Enterprise Manager 12c Cloud Control Console installation procedure.

You can use this procedure to start all the framework components after a system reboot or to shutdown all the components before bringing the system down for system maintenance.

20.6.1 Starting Cloud Control and All Its Components

The following procedure summarizes the steps required to start all the components of the Cloud Control. For example, use this procedure if you have restarted the host computer and all the components of the Cloud Control have been installed on that host.

To start all the Cloud Control components on a host, use the following procedure:

1. If your Oracle Management Repository resides on the host, change directory to the Oracle Home for the database where you installed the Management Repository and start the database and the Net Listener for the database:

   a. Set the ORACLE_HOME environment variable to the Management Repository database home directory.

   b. Set the ORACLE_SID environment variable to the Management Repository database SID (default is asdb).

   c. Start the Net Listener:

   ```
   $PROMPT> $ORACLE_HOME/bin/lsnrctl start
   ```

   d. Start the Management Repository database instance:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> startup
SQL> quit
```

See Also: *Oracle Database Administrator's Guide* for information about starting and stopping an Oracle Database.

2. Start the Oracle Management Service:

   ```
   $PROMPT> OMS_HOME/bin/emctl start oms
   ```

   See Also: "Controlling the Oracle Management Service" on page 20-5

3. Change directory to the home directory for the Oracle Management Agent and start the Management Agent:

   ```
   $PROMPT> AGENT_HOME/bin/emctl start agent
   ```

   See Also: "Controlling the Oracle Management Agent" on page 20-1

   Note: Be sure to run the `emctl start agent` command in the Oracle Management Agent home directory and not in the Management Service home directory.

20.6.2 Stopping Cloud Control and All Its Components

The following procedure summarizes the steps required to stop all the components of the Cloud Control. For example, use this procedure if you have installed all the components of the Cloud Control on the same host you want to shut down or restart the host computer.

To stop all the Cloud Control components on a host, use the following procedure:

1. Stop the Oracle Management Service:

   ```
   $PROMPT> $ORACLE_HOME/bin/emctl stop oms -all
   ```

   See Also: "Controlling the Oracle Management Service" on page 20-5

2. Change directory to the home directory for the Oracle Management Agent and stop the Management Agent:

   ```
   $PROMPT> AGENT_HOME/bin/emctl stop agent
   ```

   See Also: "Controlling the Oracle Management Agent" on page 20-1

   Note: Be sure to run the `emctl stop agent` command in the Oracle Management Agent home directory and not in the Oracle Management Service home directory.

   ---

3. If your Oracle Management Repository resides on the same host, follow these steps:

   a. Set the ORACLE_HOME environment variable to the Management Repository database home directory.

   b. Set the ORACLE_SID environment variable to the Management Repository database SID (default is asdb).

   c. Stop the database instance:

   ```
   $PROMPT> ORACLE_HOME/bin/sqlplus /nolog
   SQL> connect SYS as SYSDBA
   SQL> shutdown
   SQL> quit
   ```

   See Also: *Oracle Database Administrator's Guide* for information about starting and stopping an Oracle Database.

   d. Stop the Net Listener:

   ```
   $PROMPT> $ORACLE_HOME/bin/lsnrctl stop
   ```

20.7 Additional Management Agent Commands

The following sections describe additional `emctl` commands you can use to control the Management Agent:

- Uploading and Reloading Data to the Management Repository
- Specifying New Target Monitoring Credentials
- Listing the Targets on a Managed Host
- Changing the Management Agent Time Zone
- Reevaluating Metric Collections

20.7.1 Uploading and Reloading Data to the Management Repository

Under normal circumstances, the Management Agent uploads information about your managed targets to the Management Service at regular intervals.

To use these commands, change directory to the `AGENT_HOME/bin` directory (UNIX) or the `AGENT_HOME\bin` directory (Windows) and enter the appropriate command as described in Table 20–8.

Table 20–8 Manually Reloading and Uploading Management Data

Command	Description
`emctl upload (agent)`	Use this command to force an immediate upload of the current management data from the managed host to the Management Service. Use this command instead of waiting until the next scheduled upload of the data.
`emctl reload` (agent)	This command can be used to apply the changes after you have manually modified the `emd.properties` file. For example, to change the upload interval, emd.properties can be modified, and `emctl reload` can then be run. **Note:** Oracle does not support manual editing of the `targets.xml` files unless the procedure is explicitly documented or you are instructed to do so by Oracle Support.

20.7.2 Specifying New Target Monitoring Credentials

To monitor the performance of your database targets, Enterprise Manager connects to your database using a database user name and password. This user name and password combination is referred to as the database monitoring credentials.

> **Note:** The instructions in this section are specific to the monitoring credentials for a database target, but you can use this procedure for any other target type that requires monitoring credentials. For example, you can use this procedure to specify new monitoring credentials for your Oracle Management Service and Management Repository.

When you first add an Oracle9i Database target, or when it is added for you during the installation of the Management Agent, Enterprise Manager uses the DBSNMP database user account and the default password for the DBSNMP account as the monitoring credentials.

When you install Oracle Database 11*g*, you specify the DBSNMP monitoring password during the database installation procedure.

As a result, if the password for the DBSNMP database user account is changed, you must modify the properties of the database target so that Enterprise Manager can continue to connect to the database and gather configuration and performance data.

Similarly, immediately after you add a new Oracle Database 11*g* target to the Cloud Control, you may need to configure the target so it recognizes the DBSNMP password that you defined during the database installation. Otherwise, the Database Home page may display no monitoring data and the status of the database may indicate that there is a metric collection error.

> **Note:** You can modify the Enterprise Manager monitoring credentials by using the Oracle Enterprise Manager 12*c* Cloud Control Console.

20.7.3 Listing the Targets on a Managed Host

There are times when you need to provide the name and type of a particular target you are managing. For example, you must know the target name and type when you are setting the monitoring credentials for a target.

To list the name and type of each target currently being monitored by a particular Management Agent:

1. Change directory to the `AGENT_HOME/bin` directory (UNIX) or the `AGENT_HOME\bin` directory (Windows).
2. Enter the following command to list new monitoring credentials:

   ```
   $PROMPT>./emctl config agent listtargets
   ```

   Example 20–3 shows the typical output of the command.

Example 20–3 Listing the Targets on a Managed Host

```
$. /emctl config agent listtargets
Oracle Enterprise Manager Cloud Control 12c Release 4
Copyright (c) 1996, 2014 Oracle Corporation.  All rights reserved.
```

```
[linuxserver03.myco.com, host]
[linuxserver03.myco.com:3872, oracle_emd]
[Management Services and Repository, oracle_emrep]
[linuxserver03.myco.com:4891_Management_Service, oracle_oms]
[linuxserver03.myco.com:4891_Management_Service_CONSOLE, oracle_oms_console]
[linuxserver03.myco.com:4891_Management_Service_PBS, oracle_oms_pbs]
[agent12c10_151_linuxserver03.myco.com, oracle_home]
[EM Management Beacon, oracle_beacon]
[/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/FMW Welcome Page
Application(11.1.0.0.0), j2ee_application]
[/EMGC_GCDomain/GCDomain/EMGC_OMS1/OCMRepeater, j2ee_application]
[/EMGC_GCDomain/GCDomain/EMGC_OMS1/emgc, j2ee_application]
[/EMGC_GCDomain/GCDomain/EMGC_OMS1/empbs, j2ee_application]
[/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/mds-owsm, metadata_repository]
[/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER/mds-sysman_mds, metadata_repository]
[/EMGC_GCDomain/instance1/ohs1, oracle_apache]
[EMGC_GCDomain, oracle_ias_farm]
[/EMGC_GCDomain/GCDomain/EMGC_ADMINSERVER, weblogic_j2eeserver]
[/EMGC_GCDomain/GCDomain/EMGC_OMS1, weblogic_j2eeserver]
[/EMGC_GCDomain/GCDomain, weblogic_domain]
[oms12c10_145_linuxserver03.myco.com, oracle_home]
[common12c10_163_linuxserver03.myco.com, oracle_home]
[WebLogicServer10_3_6_0_linuxserver03.myco.com_4348, oracle_home]
[webtier12c10_164_linuxserver03.myco.com, oracle_home]
```

20.7.4 Changing the Management Agent Time Zone

The Management Agent may fail to start after the upgrade if it realizes that it is no longer in the same time zone that it was originally configured with.

You can reset the time zone used by the Management Agent using the following command:

```
emctl resetTZ agent
```

This command will correct the Management Agent side time zone and specify an additional command to be run against the Management Repository to correct the value there.

IMPORTANT: Before you change the Management Agent time zone, first check to see if there are any blackouts that are currently running or scheduled to run on any targets managed by that Management Agent. Refer to Section 5.1.3.1 to know how to check for blackouts.

If any blackouts exist, then from the Cloud Control Console, stop all the scheduled and all the currently running blackouts on all targets monitored by that Management Agent. You can then change the Management Agent's time zone and later create new blackouts on the targets as needed.

20.7.5 Reevaluating Metric Collections

Use the following command to perform an immediate reevaluation of a metric collection:

```
emctl control agent runCollection <targetName>:<targetType> <colletionItemName>
```

where `<collectionItemName>` is the name of the Collection Item that collects the metric.

Performing this command causes the reevaluated value of the metric to be uploaded into the Management Repository, and possibly trigger alerts if the metric crosses its threshold.

Related metrics are typically collected together; collectively a set of metrics collected together is called a Metric Collection. Each Metric Collection has its own name. If you want to reevaluate a metric, you first need to determine the name of the Metric Collection to which it belongs, then the CollectionItem for that Metric Collection.

When you run the previous command to reevaluate the metric, all other metrics that are part of the same Metric Collection and Collection Item will also be reevaluated.

Perform the following steps to determine the Metric Collection name and Collection Item name for a metric:

1. Go to `$INSTALL_BASE/ngagent/plugins` directory, where $INSTALL_BASE is the root of the installation. The Oracle Home of the Management Agent exists in this directory.
2. Locate the XML file for the target type. For example, if you are interested in the host metric 'Filesystem Space Available(%)' metric, look for the host.xml file.
3. In the xml file, look for the metric in which you are interested. The metric that you are familiar with is actually the display name of the metric. The metric name would be preceded by a tag that started with:

   ```
   <Label NLSID=
   ```

   For example, in the host.xml file, the metric 'Filesystem Space Available(%)" would have an entry that looks like this:

   ```
   <Label NLSID="host_filesys_pctAvailable">Filesystem Space Available (%)
   </Label>
   ```

4. Once you have located the metric in the xml file, you will notice that its entry is part of a bigger entry that starts with:

   ```
   <Metric NAME=
   ```

   Take note of the value defined for "Metric NAME". This is the Metric Collection name. For example, for the 'Filesystem Space Available(%)' metric, the entry would look like this:

   ```
    <Metric NAME="Filesystems"
   ```

   So for the 'Filesystem Space Available(%)' metric, the Metric Collection name is 'Filesystems'.

5. The Collection Item name for this Metric Collection needs to be determined next. Go to the `$INSTALL_BASE/plugins/<plugin id` directory, where $INSTALL_BASE is the Oracle Home of the Management Agent.
6. In this directory, look for the collection file for the target type. In our example, this would be host.xml.
7. In cases where a Metric Collection is collected by itself, there would be a single Collection Item of the same name in the collection file. To determine if this is the case for your Metric Collection, look for an entry in the collection file that starts with:

   ```
   <CollectionItem NAME=
   ```

where the value assigned to the CollectionItem NAME matches the Metric NAME in step (4).

For the 'Filesystem Space Available(%)' metric, the entry in the collection file would look like:

```
<CollectionItem NAME = "Filesystems"
```

8. If you find such an entry, then the value assigned to "CollectionItem NAME" is the collection item name that you can use in the emctl command.
9. Otherwise, this means the Metric Collection is collected with other Metric Collections under a single Collection Item. To find the Collection Item for your Metric Collection, first search for your Metric Collection. It should be preceded by the tag:

   ```
   <MetricColl NAME=
   ```

   Once you have located it, look in the file above it for: `<CollectionItem NAME=`

   The value associated with the CollectionItem NAME is the name of the collection item that you should use in the emctl command.

   For example if the you want to reevaluate the host metric "Open Ports", using the previous steps, you would do the following:

   a. Go to the `$INSTALL_BASE/plugins/<plugin id` directory where $INSTALL_BASE is the Oracle Home of the Management Agent. Look for the host.xml file and in that file locate: `<Metric NAME="openPorts"`.

   b. Then go to the `$INSTALL_BASE/ngagent/plugins/default_collection` directory. Look for the host.xml file and in that file look for `<CollectionItem NAME="openPorts"`.

      Failing this, look for `<MetricColl NAME="openPorts"`.

   c. Look above this entry in the file to find the `<CollectionItem NAME=` string and find `<CollectionItem NAME="oracle_security"`.

   The CollectionItem NAME oracle_security is what you would use in the emctl command to reevaluate the Open Ports metric.

21 Enterprise Manager Command Line Utility Commands

Enterprise Manager Command Line Utility (EMCTL) is a command line utility to administer or control the core components of Enterprise Manager Cloud Control, particularly Oracle Management Service (OMS) and Oracle Management Agent (Management Agent). The utility is available by default with every Enterprise Manager installation.

This chapter explains the following:

- Executing EMCTL Commands
- EMCTL Commands:
  - EMCTL Commands for OMS
  - EMCTL Commands for Management Agent
  - EMTCL Security Commands
  - EMCTL HAConfig Commands
  - EMCTL Resync Commands
  - EMCTL Connector Command
  - EMCTL Patch Repository Commands
  - EMCTL Commands for Windows NT
  - EMCTL Partool Commands
  - EMCTL Plug-in Commands
  - Syncing with OPSS Policy Store
- Using emctl.log File to Troubleshoot

21.1 Executing EMCTL Commands

To run EMCTL commands for Oracle Management Service (OMS), navigate to the `<OMS_HOME>/bin` directory and run the desired command. To run EMCTL commands for Management Agent, navigate to the `<AGENT_HOME>/bin` directory and run the desired command.

21.2 EMCTL Commands for OMS

Table 21–1 lists the EMCTL commands for OMS.

Table 21–1 EMCTL Commands for OMS

EMCTL Command	Description
`emctl getversion oms`	Shows the version of the OMS instance.
`emctl start oms`	Starts the EM components required to run the OMS application. Specifically, this command starts the Oracle HTTP Server, Oracle Management Service, BI Publisher server and other applications associated with it.
`emctl start oms -admin_only`	Starts only the Administration Server of the domain.
`emctl start oms -bip_only`	Starts only the BI Publisher server.
`emctl stop oms -all`	Stops all EM processes including Administration Server, OMS, HTTP Server, Node Manager, Management Server, and Oracle BI Publisher (if it is configured on the host).

`emctl stop oms -all -force`
and
`emctl stop oms -force`
	Stops the OMS.
	The parameter `-force` can be used with both `emctl stop oms -all` and `emctl stop oms` commands. The `-force` option forcefully stops the relevant processes. Using this parameter is not recommended.

`emctl stop oms -bip_only [-force]`	Stops only the BI Publisher server. The parameter `-force` forcefully stops the process instead of a graceful shutdown. Using this parameter is not recommended.
`emctl status oms`	Lists the statuses of the OMS and the BI Publisher server.
`emctl status oms -bip_only`	Lists the status of only the BI Publisher server.
`emctl status oms -details [-sysman_pwd <pwd>]`	Lists the OMS details such as: ■ HTTP and HTTPS upload and console ports of the OMS and the respective URLs ■ Instance home location ■ OMS log directory ■ Software Load Balancer configuration details ■ Administration server machine and port ■ Oracle BI Publisher details The `-sysman_pwd` parameter indicates the Enterprise Manager SYSMAN password. If it is not provided on the command line, you will be prompted for it.

Table 21–1 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
`emctl set property`	Sets the values of the OMS configuration properties. By default, the command `emctl set property` will set the property value for all the OMSs. To set the property value for a specific OMS, specify an extra option `-oms_name`, which should be in the format `hostname.myco.com:17707_Management_Service`. To set the property value for the current OMS, specify `-oms_name = "local_oms."`. To set the property for a remote OMS, specify `-oms_name=<name of remote OMS>.` **Note:** From Enterprise Manager 12.1.0.2.0 onwards, you can also view and edit OMS properties from the Cloud Control console as follows: 1. From the **Setup** menu, select **Manage Cloud Control**, then select **Management Services**. 2. On the Management Services page, click **Configuration Properties**. 3. On the Configuration Properties page, you can view and edit OMS properties. **Note:** You will need OMS Configuration Property resource privilege to navigate to this page.
`emctl get property`	Displays the values of OMS configuration properties.
`emctl get property -name <property name> [-oms_name <OMS name>] [-sysman_pwd "sysman password"]`	Displays the value of the specified property. `-name` indicates the name of the property and `-oms_name` indicates the name of the OMS for which the property value is to be derived. If `-oms_name` is not mentioned, the property value for all the OMSs are displayed.
`emctl set property -name <property name> -value <property value> [-oms_name <OMS name>] [-module <emoms|logging>] [-sysman_pwd "sysman password"]`	Sets the value of the specified property. The parameters are explained below: ■ `-name`: Indicates the name of the property. ■ `-oms_name`: Indicates the OMS for which the property value has to be set. In case this option is not specified, the property value is set at a global level or for the current OMS. ■ `-module_name`: Indicates the module for the property. Specify either `logging` or `emoms`. Logging properties are used to configure Log4j whereas emoms properties are used to configure the OMS.
`emctl set property -file <absolute path of the file containing properties> [-oms_name <OMS name>] [-module <emoms|logging>] [-sysman_pwd "sysman password"]`	Sets the values of the properties in the specified file. The parameters are explained below: ■ `-file_name`: Indicates the absolute path of the .properties file containing the properties and the values. This file should contain only those properties whose values need to be set. ■ `-oms_name`: Indicates the OMS for which the property values has to be set. In case this option is not specified, the property values are set at a global level or for the current OMS. ■ `-module_name`: Indicates the module for the property. Specify either `logging` or `emoms`. Logging properties are used to configure Log4j whereas emoms properties are used to configure the OMS.

Table 21–1 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
`emctl delete property -name <property name> [-oms_name <OMS name>] [-module <emoms|logging>] [-sysman_pwd "sysman password"]`	Deletes the configured value of the specified property and sets it to the default value. `-name` indicates the name of the property and `-oms_name` indicates the name of the OMS for which the property value is to be deleted. If `-oms_name` is not mentioned, the property value is deleted at the global level or for the current OMS.
`emctl list properties`	Displays the properties of all OMSs. Use `-out_file` parameter to get a list of all the properties for all OMSs. This command enables easy comparison of configuration across two OMSs.
`emctl list properties [-oms_name <OMS name>] [-module <emoms|logging>] [-out_file <output file name>] [-sysman_pwd "sysman password"]`	Displays the values of all the customer visible OMS properties. The parameters are explained below: ■ `-oms_name`: Indicates the OMS for which the property values are to be displayed. In case this option is not specified, the property values for all the OMSs are displayed. ■ `-module_name`: Indicates the module of the properties. This option can be used as a filter to display module-specific properties. Logging properties are used to configure Log4j whereas emoms properties are used to configure the OMS. ■ -out_file: Indicates the absolute path of the output file. This is an optional parameter to save the output in a file.
`emctl config oms -list_repos_details`	Displays the OMS repository details.
`emctl config oms -store_repos_details [-repos_host <host> -repos_port <port> -repos_sid <sid> | -repos_conndesc <connect descriptor> ] -repos_user <username> [-repos_pwd <pwd>]`	Configures the OMS to use the specified database as the Management Repository. All the additional parameters mentioned in the command need to be specified.
`emctl config oms -change_repos_pwd [-old_pwd <old_pwd>] [-new_pwd <new_pwd>] [-use_sys_pwd [-sys_pwd <sys_pwd>]]`	Changes the password of root user (SYSMAN) in the repository database and in the OMS. To change the Enterprise Manager root user (SYSMAN) password: 1. Stop all the OMSs using `emctl stop oms` command. 2. Run `emctl config oms -change_repos_pwd` on one of the OMSs. 3. Restart all the OMSs using the `emctl stop oms -all` and `emctl start oms` commands.
`emctl config oms -change_view_user_pwd [-sysman_pwd <sysman_pwd>] [-user_pwd <user_pwd>] [-auto_generate]`	Configures the password used by OMS for MGMT_VIEW user that is used for report generation. To change the Enterprise Manager MGMT_VIEW user password: 1. Stop all the OMSs using `emctl stop oms` command. 2. Run `emctl config oms -change_view_user_pwd` on one of the OMSs. 3. Restart all the OMSs using the `emctl stop oms -all` and `emctl start oms` commands.

Table 21–1 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
`emctl secure oms`	Sets up the SSL configuration for OMS.
`emctl genreport oms -file_name <file_name> [-dest_dir <dest_dir>]`	Generates and saves the emcli tracing performance report. `-file_name` indicates the name of the input file containing the trace data and `-dest_dir` indicates the name of the output directory where the performance report is saved.
`emctl gen_ui_trace_report oms [-start_time <start_time in hh:mm:ss format>] [-duration <duration in hh:mm format>] [-user_name <username>] [-out_file <out_file>] [-sysman_pwd <sysman_pwd>]`	Generates the performance report for user interface (UI) access. The parameters are explained below: ■ `-user_name`: Indicates the user name for which the UI access performance report has to be generated. The default is for all users. ■ `-start_time`: Indicates the start time in hh:mm:ss format from when the report has to be generated. ■ `-duration`: Indicates the duration in hh:mm format for which report has to be generated. The default is 01:00. The maximum duration is limited to 24:00. ■ `-out_file`: Indicates the name of the output report file.
`emctl config oms -set_startup_mode [pbs_only | console_only | normal]`	Configures the startup mode of the OMS. This command cannot be executed on the primary OMS. The three startup modes are as below: ■ `pbs_only`: If the startup mode is configured to `pbs_only`, then the command `emctl start oms` starts only the PBS application. ■ `console_only`: If the startup mode is configured to `console_only`, then the command `emctl start oms` starts only the console application. ■ `normal`: If the startup mode is configured to `normal`, then the command `emctl start oms` starts both the PBS application and the console application.
`emctl config oms -get_startup_mode`	Displays the OMS startup mode of the current OMS.
`emctl config oms sso -host ssoHost -port ssoPort -sid ssoSid -pass ssoPassword -das dasURL -u user`	Configures Enterprise Manager (EM) to use Oracle SSO (OSSO) for authentication. To run this command you should have registered the EM site with the OSSO server, as you will need the generated registration file as an input for this command.
`emctl config oms -update_ds_pwd -ds_name <datasource_name> [-ds_pwd <datasource_pwd>]`	Updates a new password for the specified datasource. In the command, `-ds_name` indicates the name of the datasource, and `-ds_pwd` indicates the new password of the datasource.
`emctl config oms -store_embipws_creds [-admin_pwd <weblogic_pwd>] [-embipws_user <new_embipws_username>] [-embipws_pwd <new_embipws_pwd>]`	Changes the password, and optionally the user name used by the Enterprise Manager to access the installed BI Publisher Web Server. The `emctl` verb does not change the credentials of the user in the back end. Use the corresponding application or console to configure the back end credentials to match the credentials used in this `emctl` verb. This command is operational only if the BI Publisher is installed. It is not necessary for you to restart any OMS (i.e. EMGC_OMS####, BIP####) for this command.

Table 21–1 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
`emctl config oms -bip_shared_storage -config_volume <vol1> -cluster_volume <vol2> [-admin_pwd <adminpwd>] [-sysman_pwd <sysmanpwd>]`	Sets the shared storage for BI Publisher, in preparation of adding an OMS (which will also contain a scaled-out BI Publisher). Adding an OMS automatically adds a BI Publisher server that functions in a High Availability environment. Therefore, the BI Publisher will support both redundancy and scalability. This command is used to set up or move a shared storage location in preparation of running the BI Publisher in a High Availability (HA) environment. The parameter `-config_volume` specifies the BI Publisher repository and configuration files. The existing volume is copied to the volume specified in this parameter. The parameter `-cluster_volume` specifies the storage required for the BI Publisher scheduler to operate in a HA environment. This command is normally run only once on the system that contains the primary OMS and the primary BI Publisher.
`emctl extended oms <verb> [verb_args] [-help]`	Executes the `<verb>` registered with the EMCTL extended framework. The `verb_args` parameter specifies the verb-specific arguments. The `-help` parameter provides the verb specific help. For a list of extended verbs, run `emctl extended oms`.
`emctl register oms metadata -service <Metadata Service Id> (-file <Metadata Instance file> | -file_list <File containing list of files to register>) (-core | -pluginId <Plugin Id>) [-sysman_pwd <sysman password>]`	Registers the metadata. The `-file_list` parameter provides the path to the file containing a list of the file paths (one on each line). These file paths are relative to OMS Oracle home or Plug-in Oracle home depending on whether the `-core` parameter is passed or the `-pluginId` parameter is passed.
`emctl register oms metadata -service targetType -file <XML filename> [-core | -pluginId <Plugin Id>] [-sysman_pwd "sysman password"]` and `emctl register oms metadata -service storeTargetType -file <XML filename> [-core | -pluginId <Plugin Id>] [-sysman_pwd "sysman password"]`	Registers a target type when these two commands are executed, one after the other. The parameter `-file <XML filename>` specifies the target type `.xml` file name with the absolute path or the relative path.

Table 21–1 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
`emctl deregister oms metadata -service <Metadata Service Id> (-file <Metadata Instance file> && (-old_file <File containing previous metadata instances> | -no_old_file <in case there are no previous metadata instances>)) | -file_list <File containing list of ';' separeated new and old files to deregister>) (-core | -pluginId <Plugin Id>) [-sysman_pwd <sysman password>]`	Erases the metadata. The `-file_list` option provides the path to the file containing the list of file paths (one on each line). These file paths are relative to OMS Oracle home or Plug-in Oracle home depending on whether the `-core` parameter is passed or the `-pluginId` parameter is passed.

21.3 EMCTL Commands for Management Agent

Table 21–2 lists the EMCTL commands for Management Agents.

Table 21–2 EMCTL Commands for Management Agent

EMCTL Command	Description
`emctl start agent`	Starts the Management Agent.
`emctl stop agent`	Stops the Management Agent.
`emctl status agent`	Lists the status of Management Agent.
`emctl status agent -secure`	Lists the secure status of the Mangement Agent and the secure mode port on which the Management Agent is running. It also lists the OMS security status and the port.
`emctl status agent scheduler`	Lists all the running, ready, and scheduled collection threads.
`emctl status agent jobs`	Lists the status of the jobs that are running at present on the Management Agent.
`emctl status agent target <target name>,<target type>,<metric>`	Lists the detailed status of the specified targets such as target name, target type, and so on. You can also provide a particular metric name in the `emctl status agent` command to get the status of a particular metric of a target.
`emctl upload`	Uploads the `.xml` files that are pending to the OMS under the upload directory.
`emctl status agent mcache <target name>,<target type>,<metric>`	Lists the names of the metrics whose values are present in the metric cache.
`emctl reload agent dynamicproperties [<Target_name>:<Target_Type>]...`	Recomputes the dynamic properties of a target and displays them.
`emctl pingOMS [agent]`	Pings the OMS to check if the Management Agent is able to connect to the OMS. Management Agent will wait for the reverse ping from the OMS so that Management Agent can confirm that the `pingOMS` is successful.

Table 21–2 (Cont.) EMCTL Commands for Management Agent

EMCTL Command	Description
`emctl config agent getTZ`	Configures the current time zone as set in the environment.
`emctl config agent getSupportedTZ`	Displays the supported time zone based on the setting in the environment.
`emctl config console <fileloc> [<EM loc>]`	Configures the console based on the configuration entries mentioned in the file `<fileloc>`. The `<EM loc>` parameter is optional and can be used to operate on a different Oracle home.
`emctl config agent listtargets  [<EM loc>]`	Lists all the target names and types monitored by the Management Agent, that are present in `targets.xml` file. The `<EM loc>` parameter is optional and can be used to operate on a different Oracle home.
`emctl control agent runCollection <target_name>:<target_type> <metric_name>`	Allows you to manually run the collections for a particular metric of a target. For example, `emctl control agent runCollection myOracleHomeTargetName:oracle_home oracle_home_config`.
`emctl resetTZ agent`	Resets the time zone of the Management Agent. To change the current time zone to a different time zone, stop the Management Agent and then run this command. You can then start the Management Agent.
`emctl getversion agent`	Prints the version of the Management Agent.
`emctl dumpstate agent <component> . . .`	Generates the dumps for the Management Agent. This command allows you to analyze the memory/CPU issues of the Management Agent.
`emctl gensudoprops`	Generates the sudo properties of the Management Agent.
`emctl clearsudoprops`	Clears the sudo properties.
`emctl clearstate`	Clears the state directory contents. The files that are located in the `$ORACLE_HOME/sysman/emd/state` will be deleted if this command is run. The state files are the files which are waiting for the Management Agent to convert them into corresponding `.xml` files.
`emctl getemhome`	Prints the Management Agent home directory.
`emctl start blackout <Blackoutname> [-nodeLevel] [<Target_name>[:<Target_Type>]].... [-d <Duration>]`	Starts blackout on a target. If the parameter `<Target_name:Target_type>` is not entered, then the local node target is taken as the default. If `-nodeLevel` parameter is specified after `<Blackoutname>`,the blackout will be applied to all targets and any target list that follows will be ignored. The `<Duration>` should be specified in [days] hh:mm format.
`emctl stop blackout <Blackoutname>`	Stops the blackout that was started on a particular target. Only those blackouts that are started by the emctl tool can be stopped using emctl. This command cannot stop the blackouts that are started using the console or em cli utility.
`emctl status blackout [<Target_name>[:<Target_Type>]]....`	Provides the status of the target blackout. The status includes the type of blackout and whether it is a one-time action, or repeating, or a scheduled blackout. This command also specifies whether the blackout has started or stopped.

Table 21–2 (Cont.) EMCTL Commands for Management Agent

EMCTL Command	Description
`emctl secure agent [registration password] -emdWalletSrcUrl <url> -protocol <ssl|tls>`	Secures the Management Agent with an OMS. The registration password is essential, as you will be prompted for it if you do not provide it along with the command. The `-emdWalletSrcUrl` parameter indicates the URL of the OMS with which the agent has to be secured. The `-protocol` parameter indicates the protocol to be used to secure the Management Agent. The allowed values are `ssl` and `tls`.
`emctl unsecure agent`	Un-secures the Management Agent. This command changes the Management Agent's port to a HTTP port. After executing this command the Management Agent will be able to upload to the OMS on HTTP by connecting to OMS's HTTP upload port instead of the HTTPS upload port.
`emctl verifykey`	Verifies the communication between the OMS and Management Agent by sending `pingOMS`.
`emctl deploy agent [-s <install-password>] [-o <omshostname:consoleSrvPort>] [-S] <deploy-dir> <deploy-hostname>:<port> <source-hostname>`	Creates and deploys only the Management Agent. The parameters are explained below: ■ `[-s <password>]`: Indicates the install password for securing the Management Agent. ■ `[-S ]`: Indicates that the password will be provided in STDIN. ■ `[-o <omshostname:consoleSrvPort>]`: Indicates the OMS host name and the console servlet port. Choose the un-secured port. ■ `<deploy-dir>`: Indicates the directory to create the shared (state-only) installation port. ■ `<deploy-hostname:port>`: Indicates the host name and the port of the shared (state-only) installation. Choose an unused port. ■ `<source-hostname>`: Indicates the host name of the source install. Typically, it is the machine where the EM is installed. The host name is searched for and replaced in the `targets.xml` file with the host name provided in the argument `<deploy-hostname:port>`. ■ `<sid>`: Indicates the instance of the remote database. It is only specified when deploying the `dbconsole`.
`emctl setproperty agent`	Configures the specified property name and value in the Management Agent configuration file. The flag, `allow_new` is an optional flag that inserts a new property in the Management Agent configuration file, if it does not exist.
`emctl getproperty agent`	Gets the specified properties or a category of properties from the Management Agent configuration files. Currently, this command does not support spaces in the name. The flag, `-name` provides a list of property names separated by spaces.
`emctl clear_property agent`	Clears the value of the specified property in the Management Agent configuration file.
`emctl status agent verify`	Verifies that the Management Agent is live.

21.4 EMTCL Security Commands

This section explains the EMCTL security commands.

The topics covered in this section are:

- EMCTL Secure Commands
- Security diagnostic commands
- EMCTL EM Key Commands
- Configuring Authentication

21.4.1 EMCTL Secure Commands

Table 21–5 lists the general EMCTL security commands.

Table 21–3 EMCTL Secure Commands

EMCTL Command	Description
`emctl secure console [-sysman_pwd <pwd>] (-wallet <wallet_loc>| -self_signed) [-key_strength <strength>] [-cert_validity <validity>]`	Sets up the SSL configuration for the HTTPS console port of the OMS.
`emctl secure lock [-sysman_pwd <pwd>] [-console] [-upload]`	Locks the OMS upload and console, thereby avoiding HTTP access to the OMS. The `-console` and `-upload` parameters are optional. The `-console` parameter locks and prevents HTTP access to the EM console, in which case, the EM console can be accessed only over HTTPS. The `-upload` parameter prevents the Management Agents from uploading data to the OMS over HTTP, due to which the Management Agents can connect to the OMS only over HTTPS.
`emctl secure unlock [-sysman_pwd <pwd>] [-console] [-upload]`	Unlocks the OMS upload and console thereby allowing HTTP access to the OMS. The `-console` and `-upload` parameters are optional. The `-console` parameter unlocks the console for access over HTTP as well. The `-upload` parameter unlocks the upload activity thereby allowing the Management Agents to upload data to the OMS over HTTP as well.
`emctl secure createca [-sysman_pwd <pwd>] [-root_country <root_country>] [-root_state <root_state>] [-root_org <root_org>] [-root_unit <root_unit>] [-key_strength <strength>] [-cert_validity <validity>]`	Creates a new Certificate Authority (CA) which is used to issue certificates during subsequent securing of OMS and Management Agents.
`emctl secure setpwd [sysman password] [new registration password]`	Adds a new Management Agent registration password.
`emctl secure sync`	Verifies if the Management Repository is up.

Table 21–3 (Cont.) EMCTL Secure Commands

EMCTL Command	Description
emctl secure create_admin_creds_wallet [-admin_pwd <pwd>] [-nodemgr_pwd <pwd>]	Re-creates the Administrator Credentials wallet.
emctl secure oms [-sysman_pwd <sysman password>] [-reg_pwd <registration password>] [-host <hostname>] [-ms_hostname <Managed Server hostname>] [slb_port <SLB HTTPS upload port>] [-slb_console_port <SLB HTTPS console port>] [-no_slb] [-secure_port <OHS HTTPS upload Port>] [-upload_http_port <OHS HTTP upload port>] [-reset] [-console] [-force_newca] [-lock_upload] [-lock_console] [-unlock_upload] [-unlock_console] [-wallet <wallet_loc> -trust_certs_loc <certs_loc>] [-key_strength <strength>] [-sign_alg <md5|sha1|sha256|sha384|sha512>] [-cert_validity <validity>] [-protocol <protocol>] [-root_dc <root_dc>] [-root_country <root_country>] [-root_email <root_email>] [-root_state <root_state>] [-root_loc <root_loc>] [-root_org <root_org>] [-root_unit <root_unit>]	The `emctl secure oms` command generates a root key within the Management Repository, modifies the WebTier to enable an HTTPS channel between the OMS and Management Agents, and enables the OMS to accept requests from the Management Agents using the Enterprise Manager Framework Security.
emctl secure wls [-sysman_pwd <sysman password>] (-jks_loc <loc> -jks_pvtkey_alias <alias> | -wallet <loc> | -use_demo_cert)	The `emctl secure wls` command secures the WebLogic Server.

The parameter descriptions for the above commands are explained below.

- `-host`: Indicates the Software Load Balancer (SLB) or virtual host name.
- `-ms_hostname`: Indicates the actual host name of the machine where the OMS is running.
- `-slb_port`: Indicates the HTTPS port configured on SLB for uploads.
- `-slb_console_port`: Indicates the HTTPS port configured on SLB for console access.
- `-no_slb`: Removes the SLB configuration.
- `-secure_port` : Specifies the HTTPS upload port change on WebTier.

- `-upload_http_port`: Specifies the HTTP upload port change on WebTier.
- `-reset`: Creates new CA.
- `-force_newca`: Forces OMS to secure with the new CA, even when there are Management Agents secured with the older CA.
- `-console`: Creates a certificate for console HTTPS port as well.
- `-lock_upload`: Locks upload.
- `-lock_console`: Locks console.
- `-unlock_upload`: Unlocks upload.
- `-unlock_console`: Unlocks console.
- `-wallet`: Indicates the directory where the external wallet is located.
- `-trust_certs_loc`: Indicates the file containing all the trusted certificates.
- `-key_strength`: 512|1024|2048
- `-sign_alg`: Signature Algorithm; md5|sha1|sha256|sha384|sha512.
- `-cert_validity`: Indicates the number of days the certificate should be valid. The minimum value is 1 and the maximum value is 3650.
- `-protocol`: Indicates the SSL protocol to be used on WebTier. The valid values for `<protocol>` are the allowed values for Apache's SSL protocol directive.
- `-jks_loc`: Indicates the location of JKS containing the custom certificate for administrator and managed servers.
- `-jks_pvtkey_alias`: Indicates the JKS private key alias.
- `-jks_pwd`: Indicates the JKS key store password.
- `-jks_pvtkey_pwd`: Indicates the JKS private key password.
- `-wallet`: Indicates the location of the wallet containing the custom certificate for administrator and managed servers.
- `-use_demo_cert`: Configures the demonstration certificate for administrator and managed servers.

21.4.2 Security diagnostic commands

Table 21–4 lists the EMCTL security diagnostic commands.

Table 21–4 EMCTL Security Diagnostic Commands

EMCTRL Command	Description
`emctl secdiag openurl -url <url> [-trust_store <location of jks or base64 file>] [-ssl_protocol <protocol>] [-cipher <low|medium|high|some_ciphersuite_name>] [-proxy_host <host> -proxy_port <port>] [-proxy_realm <realm>] [-proxy_user <user> -proxy_pwd <pwd>]`	Diagnoses the connectivity issues to the specified URL. The parameter descriptions are as follows: ■ `-url`: Indicates the URL to be tested. ■ `-trust_store`: Indicates the location of the trust store. It can be a `jks` or `base64` file. If it is not specified, the connection will be blindly trusted. ■ `-ssl protocol`: Indicates the protocol to be used to make the connection. ■ `-cipher`: Indicates the cipher suites to be used. You can specify low, medium, high or a cipher suite name. ■ `-proxy_host`: Indicates the host name of the proxy server. ■ `-proxy_port`: Indicates the proxy server's port number. ■ `-proxy_realm`: Indicates the proxy server's realm. ■ `-proxy_user`: Indicates the proxy user ID. ■ `-proxy_password`: Indicates the proxy user password.
`emctl secdiag dumpcertsinrepos -repos_conndesc <connect desriptor> [-repos_pwd <pwd>]`	Displays the trust certificates stored in the specified repository.
`emctl secdiag dumpcertsinfile -file <location of jks/sso/p12/base64 file>`	Displays the trust certificates present in the specified key store, or wallet, or base64 file.

21.4.3 EMCTL EM Key Commands

Table 21–5 lists the EMCTL EM Key commands.

Table 21–5 EMCTL EM Key Commands

EMCTL Command	Description
`emctl status emkey [-sysman_pwd <pwd>]`	Displays the health or status of the `emkey`.
`emctl config emkey -copy_to_credstore [-sysman_pwd <pwd>]`	Copies the `emkey` from the Management Repository to the Credential Store.
`emctl config emkey -copy_to_repos [-sysman_pwd <pwd>]`	Copies the `emkey` from the Credential Store to the Management Repository.
`emctl config emkey -remove_from_repos [-sysman_pwd <pwd>]`	Removes the `emkey` from the Management Repository.

Table 21–5 (Cont.) EMCTL EM Key Commands

EMCTL Command	Description
`emctl config emkey -copy_to_file_from_credstore -admin_host <host> -admin_port <port> -admin_user <username> [-admin_pwd <pwd>] [-repos_pwd <pwd>] -emkey_file <emkey file>`	Copies the `emkey` from the Credential Store to the specified file.
`emctl config emkey -copy_to_file_from_repos (-repos_host <host> -repos_port <port> -repos_sid <sid> | -repos_conndesc <conn desc>) -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>`	Copies the `emkey` from the Management Repository to the specified file.
`emctl config emkey -copy_to_credstore_from_file -admin_host <host> -admin_port <port> -admin_user <username> [-admin_pwd <pwd>] [-repos_pwd <pwd>] -emkey_file <emkey file>`	Copies the `emkey` from the specified file to the credential store.
`emctl config emkey -copy_to_repos_from_file (-repos_host <host> -repos_port <port> -repos_sid <sid> | -repos_conndesc <conn desc>) -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>`	Copies the `emkey` from the specified file to the Management Repository.

21.4.4 Configuring Authentication

This section explains the EMCTL commands for configuring authentications.

The commands covered in this section are:

- Configuring OSSO Authentication
- Configuring OAM Authentication
- Configuring LDAP (OID and AD) Authentication
- Configuring Repository Authentication (Default Authentication)

The parameter descriptions for all these commands are as below:

- `-enable_auto_provisioning`: Enables automatic-provisioning in EM, wherein external LDAP users need not be provisioned manually in EM.
- `-auto_provisioning_minimum_role <min_role>`: Automatically provisions only those external users in EM who have the `min_role` granted to them in LDAP.

- `-minimum_privilege <min_priv>`: Prevents access to EM to users who do not have the `min_priv` granted to them.
- `-use_ssl`: Indicates the SSL to connect to the LDAP server.
- `-cert_file <cert>`: Indicates the LDAP server certificate to establish trust while connecting to LDAP server over SSL. Specify this option if the LDAP server has the certificate signed by a non-popular (or non-trusted) certificate authority.

> **Note:** This parameter accepts only a single certificate. Importing certificate chains is not supported. Import the certificate using `keytool` utility before running this command.

- `-trust_cacerts`: Establishes trust to the LDAP server's certificate while connecting to the LDAP server. This parameter is typically used if the certificate is signed by a well known certificate authority.
- `-keystore_pwd <passwd>`: Indicates the password for the default `DemoTrust.jks keystore` (if the default password has changed), or any custom `keystore` to which the LDAP server's certificate will be imported as a part of validation.
- `-use_anonymous_bind`: Uses anonymous bind to connect to LDAP server.

21.4.4.1 Configuring OSSO Authentication

EMCTL OSSO authentication command configures the Enterprise Manager to use the Oracle Application Server Single Sign-On to register any single sign-on user as an Enterprise Manager administrator. The EMCTL command to configure OSSO authentication is:

```
emctl config auth sso -ossoconf <conf file loc> -dasurl <DAS URL>
[-unsecure] [-sysman_pwd <pwd>] [-domain <domain>]  -ldap_host <ldap host>
-ldap_port <ldap port> -ldap_principal <ldap principal> [-ldap_credential
<ldap credential>] -user_base_dn <user base DN> -group_base_dn <group base
DN>  [-logout_url <sso logout url>] [-enable_auto_provisioning] [-auto_
provisioning_minimum_role <min_role>] [-minimum_privilege <min_priv>]
[-use_ssl] [-cert_file <cert>] [-trust_cacerts] [-use_anonymous_bind]
[-keystore_pwd <passwd>]
```

For example, `emctl config auth sso -ossoconf $T_WORK/osso.conf -dasurl "http://xxx.oracle.com:11" -sysman_pwd sysman -ldap_host xxx.oracle.com -ldap_port 111 -ldap_principal cn=orcladmin -ldap_credential ackdele1 -user_base_dn "cn=Users,dc=us,dc=oracle,dc=com" -group_base_dn "cn=Groups,dc=us,dc=oracle,dc=com" -logout_url "http://xxx.oracle.com:11/pls/orasso/orasso.wwsso_app_admin.ls_logout?p_done_url=https//xyy.oracle.com:216/em.`

21.4.4.2 Configuring OAM Authentication

Oracle Access Manager authentication is the Oracle Fusion Middleware single sign-on solution. This authentication scheme is used for data centers that have standardized on Oracle Access Manager as the central tool for authentication across all enterprise applications. The EMCTL command to configure OAM authentication is:

```
emctl config auth oam [-sysman_pwd <pwd>] -oid_host <host> -oid_port
<port> -oid_principal <principal> [-oid_credential <credential>] [-use_
anonymous_bind] -user_base_dn <dn> -group_base_dn <dn> -oam_host <host<
-oam_port <port> [-logout_url <url>] [-is_oam10g] [-user_dn <dn>] [-group_
dn <dn>] [-enable_auto_provisioning] [-auto_provisioning_minimum_role
<min_role>] [-minimum_privilege <min_priv>] [-use_ssl] [-cert_file <cert>]
[-trust_cacerts] [-keystore_pwd <passwd>]
```

For example, `emctl config auth oam -oid_host "xxx.oracle.com" -oid_port "111" -oid_principal "cn=orcladmin" -user_base_dn "cn=users,dc=us,dc=oracle,dc=com" -group_base_dn "cn=groups,dc=us,dc=oracle,dc=com" -oam_host "xxx.oracle.com" -oam_port "555" -oid_credential "eldleco1" -sysman_pwd "sysman" -logout_url http://xxx.oracle.com:23716/oam/server/logout?end_url=https://yyy.oracle.com:5416/em -enable_auto_provisioning -auto_provisioning_minimum_role “EM_DBA”.`

21.4.4.3 Configuring LDAP (OID and AD) Authentication

The EMCTL command for configuring OID authentication is as below. For AD, replace the command syntax `emctl config auth oid` below with `emctl config auth ad`. All other parameters remain the same.

OID authentication command configures the Oracle Internet Directory as the identity store for all the applications to authenticate it’s users against the OID.

Similarly, AD authentication command configures the Microsoft Active Directory as the identity store for all the applications to authenticate it’s users against the AD.

```
emctl config auth oid -ldap_host <ldap host> -ldap_port <ldap port> -ldap_
principal <ldap principal> [-ldap_credential <ldap credential>] [-sysman_
pwd <pwd>] -user_base_dn <user base DN> -group_base_dn <group base DN>
[-user_dn <dn>] [-group_dn <dn>] [-enable_auto_provisioning] [-auto_
provisioning_minimum_role <min_role>] [-minimum_privilege <min_priv>]
[-use_ssl] [-cert_file <cert>] [-trust_cacerts] [-use_anonymous_bind]
[-keystore_pwd <passwd>]
```

For example, `emctl config auth oid -ldap_host "xxx.oracle.com" -ldap_port "111" -ldap_principal "cn=orcladmin" -user_base_dn "cn=users,dc=us,dc=oracle,dc=com" -group_base_dn "cn=groups,dc=us,dc=oracle,dc=com" -ldap_credential "elecmee1" -sysman_pwd "sysman" -use_ssl -cert_file “/scratch/oidcert.txt”.`

21.4.4.4 Configuring Repository Authentication (Default Authentication)

The repository authentication command validates the user credentials against the Management Repository for authentication. The EMCTL command to configure the repository authentication is:

```
emctl config auth repos [-sysman_pwd <pwd>]
```

21.5 EMCTL HAConfig Commands

Table 21–6 lists the EMCTL HA configuration commands.

Table 21–6 EMCTL HA Configuration Commands

EMCTL Commands	Description
`emctl exportconfig oms [-sysman_pwd <sysman password>]`	Exports a snapshot of the OMS configuration to the specified directory. It is recommended to save the configuration details in a secure location and to save it every time there is a change in the configuration. These details will be required during a system recovery. The parameter descriptions are as below: ■ `-oms_only`: Specifies the OMS-only backup on Administration server host. ■ `-keep_host`: Specifies that the host name will also be a part of the backup if no SLB is defined. Use this option only if recovery will be done on a machine that responds to this host name.
`emctl importconfig oms -file <backup file> [-no_resecure] [-sysman_pwd <sysman password>] [-reg_pwd <registration password>]`	Imports the OMS configuration from the specified backup file. This command is used during a system recovery. The parameter descriptions are as below: ■ `-file <backup file>`: Indicates the backup file to import from. ■ `-no_resecure`: Specifies that the system will not re-secure OMS after the import is complete. The default is to re-secure the OMS after the import is complete.
`emctl config emrep [-sysman_pwd <sysman password>]`	Configures the OMS and repository target. This command is used to change the monitoring Agent for the target and/or the connection string used to monitor this target. The parameter descriptions are as below: ■ `-agent <new agent>`: Specifies a new destination agent for the `emrep` target ■ `-conn_desc [<jdbc connect descriptor>]`: Updates Connect Descriptor with the specified value. If the value is not specified, it is taken from the stored value in `emoms.properties`. ■ `-ignore_timeskew`: Ignores time skew on Agents.
`emctl config repos [-sysman_pwd <sysman password>]`	Configures the repository database target. This command is used to change the monitoring Agent for the target and/or the monitoring properties (host name, Oracle Home and connection string used to monitor this target). The parameter descriptions are as below: ■ `-agent <new agent>`: Specifies a new destination agent for the repository target. ■ `-host <new host>]`: Specifies a new host name for the repository target. ■ `-oh <new oracle home>`: Specifies a new Oracle home for the repository target. ■ `-conn_desc [<jdbc connect descriptor>]`: Updates Connect Descriptor with the specified value. If the value is not specified, it is taken from the stored value in `emoms.properties`. ■ `-ignore_timeskew`: Ignores time skew on Agents.

Table 21–6 (Cont.) EMCTL HA Configuration Commands

EMCTL Commands	Description
`emctl enroll oms [-as_host <host>]` -as_port <port> - as_pws <admin password> -nm_pwd <nodemanager password>	Enrolls the OMS on to the specified Administration Server host. This command is used in the process of recovering an OMS in a multi-OMS environment. The parameter descriptions are as below: ■ `-as_port <port>`: Specifies the Administration Server secure port. ■ `-as_pwd <admin password>`: Specifies the Administration Server password. ■ `-nm_pwd <nodemanager password>`: Specifies the node manager password.

21.6 EMCTL Resync Commands

Table 21–7 lists the EMCTL resync commands.

Table 21–7 EMCTL Resync Commands

EMCTL Commands	Description
`emctl resync repos (-full|-agentlist "agent names") [-name "resync name"] [-sysman_pwd "sysman password"]`	Submits a repository re-synchronization operation. When the `-full` option is specified, all agents are instructed to upload the latest state to the repository. The `-agent` parameter indicates the list of agents to re-synchronize with.
`emctl abortresync repos (-full|-agentlist "agent names") -name "resync name" [-sysman_pwd "sysman password"]`	Aborts the currently running repository re-synchronization operation. The `-full` option stops the complete repository re-synchronization, and the `-agentlist` option stops the re-synchronization of the list of agents.
`emctl statusresync repos -name "resync name"`	Lists the status of the given repository re-synchronization operation.

21.7 EMCTL Connector Command

The EMCTL command to add and register a custom template on Enterprise Manager is:

```
emctl register_template connector [-t <template.xml>] [-repos_pwd <repos
password>] [-cname <connectorName>] [-iname <internalName>] [-tname
<templateName>] [-ttype <templateType>] [-d <description>]
```

The parameter descriptions are as below:

- `-t`: Indicates the full path of the template.
- `-repos_pwd`: Indicates the Enterprise Manager root (SYSMAN) password.
- `-cname`: Indicates the connector name.
- `-iname`: Indicates the internal name of the template.
- `-tname`: Indicates the displayed template name.
- `-ttype`: Indicates the template type. The different template types are:
  - `<templateType> 1`: inbound transformation
  - `<templateType> 2`: outbound transformation

  - `<templateType> 3`: xml based outbound transformation
- `-d`: Indicates the description.

21.8 EMCTL Patch Repository Commands

Table 21–8 lists the EMCTL patch repository commands.

Table 21–8 EMCTL Patch Repository Commands

EMCTL Commands	Description
`emctl applypatch repos [-patchHome <patch home directory> -pluginHome <plugin home directory>]`	Loads the `.sql` files in the patch to the repository. This command has to be run from the patch directory and the path to the location where the patch is unzipped has to be specified.
`emctl rollbackpatch repos [-patchHome <patch home directory> -pluginHome <plugin home directory>]`	Recalls the `.sql` files from the repository to the patch directory location that is specified.

21.9 EMCTL Commands for Windows NT

The `emtcl create service` command creates a service for the OMS on Windows. Use this command to manage the Windows service for the OMS on a failover host in a Cold Failover Cluster setup. This command is applicable only on Windows NT. The syntax of the command is:

```
emctl create service [-oms_svc_name <oms_service_name> -user <username>]
[-passwd <password>]
```

The parameter descriptions are as below:

- `-oms_svc_name <servicename>`: Indicates the name of the OMS service to be created. If a name is not specified, the system uses the service names in the EM properties file.
- `-user <username>`: Indicates the OS user name to register the service with. If the user name is not specified, the system registers it as LocalSystem.
- `-passwd <password>`: OS password for the OS user specified.

The `emctl delete service` command deletes the service for the OMS on Windows. This command is applicable only on Windows NT. The command syntax is as below, where, `-oms_svc_name <servicename>` indicates the name of OMS service to be deleted.

```
emctl delete service [-oms_svc_name <oms_service_name>]
```

21.10 EMCTL Partool Commands

The `emctl partool` utility helps you:

- Export deployment procedures, and its associated components and directives as `par` files
- Import `par` files to the same instance or any other instance of Cloud Control

The different flavors of the `emctl partool` command are listed below:

- `emctl partool <deploy|view> -parFile <file> -force(optional)`

- `emctl partool <deploy|view> -parFile <file> -force(optional) -ssPasswd <password>`
- `emctl partool <deploy|view> -parDir <dir> -force(optional)`
- `emctl partool export -guid <procedure guid> -file <file> -displayName <name> -description <desc> -metadataOnly(optional)`
- `emctl partool check`
- `emctl partool help`

Table 21–9 lists the EMCTL partool command options.

Table 21–9 EMCTL Partool Command Options

EMCTL Command Option	Description
`<deploy|view|export>`	Deploys, displays, or exports the `par` files.
`repPasswd <repPasswd>`	Indicates the repository password.
`force`	Forces the `swlib` entities to be created or uploaded again. If they are already present, it creates a new revision.
`check`	Checks if the software library is configured.
`file <file>`	Indicates the `par` file.
`verbose`	Indicates the `verbose` mode.
`help`	Displays the help message.
`displayName <displayName>`	Indicates the `par` file name.
`parDir <dir>`	Indicates the directory where the `par` files are located.
`metadataOnly`	Filters for metadata-only exports.
`guid <guid>`	Indicates the procedure `guid` to export. To export multiple procedures provide the `guids` separated by comma (,).
`parFile <file>`	Indicates the path of the `par` file.
`description <description>`	Indicates the `par` file description.
`ssPasswd <secretStorePassword>`	This parameter is optional. This parameter creates an Oracle Wallet with the specified password to store the value of the secret property in the exported software library entity. The user must use the same password while importing the `par` file in to a new repository.

Note: For more information on `emctl partool` command see the topic *Using emctl partool Utility* in the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

21.11 EMCTL Plug-in Commands

The EMCTL plug-in command is used to resume a previous plug-in upgrade session that had failed. If the previous failure had occurred in a schema manager session, then the execution will be resumed from failed PL/SQL block. The command syntax is:

```
emctl resume_plugin_upgrade
```

Note: To know the status of the plug-in deployments run the command `emctl status oms -details [-sysman_pwd <pwd>]`.

21.12 Syncing with OPSS Policy Store

The EMCTL command to sync roles and users between the EM repository and the OPSS policy store is:

```
emctl sync_opss_policy_store [-force]
```

Note: If `-force` parameter is specified, it removes the OPSS application roles and role memberships that are not present in the EM.

21.13 Using emctl.log File to Troubleshoot

The `emctl.log` file is a file that captures the results of all EMCTL commands you run. For Management Agent, the log file resides in the `$AGENT_INSTANCE_HOME/sysman/log` directory of the Management Agent, and for OMS, the log file resides in the `$OMS_INSTANCE_HOME/em/EMGC_OMS<n>/sysman/log/` directory. The file is updated every time you run an EMCTL command. If your EMCTL command fails for some reason, access this log file to diagnose the issue.

For example, run the following command from the Oracle home directory of the Management Agent to check its status:

For Unix:

```
<agent_instance_home>/bin/emctl status agent
```

For Windows:

```
<agent_instance_home>\bin\emctl status agent
```

After running the command, navigate to the log directory to view the following information in the `emctl.log` file:

```
1114306 :: Wed Jun 10 02:29:36 2011::AgentLifeCycle.pm: Processing status agent
1114306 :: Wed Jun 10 02:29:36 2011::AgentStatus.pm:Processing status agent
1114306 :: Wed Jun 10 02:29:37 2011::AgentStatus.pm:emdctl status returned 3
```

Here, the first column, that is, 1114306, is the PID that was used to check the status. The second column shows the date and time when the command was run. The third column mentions the Perl script that was run for the command. The last column describes the result of the command, where it shows the progress made by the command and the exit code returned for the command. In this case, the exit code is 3, which means that the Management Agent is up and running.

Similarly, for the OMS, you can run the following command from the Oracle home directory of the Management Service to check its status:

For Unix:

```
<OMS_HOME>/bin/emctl status oms
```

For Windows:

```
<OMS_HOME>\bin\emctl status oms
```

Example 21–1 Sample Log Content for OMS

```
2013-06-23 22:50:25,686 [main] INFO  wls.OMSController main.219 - Executing emctl
command : status
2013-06-23 22:50:26,281 [main] INFO  commands.BaseCommand printMessage.404 -
statusOMS finished with result: 0
2013-06-23 22:50:35,885 [main] INFO  wls.OMSController main.219 - Executing emctl
command : status
2013-06-23 22:50:36,464 [main] INFO  commands.BaseCommand printMessage.404 -
statusOMS finished with result: 0
```

In another example, run the following command from the Oracle home directory of the Management Agent to upload data:

For Unix:

```
<Agent_Instance_Home>/bin/emctl upload agent
```

For Windows:

```
<Agent_Instance_Home>\bin\emctl upload agent
```

After running the command, navigate to the log directory to view the following information in the `emctl.log` file:

```
1286220 :: Tue Jun  9 07:13:09 2011::AgentStatus.pm:Processing upload
1286220 :: Tue Jun  9 07:13:10 2011::AgentStatus.pm:emdctl status agent returned 3
1286220 :: Tue Jun  9 07:13:41 2011::AgentStatus.pm: emdctl upload returned with
exit code 6
```

Here, the entries are similar to the entries in the first example, but the exit code returned is 6, which means the upload operation is failing for some reason.

The exit codes returned depend on the emctl command executed. In general, exit code of zero means success and any exit code other than zero means failure. For details about the cause of failure, view the error message.

22

22

Locating and Configuring Enterprise Manager Log Files

When you install the Oracle Management Agent (Management Agent) or the Oracle Management Service (OMS), Enterprise Manager automatically configures the system to save certain informational, warning, and error information to a set of log files.

Log files can help you troubleshoot potential problems with an Enterprise Manager installation. They provide detailed information about the actions performed by Enterprise Manager and whether or not any warnings or errors occurred.

This chapter not only helps you locate and review the contents of Enterprise Manager log files, but also includes instructions for configuring the log files to provide more detailed information to help in troubleshooting or to provide less detailed information to save disk space.

This chapter contains the following sections:

22.1 Managing Log Files

Many Enterprise Manager components generate log files containing messages that record errors, notifications, warnings, and traces.

Table 22–1 describes the columns in the Log Message table. For any given component, the optional column may not be populated in the message.

Table 22–1 Message Columns

Column Name	Description
Time	The date and time when the message was generated. This reflects the local time zone.
Message Type	The type of message. Possible values are: Incident Error Warning, Notification, and Trace. In addition, the value Unknown may be used when the type is not known.
Message ID	The ID that uniquely identifies the message within the component. The ID consists of a prefix that represents the component, followed by a dash, then a 5-digit number. For example: `OHS-51009`
Message	The text of the error message.
Target (Expanded)	Expanded target name.
Target	Target name
Target Type	Target type
Execution Context	The Execution Context ID (ECID), which is a global unique identifier of the execution of a particular request in which the originating component participates. You can use the ECID to correlate error messages from different components. The Relationship ID, which distinguishes the work done in one thread on one process, from work done by any other threads on this and other processes, on behalf of the same request.
Component	The component that originated the message.
Module	The identifier of the module that originated the message.
Incident ID	The identifier of the incident to which this message corresponds.
Instance	The name of the Oracle instance to which the component that originated the message belongs.
Message Group	The name of the group to which this message belongs.
Message Level	The message level, represented by an integer value that qualifies the message type. Possible values are from 1 (highest severity) through 32 (lowest severity).
Hosting Client	The identifier for the client or security group to which this message relates.
Organization	The organization ID for the originating component. The ID is `oracle` for all Oracle components.
Host	The name of the host where the message originated.
Host IP Address	The network address of the host where the message originated.
User	The name of the user whose execution context generated the message.
Process ID	The ID for the process or execution unit that generated the message.
Thread ID	The ID of the thread that generated the message.
Upstream Component	The component that the originating component is working with on the client (upstream) side.
Downstream Component	The component that the originating component is working with on the server (downstream) side.
Detail Location	A URL linking to additional information regarding the message.
Supplemental Detail	Supplemental information about the event, including more detailed information than the message text.

Table 22–1 (Cont.) Message Columns

Column Name	Description
Archive	Values are Yes or No. If the checkbox is checked, the message is collected from the archive location. Otherwise, the message is collected from the live system.
Target Log Files	Link to the log files page for this target.
Log File	Log file that this message contains.

Using Log Viewer, you can do the following:

- Viewing Log Files and Their Messages
- Searching Log Files
- Downloading Log Files

22.1.1 Viewing Log Files and Their Messages

You can use Enterprise Manager Cloud Control to view messages across log files.

In particular, when you navigate in the context of a farm or domain, then the logs that you can view and search are filtered to just those associated with that farm or domain. When you navigate to Logs by way of the Enterprise menu, you can pick and choose exactly what targets you want to view and search logs against. You could also, for example pick multiple WebLogic Server targets that span across domains/farm.

For example, to view the log files and their messages:

1. From the **Enterprise** menu, select **Monitoring**, select **Logs,** then select the target from the popup target selector.

   or

   The Logs menu is available at the individual target label and at the parent target level. For example, for WebLogic server and for other j2ee components, the logs menu can be accessed by choosing **Logs** from the **Targets** menu. The same is applicable for parent targets like domain and farm targets.

2. In the context of a farm or domain, expand **Selected Targets** and in the row for a particular component or application, click the **Target Log Files** icon.

   When you are in the context of the Enterprise menu, add targets to the Target table and click the **Target Log Files** icon.

   The Log Files page is displayed. On this page, you can see a list of log files related to the target.

3. Select a file and click **View Log File.**

   The View Log File page is displayed. On this page, you can view the list of messages and download the log file from this page.

4. To view the details of a message, select the message.

   By default, the messages are sorted by time, in ascending order. You can sort the messages by the any of the columns, such as Message Type, by clicking the column name. The Message Type is sorted by importance from highest to lowest and uses the order of Incident Error, Error, Warning, Notification, and then Trace.

5. When you are in context of one domain or one farm and looking at logs, the related messages are confined to that one domain or one farm. For example, to

view messages that are related by time or ECID, click **View Related Messages** and select **by Time** or **by ECID (Execution Context ID).**

The Related Messages page is displayed.

When trying to view log messages, you may see the following error:

Logging Configuration is missing or invalid for the targets (). Also, make sure that these targets are up and EM User has the CONFIGURE_TARGET privilege on the corresponding domains.

To ascertain which method to use to fix the problem, choose one of these three alternatives:

- The domain's Administration Server is down. To resolve the problem, start the Administration Server and try viewing log messages again.
- The Managed Server for which you are trying to view log messages is down. To resolve the problem, start the Managed Server and try viewing log messages again.
- The Enterprise Manager Cloud Control administrator who is trying to access log messages does not have the necessary target privileges to do so. In order to view log messages, the administrator must have been granted the target privilege "Configure target" for the corresponding WebLogic Domain target. Talk to your Oracle Enterprise Manager site administrator or super administrator regarding whether or not you have this privilege.

22.1.1.1 Restricting Access to the View Log Messages Menu Item and Functionality

You can restrict which administrators in Oracle Enterprise Manager Cloud Control have access to the View Log Messages menu item and its corresponding functionality. You can grant a target privilege labeled "Ability to view Fusion Middleware Logs" to administrators and/or roles. This target privilege is applicable to all Oracle Fusion Applications related and Oracle Fusion Middleware related target types. This target privilege is automatically included as part of the following other target privileges: Operator Fusion Middleware, Operator, and Full. Consequently, you can grant an administrator one of the following privileges in order for him/her to be able to view log messages for Oracle Fusion Applications related and Oracle Fusion Middleware related log files:

- Ability to view Fusion Middleware Logs target privilege
- Operator Fusion Middleware target privilege
- Operator target privilege
- Full target privilege

To grant the ability to an administrator to view the Fusion Middleware Logs target privilege, follow these steps:

1. Log in to the Oracle Enterprise Manager 12c Cloud Control console as a super administrator.
2. From the **Setup** menu, choose **Security**, then **Administrators**.
3. Select the appropriate administrator and click **Edit**.
4. Click **Next** twice to arrive on the Target Privileges page of the wizard.
5. Scroll down the page and click **Add** in the Target Privileges section of the page.
6. From the **Search and Add: Targets** popup dialog, select the appropriate targets for which the administrator should have access to view logs. Click **Select**.

7. From the Target Privileges section of the Target Privileges page of the wizard, select the targets to which you want to grant the “Ability to view Fusion Middleware Logs” target privilege and select **Grant to Selected**. Notice that the default target privilege automatically given for this target is View.
8. Select the **Ability to view Fusion Middleware Logs** target privilege and click **Continue**. Notice that the “Ability to view Fusion Middleware Logs” target privilege is also included as part of other target privileges (for example, Operator target privilege). So, depending on the responsibilities of the administrator, you may want to grant the Operator target privilege to the administrator.
9. Notice on the Target Privileges page of the wizard the appearance of the new privilege. Click **Review** and then **Finish** to conclude the operation.

22.1.2 Searching Log Files

You can search for diagnostic messages using the Log Messages page. By default, this page shows a summary of the logged issues for the last 10 minutes.

You can modify the search criteria to identify messages of relevance. You can view the search results in different modes, allowing ease of navigation through large amounts of data.

The following sections describe how to search log files:

- Searching Log Files: Basic Searches
- Searching Log Files: Advanced Searches

22.1.2.1 Searching Log Files: Basic Searches

You can search for all of the messages for all of the entities in a domain, an Oracle WebLogic Server, a component, or an application.

For example, to search for messages for a domain:

1. From the **Enterprise** menu, select **Monitoring**, select **Logs**, then select the target from the popup target selector.

   or

   From the **Targets** menu, select **Middleware**, click a farm. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

   The Log Messages page displays a Search section and a table that shows a summary of the messages for the last hour.
2. In the Search Mode secstion, you can choose to search for only **Live Logs**, only **Archive Logs**, or **Both**.
3. In the Date Range section, you can select either:
   - **Most Recent:** If you select this option, select a time, such as 3 hours. The default is 10 minutes.
   - **Time Interval:** If you select this option, select the calendar icon for **Start Date.** Select a date and time. Then, select the calendar icon for **End Date.** Select a date and time.
4. In the Message Types section, select one or more of the message types.
5. You can specify more search criteria, for example, by providing text in the Message text field, so you can search on explicit words or patterns across log files.You can specify more search criteria, as described in Searching Log Files: Advanced

Searches.

6. Click **Search.**
7. To help identify messages of relevance, in the table, for **Show,** select one of the following modes:

   - Messages - You can select an operator, such as **contains** and then enter a value to be matched.

     To see the details of a particular message, click the message. The details are displayed below the table of messages.

     To view related messages, select a message, then click **View Related Messages** and select **by Time** or **by ECID (Execution Context ID).**
   - Application ID - Groups messages related to a particular application.
   - ECID + Relationship ID - Groups messages by Execution Context (ECID) and Relationship ID (RID) which enables you to use log file entries to correlate messages from one application or across application server components. By searching related messages using the message correlation information, you can examine multiple messages and identify the component that first generated the problem.
   - Host - Groups messages associated with a particular host.
   - Host IP Address - Groups messages associated with a particular host IP address.
   - Incident ID
   - Message Type - Groups messages for each target based on the message type. It displays the total number of messages available for each message type, for example, ERROR, INCIDENT ERROR, WARNING, NOTIFICATION, TRACE, and UNKNOWN for every target.
   - Message ID - Groups messages based on the combination of Message ID, Message Type, Target, Message Level, Component, Module, and Organization.
   - Module - Groups the classes / modules that originated the message.
   - Target
   - Thread ID - Groups messages by Thread ID
   - User - Groups all messages for a particular user. For example, all the messages for user Jones will be listed before the messages for user Smith.

22.1.2.2 Searching Log Files: Advanced Searches

You can refine your search criteria using the following controls in the Log Messages page:

- **Message:** You can select an operator, such as **contains** and then enter a value to be matched.
- **Add Fields:** Click this to specify additional criteria, such as Host, which lets you narrow the search to particular hosts. Then click **Add.**

  For each field you add, select an operator, such as **contains** and then enter a value to be matched.
- **Selected Targets:** Expand this to see the targets that are participating in the search. To add targets, click **Add** and provide information in the dialog box. To remove targets, select the target and click **Remove.**

- **Search Archived Logs:** Enable this check box to access the log viewer. These are the archive log file locations for multiple targets you configured on the Configure Archive Locations page.

> **Note:** The Search Archived Logs check box is not applicable to standalone Oracle HTTP Servers.

22.1.3 Downloading Log Files

You can download the log messages to a file. You can download either the matching messages from a search or the messages in a particular log file.

To download the matching messages from a search to a file:

1. From the **Enterprise** menu, select **Monitoring**, then select **Logs**.

   or

   From the **Targets** menu, select **Middleware**, then select a domain. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

   The Log Messages page is displayed.

2. Search for particular types of messages as described in Searching Log Files: Basic Searches.

3. Select a file type by clicking **Export Messages to File** and select one of the following:

   - **As Oracle Diagnostic Log Text (.txt)**
   - **As Oracle Diagnostic Log XML (.xml)**
   - **As Comma-Separated List (.csv)**

   An Opening dialog box is displayed.

4. Select either **Open With** or **Save to Disk.** Click **OK.**

To export specific types of messages or messages with a particular Message ID to a file:

1. From the **Enterprise** menu, select **Monitoring**, then select **Logs**.

   or

   From the **Targets** menu, select **Middleware**, then select a domain. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

   The Log Messages page is displayed.

2. Search for particular types of messages as described in Searching Log Files: Basic Searches.

3. For **Show,** select **Group by Message Type** or **Group by Message ID.**

4. To download the messages into a file, if you selected Group by Message Type, select the link in one of the columns that lists the number of messages, such as the Errors column. If you selected Group by Message ID, select one of the links in the Occurrences column.

   The Messages by Message Type page or Message by Message ID is displayed.

5. Select a file type by clicking the arrow near **Export Messages to File.**

   You can select one of the following:

- **As Oracle Diagnostic Log Text (.txt)**
- **As Oracle Diagnostic Log XML (.xml)**
- **As Comma-Separated List (.csv)**

An Opening dialog box is displayed.

6. Select either **Open With** or **Save to Disk.** Click **OK.**

To download the log files for a specific component:

1. From the **Enterprise** menu, select **Monitoring**, then select **Logs**.

   or

   From the **Targets** menu, select **Middleware**, click a domain. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

   The Log Messages page is displayed.

2. Expand the Selected Targets section because it is hidden by default. Click **Target Log Files.**

   The Log Files page is displayed.

   Select one of the possibly many Target Log Files icons. Select the icon that is associated with the target type log files you want to view.

3. Select a log file and click **Download.**
4. An Opening dialog box is displayed.
5. Select either **Open With** or **Save to Disk.** Click **OK.**

22.2 Managing Saved Searches

The following sections provide information on creating, retrieving, and managing saved searches:

- Saving Searches
- Retrieving Saved Searches
- Managing Saved Searches

22.2.1 Saving Searches

Saved searches save administrators time by not having to redefine the same search again in the future. Saved searches help you in diagnosing problems faster because you are only a few clicks away from accessing a saved search as opposed to redefining the search again and again.

Note: Saved searches are per administrator. Therefore when the administrator logs out of the console, the search is stored and is available the next time the administrator logs in. In other words, saved searches that one administrator defines are not accessible by another administrator.

Once you have specified search criteria as described in Searching Log Files, you save it by clicking **Save Search** located at the top-right of the page. The name of the search is automatically created by concatenating fields used in the search, for example, Log Messages - Saved Search: "error", Last 1 hours, Incident Error,Error,Unknown.

Note: You can change the default name using the Manage Saved Search popup. This allows you to accept the default name and change it later.

22.2.2 Retrieving Saved Searches

To retrieve a saved search. follow these steps:

1. From the **Enterprise** menu, select **Monitoring**, select **Logs**., then select the target from the popup target selector.

   or

   From the **Targets** menu, select **Middleware**, click a farm. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

   or

   Access the saved search from the **Favorites** menu.

   The Log Messages page appears.

2. On the Logs page, click **Saved Searches** located at the top-right of the page.
3. Choose a search.

   The search results populate the Search region.

22.2.3 Managing Saved Searches

To manage a saved search, follow these steps:

1. From the **Enterprise** menu, select **Monitoring**, select **Logs**, then select the target from the popup target selector.

   or

   From the **Targets** menu, select **Middleware**, click a farm. From the **Farm** menu, select **Logs**, then select **View Log Messages**. You can manage the saved searches pertaining to the target context only.

   or

   Access the saved search from the **Favorites** menu and select **Manage Favorites**. You can manage all the log-saved searches which you have created irrespective of the context. You can see all the saved searches.

   The Log Messages page appears.

2. On the Logs page, click **Saved Searches** located at the top-right of the page.
3. On the list, click **Manage Saved Searches**.

   The Manage Favorites pop-up appears. You can:

   - Change the name of the search.

     When you select a row from the table, the name of search appears in the Name field at the bottom of the screen. You can edit the name of the search and click **OK** or you can click **Cancel**.

     Note: When you click **OK**, you will only be changing the name of the search, not the saved search criteria. Once the search criteria is changed, the Save Searches button is enabled.

   - Edit the search criteria.

     Click the link of the saved search. The Log Viewer screen appears in the context of the saved search. Make the changes and click **Save**.

   - Delete a search

Choose a search and click **Remove Selected**.

22.3 Locating Management Agent Log and Trace Files

The following sections provide information on the log and trace files for the Oracle Management Agent:

- About the Management Agent Log and Trace Files
- Locating the Management Agent Log and Trace Files

22.3.1 About the Management Agent Log and Trace Files

Oracle Management Agent log and trace files store important information that support personnel can later use to troubleshoot problems. The agent main log is located in `$EMSTATE/sysman/log`. The log is segmented by default to 11 segments, 5MB each. The segments are named gcagent.log and gcagent.log.# where # is a number in the range of 1-10. These settings are controlled by properties in emd.properties as explained in the following sections. The latest segment is always gcagent.log and the oldest is the gcagent.log.X where X is the highest number.

The Management Agent uses the following log files:

- Oracle Management Agent metadata log file (`gcagent.log`)

  This log file contains trace, debug, information, error, or warning messages from the agent.

- Oracle Management Agent fetchlet trace file (`gcagent_sdk.trc`)

  This log file contains logging information about fetchlets and receivelets.

- Oracle Management Agent errors log file (`gcagent_errors.log`)

  This error log file contains information about errors. The errors in this file are duplicate of the errors in `gcagent.log`.

- Oracle Management Agent metadata log file (`gcagent_mdu.log`)

  This log tracks the metadata updates to the agent.

- Enterprise Manager Control log file (`emctl.log`)

  The information is saved to `emctl.log` file, when you run the Enterprise Manager Control commands. For more information about `emctl.log` file, see chapter *Starting and Stopping Enterprise Manager Components*.

> **Note:** All the agent logs mentioned above (existing in $EMSTATE/sysman/log) are transient. Agent logs are segmented and have a limited overall size and hence need not be deleted or managed.

22.3.1.1 Structure of Agent Log Files

The log contain individual log messages with the following format:

```
YYYY-MM-DD HH:MM:SS,### [<tid>:<thread code or code:name>] <level> -<the message>
```

Where:

- YYYY-MM-DD HH:MM:SS,### is a timestamp (in 24 hours format and ### is the fraction in msec).
- <tid> is the thread id (as a decimal number)

- <thread name or code> is the thread full name or an abbreviated hexadecimal code (see the following example).
- <level> is the logging level that can be one of (in ascending order of importance): DEBUG, INFO, WARN, ERROR, FATAL.
- <the message> is the free text message that is being logged. The message can contain new lines and spawn multiple lines.

For example:

```
2011-06-07 15:00:00,016 [1:3305B9:main] DEBUG - ADR_BASE='/ade/example_
user/oracle/example/agentStateDir'
2011-06-07 15:00:01,883 [1:3305B9] INFO - Agent is starting up
```

22.3.2 Locating the Management Agent Log and Trace Files

The log and trace files for the Management Agent are written in the agent runtime directory. You can find the runtime directory by using this command:

```
$ emctl getemhome
```

The log and trace files will be located at `<EMHOME>/sysman/log`.

22.3.3 Setting Oracle Management Agent Log Levels

Every log message is logged using a specific log level. The log levels are ordered in priority order: DEBUG, INFO, WARN, ERROR, and FATAL. The log setting determines the minimum level that will be included in the log. For example, if the log level is set to INFO (the default), only log messages of level INFO and above (INFO, WARN, ERROR and FATAL) are going to be included in the log.

The logging configuration syntax uses the concept of handlers (appendares in log4j terms) and loggers. A handler defines a single output file and how the file is to be managed (maximum file size, number of segments, and so on). Note that there is a default logging prefix oracle.sysman that is used for all handlers that does not specify any logging prefix. The logging properties uses the `Logger.` prefix for agent (log4j) logging configuration and `ODLLogger.` prefix for the ODL (which is based on java.util.logger.*) logging configuration. Beside the prefix, both systems share the same syntax. The configuration full syntax (without a Logger or ODLLogger prefix) is the following:

Table 22–2

Property Name	Description	Mandatory	Default Value
directory=<directory>	Defines the logging system (log4j or ODL) logging directory. Specifing a directoryfor one system does not affect the other system (setting `Logger.` directory will only affect the `Logger.` configuration but not `ODLLogger.`)	No	$EMSTATE/sysman/log
<handler>.filename=<file name>	The filename to use for the handler. If the filename is relative it will be relative to the logging directory (see direrctory property above). An absolute file name will be used as is.	Yes	

Table 22–2 (Cont.)

Property Name	Description	Mandatory	Default Value
<handler>.level=<level>	The default logging level for the handler. Possbile levels are: DEBUG, INFO, WARN, ERROR, FATAL	Yes	
<handler>.totalSize=<size>	The total size in MB for all the handler file segments.	No	No limit
<handler>.segment.count=<count>	The number of segments to use for the handler.	No	1
<handler>.logger=<logger names>	A comma delimited list of logger names that will use this handler.	No	When not specified, the default logger is used.
level.<logger name>=<level>	Set a specific logging level to the logger and all its descendants. Possbile levels are: DEBUG, INFO, WARN, ERROR, FATAL	No	
additivity.<logger name>=<true or false>	If set to false, only handlers that are configured for the specific logger name will be used. Otherwise, handlers that are configured for the logger parent name will also be used.	No	true

An example of the syntax is as follows:

```
# logging properties
Logger.log.filename=gcagent.log
Logger.log.level=INFO
Logger.log.totalSize=100
Logger.log.segment.count=20

ODLLogger.wsm.level=ERROR
ODLLogger.wsm.totalSize=5
ODLLogger.wsm.segment.count=5
ODLLogger.wsm.filename=gcagent_wsm.log
```

The above log configuration sets up a handler (log) that creates a gcagent.log file (in the default logging directory) with a default logging level of INFO, total size of 100MB, uses up to 20 segments, and is configured to be used by the default logger (oracle.sysman).

22.3.3.1 Modifying the Default Logging Level

To enable DEBUG level logging for the Management Agent, set the log handler level to DEBUG (see below). And then reload the agent.

```
Logger.log.level=DEBUG
```

Alternatively, use emctl setproperty agent command as follows:

```
$ emctl setproperty agent -name "Logger.log.level" -value DEBUG
```

or

```
$ emctl setproperty agent -name "Logger.log.level" -value "DEBUG"
```

22.3.3.2 Setting gcagent.log

The gcagent.log is the agent main log that contain log entries from all the agent core code. The following is gcagent.log configuration:

```
Logger.log.filename=gcagent.log
Logger.log.level=DEBUG
Logger.log.totalSize=100
Logger.log.segment.count=20
```

22.3.3.3 Setting gcagent_error.log

The gcagent_errors.log is a subset of the gcagent.log and contains log messages of ERROR and FATAL levels. The logging configuration for gcagent_errors.log is specified in `emd.properties`. Following are the settings for gcagent_errors.log:

```
Logger.err.filename=gcagent_errors.log
Logger.err.level=ERROR
Logger.err.totalSize=100
Logger.err.segment.count=5
```

22.3.3.4 Setting the Log Level for Individual Classes and Packages

The logging level for individual class and/or packages can also be set. The following are examples that are currently configured by default:

```
# Set the class loaders to level INFO
Logger.level.oracle.sysman.gcagent.metadata.impl.ChainedClassLoader=INFO
Logger.level.oracle.sysman.gcagent.metadata.impl.ReverseDelegationClassLoader=INFO
Logger.level.oracle.sysman.gcagent.metadata.impl.PluginLibraryClassLoader=INFO
Logger.level.oracle.sysman.gcagent.metadata.impl.PluginClassLoader=INFO
```

The above configuration changed the default level of logging for the four classes to be INFO. When the default level of logging is INFO it does not make any difference but if the default log level is set to DEBUG (when debugging the code) it will prevent those four classes from logging at DEBUG level (as they are normally too verbose).

The reverse is also true, for example if the following configuration is added (not set by default):

```
Logger.level.oracle.sysman.gcagent.metadata.impl.collection=DEBUG
```

It will cause all classes in the oracle.sysman.gcagent.metadata.impl.collection package to log at DEBUG level even if the default log level is INFO.

22.3.3.5 Setting gcagent_mdu.log

A set of entries are created in the gcagent_mdu.log file for each client command that modifies target instances, target instance collections, or blackouts. Entries are as follows:

```
2011-08-18 22:56:40,467 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SAVE
TARGET(S)
<Target IDENTIFIER="TARGET_GUID=6A3A159D0BB320C50B7926E0671A1A98"
STATUS="MONITORED" TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="EM Management
Beacon" NAME="EM Management Beacon" TYPE="oracle_beacon"/>
<Target IDENTIFIER="TARGET_GUID=51F9BBC6F5B833058F4278B51E496000"
STATUS="MONITORED" TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="mytestBeacon"
NAME="mytestBeacon" TYPE="oracle_beacon"><Property VALUE="***"
NAME="proxyHost"/><Property VALUE="***" NAME="proxyPort"/><Property VALUE="***"
NAME="dontProxyFor"/></Target>
<Target IDENTIFIER="TARGET_GUID=7C4336B536C9F241DBCAC4D1D082AD22"
```

```
STATUS="MONITORED" TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="CSAcollector"
NAME="CSAcollector" TYPE="oracle_csa_collector"><Property VALUE="***"
NAME="recvFileDir"/></Target>
<Target IDENTIFIER="TARGET_GUID=207B57A3FE300C86F81FE7D409F5DD1C"
STATUS="MONITORED" TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="Oemrep_Database"
NAME="Oemrep_Database" TYPE="oracle_database"><Property VALUE="***"
NAME="MachineName"/><Property VALUE="***" NAME="Port"/><Property VALUE="***"
NAME="SID"/><Property VALUE="***" NAME="OracleHome"/><Property ENCRYPTED="FALSE"
VALUE="***" NAME="UserName"/><Property ENCRYPTED="FALSE" VALUE="***"
NAME="Role"/><Property ENCRYPTED="FALSE" VALUE="***" NAME="password"/></Target>
<Target IDENTIFIER="TARGET_GUID=0C48C5AE0FAFB42ED91F897FF398FC84"
STATUS="MONITORED" TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="Management Services
and Repository" NAME="Management Services and Repository" TYPE="oracle_
emrep"><Property VALUE="***" NAME="ConnectDescriptor"/><Property ENCRYPTED="FALSE"
VALUE="***" NAME="UserName"/><Property ENCRYPTED="FALSE" VALUE="***"
NAME="password"/><AssocTargetInstance ASSOC_TARGET_TYPE="oracle_oms" ASSOC_TARGET_
NAME="linuxserver07.myco.com:41034_Management_Service" ASSOCIATION_NAME="app_
composite_contains"/><AssocTargetInstance ASSOC_TARGET_TYPE="oracle_oms" ASSOC_
TARGET_NAME="linuxserver07.myco.com:41034_Management_Service" ASSOCIATION_
NAME="internal_contains"/><CompositeMembership><Member ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE" TYPE="oracle_oms_
console"/><Member ASSOCIATION="" NAME="linuxserver07.myco.com:41034_Management_
Service_PBS" TYPE="oracle_oms_pbs"/><Member ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service" TYPE="oracle_
oms"/></CompositeMembership></Target>
<Target IDENTIFIER="TARGET_GUID=DF64B4A7C0F2EEBA7894EA3AD4CAF61E"
STATUS="MONITORED" TIMEZONE_REGION="" ON_HOST="" DISPLAY_
NAME="linuxserver07.myco.com:41034_Management_Service"
NAME="linuxserver07.myco.com:41034_Management_Service" TYPE="oracle_oms"><Property
VALUE="***" NAME="InstanceHome"/><Property VALUE="***"
NAME="OracleHome"/><AssocTargetInstance ASSOC_TARGET_TYPE="oracle_oms_console"
ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE"
ASSOCIATION_NAME="app_composite_contains"/><AssocTargetInstance ASSOC_TARGET_
TYPE="oracle_oms_pbs" ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_
Service_PBS" ASSOCIATION_NAME="app_composite_contains"/><AssocTargetInstance
ASSOC_TARGET_TYPE="oracle_oms_console" ASSOC_TARGET_
NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE" ASSOCIATION_
NAME="internal_contains"/><AssocTargetInstance ASSOC_TARGET_TYPE="oracle_oms_pbs"
ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_Service_PBS"
ASSOCIATION_NAME="internal_contains"/><CompositeMembership><MemberOf
ASSOCIATION="" NAME="Management Services and Repository" TYPE="oracle_
emrep"/><Member ASSOCIATION="" NAME="linuxserver07.myco.com:41034_Management_
Service_CONSOLE" TYPE="oracle_oms_console"/><Member ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service_PBS" TYPE="oracle_oms_
pbs"/></CompositeMembership></Target>
<Target IDENTIFIER="TARGET_GUID=4D290260F13596502EFD8F3E22752404"
STATUS="MONITORED" TIMEZONE_REGION="" ON_HOST="" DISPLAY_
NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE"
NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE" TYPE="oracle_oms_
console"><Property VALUE="***" NAME="InstanceHome"/><Property VALUE="***"
NAME="OracleHome"/><CompositeMembership><MemberOf ASSOCIATION="" NAME="Management
Services and Repository" TYPE="oracle_emrep"/><MemberOf ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service" TYPE="oracle_
oms"/></CompositeMembership></Target>
<Target IDENTIFIER="TARGET_GUID=D0A23AE06A9E678221B075A216364541"
STATUS="MONITORED" TIMEZONE_REGION="" ON_HOST="" DISPLAY_
NAME="linuxserver07.myco.com:41034_Management_Service_PBS"
NAME="linuxserver07.myco.com:41034_Management_Service_PBS" TYPE="oracle_oms_
pbs"><Property VALUE="***" NAME="InstanceHome"/><Property VALUE="***"
NAME="OracleHome"/><CompositeMembership><MemberOf ASSOCIATION="" NAME="Management
```

```
Services and Repository" TYPE="oracle_emrep"/><MemberOf ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service" TYPE="oracle_
oms"/></CompositeMembership></Target>
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] -
SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] -
SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] -
SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] -
SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] -
SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] -
SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] -
SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] -
SUCCESS
```

For the batch of saved targets in the above example, the original request came in at 22:56:40 and the list of targets saved are found in the line(s) following the SAVE TARGET(S) message. In this case, there were 8 targets. The result of saving the targets is available in the next 8 lines (for the same thread) and in this case all were saved successfully by 22:57:10.

The pattern is the same for saved collection items (or collections) and blackouts.

The logging configuration for the gcagent_mdu log is specified in `emd.properties` but you must not modify this log. For example, these entries are logged at INFO level, which means that if you decided to save space and change this to WARN only by editing the mdu log entries in the `emd.properties` file, you will have effectively disabled this log.

Following are the settings for gcagent_mdu log:

```
Logger.mdu.filename=gcagent_mdu.log
Logger.mdu.level=INFO
Logger.mdu.totalSize=100
Logger.mdu.segment.count=5
Logger.mdu.logger=Mdu
```

Note: Change the filename and logger settings only if asked by Support.

22.3.3.6 Setting the TRACE Level

The following `_enableTrace` property when set to "true" will enable the TRACE logging level that shows as DEBUG messages.

```
Logger._enableTrace=true
```

The default log level for the agent log must be set to DEBUG for the tracing level to work.

22.4 Locating and Configuring Oracle Management Service Log and Trace Files

The following sections describe how to locate and configure the OMS log files:

- About the Oracle Management Service Log and Trace Files
- Locating Oracle Management Service Log and Trace Files
- Controlling the Size and Number of Oracle Management Service Log and Trace Files
- Controlling the Contents of the Oracle Management Service Trace File
- Controlling the Oracle WebLogic Server and Oracle HTTP Server Log Files

22.4.1 About the Oracle Management Service Log and Trace Files

OMS log and trace files store important information that Oracle Support can later use to troubleshoot problems. OMS uses the following six types of log files:

- Oracle Management Service log file (`emoms.log`)

  The Management Service saves information to the log file when it performs an action (such a starting or stopping) or when it generates an error. This is a log file for console application.

- Oracle Management Service trace file (`emoms.trc`)

  OMS trace file provides an advanced method of troubleshooting that can provide support personnel with even more information about what actions the OMS was performing when a particular problem occurred. This is a trace file for Console application.

- Oracle Management Service log file (`emoms_pbs.log`)

  The Management Service saves information to this log file for background modules such as the loader, job system, event system, notification system, and so on. This file contains messages logged at ERROR or WARN levels.

- Oracle Management Service trace file (`emoms_pbs.trc`)

  This trace file provides additional logging for the background modules such as the loader, job system, event system, notification system, and so on when DEBUG or INFO level logging is enabled for these modules. This file can provide Support personnel with even more information about actions these modules were performing when a particular problem occurred.

- Enterprise Manager Control log file (`emctl.log`)

  The information is saved to `emctl.log` file, when you run the Enterprise Manager Control commands. For more information about emctl.log file, see chapter *Starting and Stopping Enterprise Manager Components*.

- Enterprise Manager Control message file `(emctl.msg)`

  This file is created by the HealthMonitor thread of the OMS when it restarts the OMS because of a critical error. This file is used for troubleshooting the OMS restart problem. It provides information such as the exact time when the OMS is restarted and which module has caused the crash.

22.4.2 Locating Oracle Management Service Log and Trace Files

The OMS Instance Base directory is `gc_inst` in the Oracle Middleware Home (middleware home). This directory stores all log and trace files related to OMS 12c.

You can choose to change this, if you want, in the installer.

For example, if the Middleware home is `/u01/app/Oracle/Middleware/`, then the instance base location is `/u01/app/Oracle/gc_inst`. You can choose to change this, if you want, in the installer. However, you can change it for only advanced installation and not for simple installation.

22.4.3 Controlling the Size and Number of Oracle Management Service Log and Trace Files

OMS log and trace files increases in size over time as information is written to the files. However, the files are designed to reach a maximum size. When the files reach the predefined maximum size, the OMS renames (or rolls) the logging information to a new file name and starts a new log or trace file. This process keeps the log and trace files from growing too large.

As a result, you will often see multiple log and trace files in the OMS log directory. The following example shows one archived log file and the current log file in the `/u01/app/Oracle/gc_inst/em/EMGC_OMS1/sysman/log/` directory:

```
emoms.log
emoms.log.1
```

To control the maximum size of the OMS log and OMS trace files, as well as the number of rollover files, run the following command, and specify details as described in Table 22–3:

```
emctl set property -name <property> -value <property value> -module logging
```

The above command will set the property for all OMSes. If you want to set it for a single OMS, then specify an extra option `-oms_name` as follows:

```
emctl set property -name <name> -value  <value> -module logging -oms_name
example.myco.com:portnumber_Management_Service
```

To set it for the current OMS, use the property -oms_name local_oms. To set it for any other OMS, you can provide the name of that OMS. The OMS name has to be similar to `example.myco.com:portnumber_Management_Service`.

Note: In Oracle Enterprise Manager Cloud Control 12*c*, you do not have to restart OMS for the changes to take effect.

Note: In Oracle Enterprise Manager Cloud Control 12c, `emctl set property` by default sets the logging properties for all the OMS. To set the property for only one OMS, use the `-oms_name` option.

Table 22–3 Oracle Management Service Log File Properties in the emomslogging.properties File

Property	Purpose	Example
log4j.appender.emlogAppender. MaxFileSize	When OMS log file reaches this size, then OMS copies the logging data to a new rollover file and creates a new `emoms.log` log file. The size of the log is specified in units of bytes. This property is also applicable for emoms_pbs.log.	log4j.appender.emlogAppender. MaxFileSize=20000000
log4j.appender.emlogAppender. MaxBackupIndex	This optional property indicates how many times OMS will rollover the log file to a new file name before deleting logging data. This property is also applicable for emoms_pbs.log. **Note:** Because the log file does not contain as much data as the trace file, it is usually not necessary to create more than one rollover file.	log4j.appender.emlogAppender. MaxBackupIndex=1
log4j.appender.emtrcAppender. MaxFileSize	When the OMS trace file reaches this size, then OMS copies the logging data to a new rollover file and creates a new `emoms.trc` log file. This property is also applicable for emoms_pbs.trc.	log4j.appender.emtrcAppender. MaxFileSize=5000000
log4j.appender.emtrcAppender. MaxBackupIndex	This property indicates how many times the OMS will rollover the trace file to a new file name before deleting tracing data. This property is also applicable for emoms_pbs.trc.	log4j.appender.emtrcAppender. MaxBackupIndex=10

22.4.4 Controlling the Contents of the Oracle Management Service Trace File

By default, the OMS will save all critical and warning messages to the `emoms.trc` file. However, you can adjust the amount of logging information that the OMS generates.

To change the amount of logging information generated by the OMS, run the following command:

```
emctl set property -name "log4j.rootCategory" -value "<LEVEL>, emlogAppender,
emtrcAppender" -module logging
```

The above command will change the log level for all OMS, unless `-oms_name option` is specified.

Note: If you change the root logging level for the emoms.trc file, then a lot of messages are written to the trace file filling up the space quickly, and potentially slowing down the system. Run the following command to enable debug selectively for specific modules that need to be assessed:

```
emctl set property -name <logging module> -value DEBUG -module
logging
```

Where, <logging module> represents the logging module from a specific subsystem.

For example, oracle.sysman.emdrep.dbjava.loader.

The logging level can be changed for specific modules by running the following command:

```
emctl set property -name "<CATEGORY>" -value "<LEVEL>" -module
logging
```

where LEVEL can be DEBUG, INFO, WARN, or ERROR, and CATEGORY is specific to the module for which level has to be changed. To change the logging module, contact Oracle Support.

Note: The location of emoms.trc, emoms.log, emoms_pbs.trc, and emoms_pbs.log files can be changed to a different location from the default location. However, it is not advisable to do so.

22.4.5 Controlling the Oracle WebLogic Server and Oracle HTTP Server Log Files

Oracle Management Service is a Java EE application deployed on an Oracle WebLogic Server. Different components of the Oracle WebLogic Server generate their own log files. These files contain important information that can be used later by support personnel to troubleshoot problems.

Table 22–4 lists the location of the log files for some components.

Table 22–4 Component Log File Location

Component	Location

Oracle HTTP Server (OHS)	`<EM_INSTANCE_BASE>/<webtier_instance_name>/diagnostics/logs/OHS/<ohs_name>`
	For example,
	`/u01/app/Oracle/gc_inst/WebTierIH1/diagnostics/logs/OHS/ohs1`

OPMN	`<EM_INSTANCE_BASE>/<webtier_instance_name>/diagnostics/logs/OPMN/<opmn_name>`
	For example,
	`/u01/app/Oracle/gc_inst/WebTierIH1/diagnostics/logs/OPMN/opmn`

Table 22–4 (Cont.) Component Log File Location

Component	Location

Oracle WebLogic	The log data from WebLogic will be at:
	`<EM_INSTANCE_BASE>/user_projects/domains/<domain_name>/servers/<SERVER_NAME>/logs/<SERVER_NAME>.log`
	This log can be restricted, rotated by size, time, and other conditions from the WebLogic Console. The default settings are:
	■ In production mode, they are rotated at a default of 5MB.
	■ The log level is WARNING.
	■ The number files are restricted to 10.
	For example,
	`/u01/app/Oracle/gc_inst/user_projects/domains/GCDomain/servers/EMGC_OMS1/logs/EMGC_OMS1.log`
	The messages written to sysout and syserr will be available in the .out files. They cannot be rotated by size or time. They are rotated only when the server starts. They are located at:
	`<EM_INSTANCE_BASE>/user_projects/domains/<domain_name>/servers/<SERVER_NAME>/logs/<SERVER_NAME>.out`
	For example,
	`/u01/app/Oracle/gc_inst/user_projects/domains/GCDomain/servers/EMGC_OMS1/logs/EMGC_OMS1.out`
	The node manager logs are at `<INST_HOME>/NodeManager/emnodemanager` and the admin server logs are at `<INST_HOME>/user_projects/domains/GCDomain/servers/EMGC_ADMINSERVER/logs`.

By default, the Enterprise Manager Cloud Control configures Oracle HTTP Server logs to roll over periodically to a new file, so that each file does not grow too large in size. You must also ensure that you delete the old rollover files periodically to free up the disk space. You can use an operating system scheduler, like cron on UNIX, to periodically delete the rollover files.

Note: Following are log files that you will need to maintain and manually purge:

- `<gc_inst>/user_projects/domains/<domain_name>/servers/EMGC_ADMINSERVER/logs/<domain_name>.log*`
- All files under `<gc_inst>/WebTierIH1/diagnostics/logs/OHS/ohs1/`. For example:

  ```
  em_upload_http_access_log.*
  access_log.*
  em_upload_https_access_log.*
  ohs1-*.log
  console~OHS~1.log*
  mod_wl_ohs.log*
  ```

- Log files under the admin server and emgc_oms server:

  ```
  <gc_inst>\users_projects\domains\<domain_name>\servers\EMGC_
  ADMINSERVER\logs\*.out*
  <gc_inst>\users_projects\domains\<domain_name>\servers\EMGC_
  OMS?\logs\*.out*
  ```

For instructions on controlling the size and rotation of these log files, refer to chapter "Managing Log Files and Diagnostic Data" in *Oracle Fusion Middleware Administrator's Guide*.

For information about configuring Enterprise Manager to view Fusion Applications PL/SQL and C diagnostic log files, see chapter "Managing Oracle Fusion Applications Log Files and Diagnostic Tests" in *Oracle Fusion Applications Administrator's Guide*.

22.5 Monitoring Log Files

You can use Log File Monitoring to monitor WebLogic Server and Application Deployment log files for specific patterns. You can set up Cloud Control to receive alert notifications in the context of targets when patterns are found. This allows you to be more proactive and learn of problems as an administrator before end users discover them.

Use the following topics to learn how to set up and use Log File Monitoring:

- About Log Viewer
- Overview of WebLogic Server and Application Deployment Log File Monitoring
- Enabling Log File Monitoring
- Configuring Log File Monitoring
- Viewing Alerts from Log File Monitoring

22.5.1 About Log Viewer

Log Viewer enables administrators to view, search, and download middleware-related log files regardless of where the files reside on disk. Complex search criteria can be specified and saved for future reference in order to help administrators quickly diagnose performance problems across multiple middleware components spanning multiple Fusion Middleware Farms and WebLogic Domains.

Note: If you want to use all features of the log viewer in Cloud Control, and the target domain for which you want to view log messages is SSL-enabled with a custom certificate, then log viewer features will not function properly. For most features of log viewer, the OMS makes a JMX connection to the Admin Server of that domain. The only log viewer feature that does not have the OMS make a direct JMX connection to the Admin Server is the feature used for archived log files. Instead, the agent is used for viewing archived log files.

For log viewer features to fully function in this environment, you must apply additional configuration changes.You must take the *rootca* of the custom certificate from the Admin Server target for the domain against which you want to view log messages and import it into the trust store of the OMS.

When accessing Log Viewer, default search criteria is specified for the selected target type. The administrator can then refine the search criteria based on diagnostic requirements for the particular Fusion Middleware Farm. By using the Add Fields button, you can refine the search criteria to include:

- Selecting one or more member targets of the Fusion Middleware Farm
- Specifying the date range
- Selecting the message types
- Specifying the messages to be searched
- Specifying the ECIDs to be searched
- Specifying the application name
- Specifying the user name

Once the search criteria has been defined, the administrator clicks on the search button.

The administrator modifies the search as needed and clicks the **Save Search** button on the Log Viewer.

The search criteria specified, including the targets against which the search was performed, is then saved to the Management Repository for the currently logged in administrator.

You can click on the **Saved Searches** button to retrieve and apply a previously stored Search Criteria.

You can click on the Manage Saved Searches and bring up a pop-up to edit or delete the previously Saved Search Criteria.

22.5.2 Overview of WebLogic Server and Application Deployment Log File Monitoring

You can use Log File Monitoring to monitor WebLogic Server and Application Deployment log files for specific patterns and thereby reduce troubleshooting time. You can set up Cloud Control to receive alert notifications in context of targets when patterns are found.

The Log File Monitoring metric, Log File Pattern Matched Line Count for WebLogic Server and Application Deployment target types allows you to monitor one or more log files for the occurrence of one or more perl patterns. In addition, you can specify a perl pattern to be ignored for the log file. Periodic scanning, which occurs by default every 60 minutes, is performed against any new content added since the last scan. Lines matching the ignore pattern are ignored first, then lines matching specified match patterns result in one record being uploaded to the repository for each pattern. You can set a threshold against the number of lines matching the given pattern. File rotation will be handled within the given file.

You can also use the monitoring templates functionality, which allows an administrator to configure a metric once in a template and then apply the template to several WebLogic Server or Application Deployment targets at once, rather than having to configure each WebLogic Server log file monitoring metric individually.

If you are currently using log file monitoring via the Host target type, you should configure log file monitoring via the Fusion Middleware related target type instead so you can see alerts in context of a Fusion Middleware target.

Prerequisites to Use Log File Monitoring

Log File Monitoring requires a local Management Agent monitoring target. In other words, the host on which the log files you want to monitor reside must have an agent installed and running. The OS user who installed the agent must have read access to directories where the monitored log files reside. Log file monitoring is disabled by default. You must enable it in order to use this feature.

22.5.3 Enabling Log File Monitoring

Log File Monitoring is disabled by default. To enable Log File Monitoring, follow these steps:

1. From the target menu, select **Monitoring**.
2. Choose **Metric and Collection Settings**.
3. Under the Log File Monitoring row, click the **Disabled** link to change the setting to Enabled.
4. On the Edit Collection Settings: Log File Monitoring page, click **Enable** in the Collection Schedule section.
5. Click **Continue**.

Once you enable and configure Log File Monitoring, the default collection schedule is set for every 60 minutes.

22.5.4 Configuring Log File Monitoring

To configure Log File Monitoring, follow these steps:

1. From the target menu, choose **Monitoring**.
2. From the Monitoring menu, select **Metric and Collection Settings**, then choose the **Log File Pattern Matched Line Count** metric.
3. Click the **Edit** icon on the right.

   Cloud Control displays the Edit Advanced Settings:Log File Pattern Matched Line Count page.
4. Click **Add** to add new object(s) in order to specify settings for the log files to be monitored.

Add objects to the Monitored Objects table. The table lists all Log File Name/Match Pattern in Perl/Ignore Pattern in Perl objects monitored for this metric. You can specify different threshold settings for each Log File Name/Match Pattern in

Perl/Ignore Pattern in Perl objects. The Reorder button specifies which log file to scan first.

In past releases, if % was provided, the text was not ignored and all lines read from the file were included for pattern matching. However, this behavior has been updated wherein only "" (an empty string) is the prescribed method not to ignore any lines. However for backward compatibility "%" will still be considered as the equivalent to the "" string.

Good examples:

```
/u01/middleware/user_projects/domains/riddles_
domain/servers/ManagedServer_1/logs/access.log
```

```
C:\\u01\middleware\user_projects\domains\riddles_
domain\severs\ManagedServer_1\logs\access.log
```

Bad example:

```
/u01/middleware/user_projects/domains/riddles_
domain/servers/ManagedServer_1/logs/%.log
```

The Match Pattern in Perl value specifies the pattern that should be monitored in the log file. Perl expressions are supported in this field, and case is ignored.

Examples:

- FATAL - This pattern will be true for any lines containing fatal
- *fatal.*critical.* - This pattern will be true for any lines containing fatal and critical

The Ignore Pattern in Perl value specifies the pattern that should be ignored in the log file. If the Ignore Pattern in Perl field has a default value of % in the field, you should remove the default value if nothing should be ignored. Perl expressions are supported in this field, and case is ignored.

The Warning Threshold and Critical Threshold values should be set to a number such that if the pattern occurs in the log file the specified number of times within the collection schedule, then an alert will be triggered. If the number of occurrences is specified in the advanced settings, then this factors into when alert is raised.

For example, if you set the critical threshold to 1 (if pattern found more than 1 time in log file, it is critical alert) and the number of occurrences to 2, then a critical alert is raised only when the pattern is found more than once in the log file within 2 consecutive collections.

Once log file monitoring is enabled and configured, you can include the 'Log File Pattern Matched Line Count' metric as part of a Monitoring Template. Log file locations must be the same across targets to which the template is applied. You can apply the template to multiple WebLogic servers or Application Deployment targets at once rather than setting monitoring settings individually on a per-target basis.

If after configuring the Log File Monitoring metric the log file contains the specified patterns but the alerts are not generated in the OMS, you should do the following:

- Check whether the log file name contains a perl pattern.
- Check whether the ignore pattern contains an asterisk (*). Providing an asterisk in the ignore pattern field will also ignore all the lines which include the matched patterns.

Configuration Issues

If an error message displays indicating that logging configuration is missing or invalid for certain targets, you can try the following options.

First, the WebLogic Domain that you are accessing may not be Oracle JRF (Java Required Files) enabled. Oracle JRF consists of components not included in the Oracle WebLogic Server installation and that provide common functionality for Oracle business applications and application frameworks. To view log messages, the target must be Oracle JRF enabled. To check to see if your WebLogic Domain, for example, is Oracle JRF enabled, perform the following steps:

1. From the WebLogic Domain menu, select Target Setup submenu and then Monitoring Configuration.
2. On the Monitoring Configuration page for the domain, look for the property labeled “Can Apply JRF”. The value for this property could be true or false. If the value is false, then the domain is not Oracle JRF enabled.

If the value of the “Can Apply JRF” property is true for the domain, this does not necessarily mean that all managed servers within the domain are Oracle JRF enabled. If you are unable to access log messages in the context of a specific managed server, then navigate to the relevant managed server’s Monitoring Configuration page. From the Monitoring Configuration page, look for the property “Is JRF Enabled”. The value for this property could be true or false. If the value is false, then the managed server is not Oracle JRF enabled.

Second, the Enterprise Manager Cloud Control administrator who is trying to access log messages does not have the necessary target privileges to do so. In order to view log messages, the administrator must have been granted the target privilege “Ability to view Fusion Middleware Logs” for the corresponding target. Talk to your Oracle Enterprise Manager’s site administrator or super administrator regarding whether you have this privilege or not. Refer to later questions in this document for additional details on this target privilege and granting the privilege to administrators.

22.5.5 Viewing Alerts from Log File Monitoring

Alerts generated from the Log File Pattern Matched Line Count metric appear on the home page of the target or the Alert History page.

Triggered alerts must be manually cleared.

22.6 Configuring Log Archive Locations

You can configure the host, its credentials, and archive location information for a WebLogic domain and for all targets under the domain. You can either configure everything collectively under the target at the same time, or you can configure the targets individually.

To configure all of the targets at the same time, follow these steps:

1. From the WebLogic domain home page, select **Logs** from the WebLogic Domain menu, then select **Configure Archive Locations**.

   The Configure Archive Locations page appears.

2. Select the WebLogic domain in the table, then click **Assign Host Credentials**.

   An Assign Host Credentials pop-up appears.

3. Provide the requisite information and make sure that the Apply Above Host Credentials to Child Targets check box is enabled, then click **OK**.

The host name you selected now appears in the Host column of the Configure Archive Locations page, and the column also displays this host for all of the child targets.

4. Click **Assign Archive Location**.

   A Remote File Browser pop-up appears.

5. Double-click a directory name to enter in the host name field, then repeat this process for each sub-directory that you want to in the field. Click **OK** when you have finished.

   The directory location you selected now appears in the Archive Location column of the Configure Archive Locations page, and the column also displays this location for all of the child targets.

To configure the targets separately, follow the procedure above, except select a particular target rather than the WebLogic domain.

23

Configuring and Using Services

This chapter provides an overview of services and describes the procedures to configure and monitor services with Enterprise Manager. It contains the following sections:

23.1 Introduction to Services

The critical and complex nature of today's business applications has made it very important for IT organizations to monitor and manage application service levels at high standards of availability. Problems faced in an enterprise include service failures and performance degradation. Since these services form an important type of business delivery, monitoring these services and quickly correcting problems before they can impact business operations is crucial in any enterprise.

Enterprise Manager provides a comprehensive monitoring solution that helps you to effectively manage services from the overview level to the individual component level. When a service fails or performs poorly, Enterprise Manager provides diagnostics tools that help to resolve problems quickly and efficiently, significantly reducing administrative costs spent on problem identification and resolution. Finally, customized reports offer a valuable mechanism to analyze the behavior of the applications over time.

Enterprise Manager monitors not only individual components in the IT infrastructure, but also the applications hosted by those components, allowing you to model and monitor business functions using a top-down approach, or from an end-user perspective. If modeled correctly, services can provide an accurate measure of the availability, performance, and usage of the function or application they are modeling.

23.1.1 Defining Services in Enterprise Manager

A **service** is defined as an entity that provides a useful function to its users. Some examples of services include CRM applications, online banking, and e-mail services. Some simpler forms of services are business functions that are supported by protocols such as DNS, LDAP, POP, FTP or SMTP.

Enterprise Manager allows you to define one or more services that represent the business functions or applications that run in your enterprise. You can define these services by creating one or more tests that simulate common end-user functionality. You can also define services based on system targets, or on both system and service tests.

You can create service tests to proactively monitor your services. Using these tests, you can measure the performance and availability of critical business functions, receive notifications when there is a problem, identify common issues, and diagnose causes of failures.

You can define different types of service models based on your requirement. Some of the types of service models that you can create are:

- **Generic Service**: A Generic Service is the simple service model you can create in Enterprise Manager. You can define one or more service models by associating service tests and/or associating relevant system targets that represent a critical business function.
- **Aggregate Service**: A number of services can be combined together to form an Aggregate Service. Within the context of an Aggregate Service, the individual services are referred to as **sub-services**. An Aggregate Service can also be used as a sub-service to create other Aggregate Services.

  An aggregate service must contain at least one of the following: member service, system, or test. The metrics can be promoted from a member service, or a system, or a test.

  You can define other service models based on your requirement.

23.2 Creating a Service

Before you create a service, you must be familiar with the concepts of service management. You must also perform the following tasks:

- Identify the locations where the Management Agents must be available to monitor the services using the appropriate service tests and protocols. For example, if your service includes HTTP based service tests or IMAP based service tests, ensure that the location of the Management Agent within your network architecture allows these tests. You must ensure that the Management Agents are installed at appropriate locations according to the network security (firewalls) and network routing guidelines.

  Note that the beacon targets must already be created on the Management Agents before creating the service.
- Discover all the components for your service so that they can be listed as Enterprise Manager targets.
- Define systems on which the service is based.

You can create:

- Generic Service - Test Based: You can create a service that is based on a type of service test such as ATS, CalDAV, DNS, FTP, and so on.

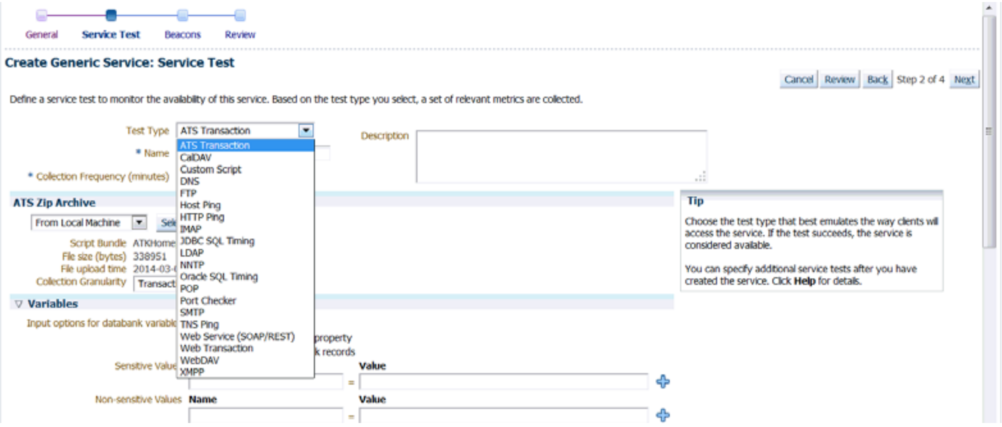
- Generic Service - System Based: You can create a service that is based on a system or one or more system components.
- Aggregate Service: An aggregate service consists of one or more sub services which can either test based or system based generic services.

23.2.1 Creating a Generic Service - Test Based

To create a test based generic service, follow these steps:

1. From the Targets menu, select Services. The Services main page is displayed.
2. From the Create menu, select Generic Service - Test Based. The Create Generic Service: General page appears.
3. Enter a name for the service and select a time zone in which the service has to be monitored. The availability of the service and the SLA computation is based on the time zone you select here. Click **Next**.
4. The Create Generic Service: Service Test page appears. Select a test from the Test Type drop down list.

Figure 23–1 Create Generic Service: Service Test Page



Create Generic Service: Service Test

Define a service test to monitor the availability of this service. Based on the test type you select, a set of relevant metrics are collected.

Test Type: ATS Transaction

* Name

* Collection Frequency (minutes)

Description

ATS Zip Archive

From Local Machine

Script Bundle: ATKHome

File size (bytes): 338951

File upload time: 2014-03-

Collection Granularity: Transact

Variables

Input options for databank variabl ... property ... k records

Sensitive Value

Non-sensitive Values

Tip

Choose the test type that best emulates the way clients will access the service. If the test succeeds, the service is considered available.

You can specify additional service tests after you have created the service. Click **Help** for details.

> **Note:** If you select **ATS Transaction** test type, then in the ATS Zip Archive section you can import the files either from your local machine or from test repository. However, to use the latter, ensure that you have uploaded the test script to the test repository. For information on how to use the Test Repository, see Section 23.8.

5. Depending on the test type you selected, enter the other parameters on this page and click **Next**. The Create Generic Service: Beacons page appears.
6. Click **Add** to add one or more beacons for monitoring the service. It is recommended that you use beacons that are strategically located in your key user communities in order for them to pro-actively test the availability of the service from those locations. If no beacons exist, you must create a new beacon. See Deploying and Using Beacons for details.

Notes:

- Only a single beacon should be added from a Management Agent to monitor service tests. Adding multiple beacons from the same Management Agent to a service test is not recommended.

  Beacons are targets that are used to monitor service tests, primarily to measure performance of the service or business function from a different geographic location. Thus, adding multiple beacons from the same Management Agent does not add any value.
- Beacons marked as key beacons will be used to determine the availability of the service. The service is available if one or more service tests can be successfully executed from at least one key beacon.
- It is recommended that you create the beacons before you create the service.

7. Click **Next**. The Create Generic Service: Review page appears. Review the information entered so far and click Finish to create the service. The newly created service appears on the main Services page.

23.2.2 Creating a Generic Service - System Based

To create a system based generic service, follow these steps:

1. From the Targets menu, select Services. The Services main page is displayed.
2. From the Create menu, select Generic Service - System Based. The Create Generic Service: General page appears.
3. Enter a name for the service and select a time zone for the service. Click **Next**. The Create Generic Service: System page appears. Select a system on which the service is to be based. A system refers to the infrastructure used to host the service. A system can consist of components such as hosts, databases, and other targets.
4. Click **Next**. The Create Generic Service: Review page appears. Review the information entered so far and click Submit to create the service. The newly created service appears on the main Services page.

23.2.3 Creating an Aggregate Service

Aggregate services consist of one or more services, called sub services or member services. A subservice is any service created in Enterprise Manager Cloud Control. The availability, performance, and usage for the aggregate service depend on the availability, performance, and usage for the individual sub services comprising the service. When creating an aggregate service, at the very least, either a system or one or more sub services must be associated. You can include both sub services and a system if required.

To create an aggregate service, follow these steps:

1. From the Targets menu, select Services. The Services main page is displayed.
2. From the Create menu, select Aggregate Service. The Create Aggregate Service: General page appears.

3. Enter a name for the aggregate service and select a time zone in which the service is to be monitored. The monitored data will be displayed in the selected time zone. Click **Next**.
4. The Create Aggregate Service: Services page appears. Click **Add** and select one or more member services (sub services) that are to be part of the aggregate service. You can add one or more test based, system based generic services, and one or more aggregate services. Click Next.
5. The Create Aggregate Service: System page appears. Select a system target on which the service is to be based. Associating a system with a service is not mandatory but is recommended. Features like Root Cause Analysis depend on key system components being correctly defined.

After you have created an aggregate service, you can add or remove its constituent sub services, modify the availability definition and add or delete performance or usage metrics.

WARNING: If you delete or remove a subservice from an aggregate service, the aggregate service performance, usage, and business metrics may be affected if they are based on a deleted subservice's metrics.

23.3 Monitoring a Service

After a service has been defined, you can monitor the status of the service, view the availability history, performance, enabled SLAs, topology, and so on. This section describes the following:

- Generic / Aggregate Service Home Page
- Performance Incidents Page
- SLA Dashboard
- Test Summary
- Topology

23.3.1 Viewing the Generic / Aggregate Service Home Page

To view the overview of the performance, availability, and usage of your service, click on a selected service in the main service pages. The Home page of the selected service appears. It contains the following regions:

- General: In this region, you can view the current status of the service and the availability (%) over the last 24 hours. You can also view whether the availability is based on the service test, or the system. In the case of aggregate services, availability can also be based on the sub services. The Availability History chart shows the period of time for which the service was available, when it was down, in a blackout status, and so on.
- Component Availability: This region shows the availability of the service tests or system components on which the service is based. Select the **Show Only Key Tests** check box to view only the key components or tests.

23.3.2 Viewing the Performance / Incidents Page

On this page, you can view charts for the performance and usage metrics defined for the service and drill down to view additional metric details.

Performance metrics to help you identify how well the service test is performing for each of the remote beacons. In general, the local beacon should have a very efficient and consistent response time because it is local to the Web application host. Remote beacons provide data to reflect the response time experienced by your application end users.

Usage metrics are used to measure the user demand or workload for the service. Usage metrics are collected based on the usage of the underlying system components on which the service is hosted. You can monitor the usage of a specific component or statistically calculate the average, minimum and maximum value from a set of components.

In the Incidents and Problems region, you can view any incidents or problems associated with the service.

23.3.3 Viewing the SLA Dashboard

This page displays the list of enabled SLAs for this service. For each SLA, you can see the following:

- The current status of the SLA and its SLOs along with the service level value for the current SLA period.
- The History column shows the SLA status for the last seven days.
- The Violations column shows the actual, remaining, and total allowable SLA violation times for that SLO.

23.3.4 Viewing the Test Summary

The Test Reporting Dashboard shows the list of all the enabled tests for that particular service. Apart from the execution history of the tests over the last 24 hours, the most failed step of the test information is also displayed, both at the beacon level and at the test (aggregate) level.

The trend of the total time taken by the transaction is also displayed over the last 24 hours. Also, the breakdown of the step metrics are displayed for a particular transaction execution.

Use this page to see an overview of all the tests, by performance and issues, and to drill down to individual executions per beacon and drill down to transaction results with an execution.

How to Use This Page

By default, on arriving at this page, all the enabled tests are shown at the overall level. The most failed step information is displayed which shows the most failing step of the test across all executing beacons.

On expanding any test node in the tree-table, the beacon level execution summary is displayed showing the test execution history (last 24 hours) along with the information of the most failed step.

On clicking on the test node in the tree table, the transaction diagnostics region shows up in the lower part of page. If the parent node, that is the test (overall) node, is selected, then the diagnostics regions in the lower part show the aggregated data across all successfully executing beacons.

The left part of this region shows the transaction total time trend (last 24 hours) and has a time selector slider. The intention of this slider is to select the transaction/transaction period to see the step diagnostics region which occupies the right part of the lower region.

23.3.5 Viewing the Service Topology

The topology viewer provides a graphical representation of the components of your service. The topology viewer shows all dependent components and sub services, represented as icons, as well as the relationships between them, represented as links. For system components, only key components are displayed.

You can do the following:

- View the relationship between the service and its dependencies, including other services, and system key components. All determinants for your service's availability are displayed in the Enterprise Manager Cloud Control Topology Viewer.
- View the causes of service failure, as identified by Root Cause Analysis. Potential root causes and down targets are highlighted. Select highlighted links between components to view details on the cause of service failure. For more information, see About Root Cause Analysis. If you have installed and configured the SMARTS Network Adapter, the topology page shows the status of the network for your failed service as well. For more information on Network Manager Adapter plug-ins, refer to About the SMARTS Network Adapter.

For more details on the topology viewer, refer to the Enterprise Manager Online Help.

23.3.6 Sub Services

Aggregate services consist of one or more services, called sub services or member services. A subservice is any generic test based on system based service The availability, performance, and usage for the aggregate service depend on the availability, performance, and usage for the individual sub services comprising the service.

This page lists all the sub services that are part of the aggregate service. For each sub service, the status of the service, key components, incidents, and so on are displayed.

23.4 Configuring a Service

After you have created a service, you can define the service availability, associate a system with the service, define performance and usage metrics, and so on. This section describes the following:

- Availability Definition
- Root Cause Analysis Configuration
- System Association
- Service Tests and Beacons
- Test Summary
- Monitoring Settings for Tests
- Usage Metrics
- Performance Metrics

- Edit Service Level Rule

23.4.1 Availability Definition (Generic and Aggregate Service)

The availability of a service indicates whether the service is available to the users at any given point in time. The rules for what constitutes availability may differ from one application to another. For example, for a Customer Relationship Management (CRM) application, availability may mean that a user can successfully log onto the application and access a sales report. For an e-mail application, it may be mean that the user can access the application, send and receive e-mails.

Click on the service for which you want to define the availability and navigate to the Service Home page. From the Generic Service menu, select Administration, then select Availability. The availability of a service can be based on:

- **Service Tests**: Choose this option if the availability of your service is determined by the availability of a critical functionality to your end users. Examples of critical functions include accessing e-mail, generating a sales report, performing online banking transactions, and so on. While defining a service test, choose the protocol that most closely matches the critical functionality of your business process, and beacon locations that match the locations of your user communities.

  You can define one or more service tests using standard protocols and designate one or more service tests as **Key Tests**. These key tests can be executed by one or more **Key Beacons** in different user communities. You can also indicate whether the service test is a key test by enabling the Key Service Test checkbox. Only key service tests are used to compute the availability of the service. You can then select the beacons that will be used to execute the key tests and determine the availability of the service. Depending on the definition, a service is considered available if all key service tests are successful or at least one key service test is successful. See Deploying and Using Beacons for details on beacons and how to create them.

  You can specify whether the service should be available when:

  - All key service tests are successful (Default). This option is recommended.
  - At least one key service test is successful

  Note: A service test is considered available if it can be executed by at least one key beacon. If there are no key beacons, the service test will have an unknown status.

- **System**: The availability of a service can alternatively be based on the underlying system that hosts the service or selected components of the system. If availability is based on selected system components, you must select the components that are critical to running your service and designate one or more components as **Key Components**, which are used to determine the availability of the service. The service is considered available as long as at least one or all key components are up and running, depending on your availability definition.

  You can specify whether the service should be available when:

  - All key components are up (Default)
  - At least one key component is up

  You can also mark one or more components as key system components that will be used to compute the availability of the service. Key system components are used to determine the possible root cause of a service failure. For more information, refer to "Root Cause Analysis Configuration" on page 23-9.

- **Sub Service**: For an aggregate service, availability can also be based on the availability of the sub services. You can specify if availability should be determined based on the availability of all sub services or a single sub service.

23.4.2 Root Cause Analysis Configuration

You can use Root Cause Analysis (RCA) to filter a set of events to determine the cause of a higher level system, service, or application problem. RCA can help you to eliminate apparent performance problems that may otherwise appear to be root causes but which are only side effects or symptoms of the actual root cause of the problem, allowing you to quickly identify problem areas. You can view the RCA results on the Home page or Topology page of any service that is currently down. The Topology page gives you a graphical representation of the service, along with the system and component dependencies. Targets that have caused the service failure are highlighted in the Topology page.

Before running RCA, you can choose to:

- Configure the tool to run automatically whenever a service fails.
- Disable RCA by changing the default Analysis Mode to Manual.
- Define component tests for the service and thresholds for individual tests.

To configure Root Cause Analysis, follow these steps:

1. From the Service Home page, click **Monitoring Configuration**.
2. From the Monitoring Configuration page, click **Root Cause Analysis Configuration**.
3. If the current mode is set to Automatic, click **Set Mode Manual** to disable RCA. If you choose to perform the analysis manually, you can perform the analysis from the Service home page at anytime by choosing **Perform Analysis** if the service is down. If the current mode is set for Manual, click **Set Mode Automatic** to enable RCA when the state of the service and its components change
4. Click the link in the **Component Tests** column of the table for the key component you want to manage. You can then manage the key components for the service on the Component Tests page by adding, removing, or editing component tests. When a service is down, you can drill down to the key components to verify the underlying issue. Refer to the Enterprise Manager Online Help for details on defining component tests.

> **Note:** When you disable RCA and set it back to automatic mode, RCA does not store the previous history results for you, thus providing no history for later reference.

23.4.2.1 Getting the Most From Root Cause Analysis

Root Cause Analysis (RCA) can provide you with great value by filtering through large amounts of data related to your services and identifying the most significant events that have occurred that are affecting your service's availability. If you are constructing your own services to manage in Enterprise Manager it is important that the services are defined with some thought and planning in order to get the most out of RCA.

The first item to consider in getting the most from RCA is the set of dependencies that your service has on other services or system components. Be sure to identify all of the system components that your service utilizes in order to accomplish its task. If you omit a key component and the service fails, RCA will not be able to identify that component as a possible cause. Conversely, if you include components in the service definition that the service does not actually depend on, RCA may erroneously identify the component as a cause of service failures.

When building service dependencies, keep in mind that you can take advantage of the aggregate service concept that is supported by Enterprise Manager. This allows you to break your service into smaller sub-services, each with its own set of dependencies. RCA considers the status of a sub-service (a service that you depend on) as well the system components or service on which the sub-service depends.

The second item to consider in getting the most from RCA is the use of component tests. As you define the system components that your service depends on, consider that there may be aspects of these components that may result in your service failure without the component itself failing. Component tests allow RCA to test the status not only of the target itself but also the status of its key aspects.

The RCA system allows you to create component tests based on any metric that is available for the key component. Remember, this includes any user-defined metrics that you have created for the component, allowing you great flexibility in how RCA tests the aspects of that component should your service fail. RCA can be configured to run in two modes. It can run automatically based on the failure of a service or can be configured to run manually. You can decide the mode based on the Expected Service Level Agreement % of the service being monitored. If the Expected Service Level Agreement % is high, you must select the automatic mode to ensure that that possible errors and the root cause of the failure is easily detected.

23.4.3 System Association

A system is the set of infrastructure components (hosts, databases, application servers, etc.) that work together to host your applications. For example, an e-mail application can be hosted by a database, listener, application server, and the hosts on which these components reside.

After you create a service, you can specify the associations between the components in the system to logically represent the connections or interactions between them. For example, you can define an association between the database and the listener to indicate the relationship between them. These associations are displayed in the topology viewer for the system. Some data centers have systems dedicated to one application or service. Alternatively, others have systems that host multiple services. You can associate single or multiple services to a System, based on how the data center is set up.

Use this page to select the Enterprise Manager system that will be used to host this service. You can do the following:

- Add or select a system
- Change or remove a selected system

After you have selected the system, mark one or more system components as key components that are critical for running the service. These key components are used to determine service availability or identify causes of service failure.

23.4.4 Monitoring Settings

For each service, you can define the frequency (which determines how often the service will be triggered against your application) and the performance thresholds. When a service exceeds its performance thresholds, an alert is generated.

To define metrics and thresholds, from the **Generic Service** menu, select **Administration**, then select **Monitoring Settings for Tests**. The Metric and Policy Settings page is displayed. Click the **Monitoring Settings** link. The Monitoring Settings - Thresholds page appears.

- **View By Metric, Beacon** - In this view, you can click **Add Beacon Overrides** to override the default threshold values for one or more beacons. In this case, the default thresholds will only be used for beacons without any overrides. Any new beacons added to the service will use the default thresholds. Click **Add Metric** to add one or more metrics.
- **View By Beacon, Metric** - In this view, you can click on the **Default** icon to toggle between Edit and View modes for a specific metric. In the Edit mode, you can modify the parameters of the metric. You can also modify the parameters of the metric for a specific beacon. In the View mode, the default parameters of the metric will be used.

  Apart from these procedures, you can also define metrics at the step, and step group level for Web transactions. You can choose either of the following views:

  - **View By Step, Metric, Beacon:** In this view, you can click **Add Beacon Overrides** to override the default threshold values for one or more beacons. In this case, the default thresholds will only be used for beacons without any overrides. Any new beacons added to the Web transaction will use the default thresholds. Click **Add Metric** to define thresholds for one or more metrics. Incidents are generated only if the value of the Data Granularity property is set to 'Transaction' for the service tests. For more information on the Web transaction properties, refer to the Create / Edit Service Test - Web Transaction help page in the Enterprise Manager Online Help.
  - **View By Step, Beacon, Metric:** In this view, you can click on the **Default** icon to toggle between Edit and View modes for a specific metric. In the Edit mode, you can modify the parameters of the metric for a specific beacon. In the View mode, the default parameters of the metric will be used. Incidents are generated only if the value of the Data Granularity property is set to ' Step'.

To define the default collection frequency and collection properties, click the **Collection Settings** tab on the Monitoring Settings page. You can do the following:

- Specify the default collection frequency for all the beacons. To override the collection frequency for a specific beacon, click **Add Beacon Overrides**.
- Specify the collection properties and their corresponding values for one or more beacons.

Refer to the Enterprise Manager Online Help for more details on the defining the collection intervals and performance thresholds.

23.4.5 Service Tests and Beacons

You can add additional service tests and specify one or more beacons that will execute these service tests. To add a service test or modify an existing service test, click the **Service Test and Beacons** link in the **Monitoring Configuration** page. The Service Tests and Beacons page appears. You can select a test type from the drop down list and create a service test.

23.4.5.1 Defining Additional Service Tests

You can create different types of service tests based on the protocol and the location of the beacons. From the Service Tests and Beacons page, you can do the following:

- Add one or more service tests for your service. Select the Test Type and click **Add**. Some of the test types that can be defined are ATS, FTP, Web Transaction, DNS, SOAP and others.
- After you have created the service test, you must enable it. If your service test is not enabled, it will not be executed by any of the beacons. You can define one or more service tests as key tests. These key tests are used to monitor the availability and performance of your service. Only service tests that are enabled can be designated as key tests. To set up a service test as a key test, click the **Availability Definition** link at the bottom of the page.
- Create, add, or remove a beacon. When you identify the beacon locations, select locations on your internal network or on the Internet that are important to your e-business. These are typical locations where your end users are located. For example, if your business is hosted in Canada and you have customers in the United States, use a beacon installed on a host computer in the United States to measure the availability and performance of your applications.
- After you have created the service test, you can verify it by clicking **Verify Service Test**. The Status icon indicates the status of the service test i.e. whether it can be successfully executed by the key beacons. If there are no key beacons defined for the service, the status will be unknown even if there are other beacons executing the service test. Click **Status** to go to the Status History page.

Note:

- While defining a SOAP (Simple Object Access Protocol) service test, if the WSDL URL to be accessed is outside the company's intranet, proxy settings need to be added to the `$OMS_HOME/sysman/config/emoms.properties` file.

  For example, to set up `www-myproxy.myco.com` as proxy, specify the values as follows:

  ```
  proxyHost=www-myproxy.myco.com

  proxyPort=80

  dontProxyFor=myco.com,mycorp.com
  ```

  The `proxyUser`,`proxyPwd`,`proxyRealm`,and `proxyPropsEncrypted` properties are used to configure an authenticated proxy. After you have modified the proxy settings, you must restart all the OMSes for the changes to be effective.

- The Forms Transaction test type has been deprecated in Enterprise Manager 12c. Forms transactions created in earlier releases can still be used but you cannot create new Forms Transaction test types. You must create a Generic Service target and create an ATS Transaction using OATS EBS/Forms Load test scripts. This ATS test type is used to monitor Oracle Forms applications.

- The Web Transaction test type is in maintenance mode only. To monitor Web applications, we recommend that you create an ATS load script and use the ATS Transaction test type to monitor Web applications. See Creating an ATS Service Test Using OATS Load Script for details.

The creation of different types of service tests is covered in detail in the Enterprise Manager Online Help. In this chapter, we have covered the creation of the ATS test type as an example.

23.4.5.2 Deploying and Using Beacons

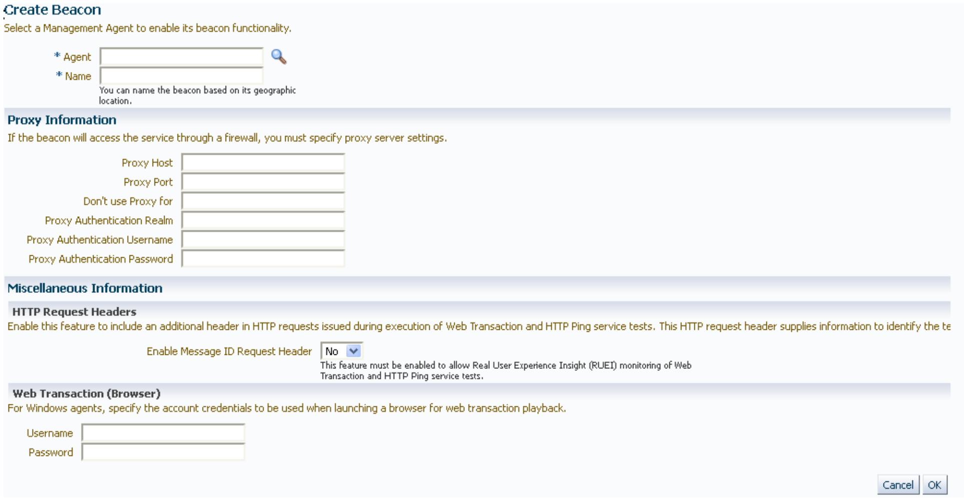
A beacon is a target that allows the Management Agent to remotely monitor services. A beacon can monitor one or more services at any point in time.

Note: Before you create a beacon, you must ensure that the Oracle Beacon 12.1.0.2 or higher plug-in has been deployed.

To create a beacon to run one or more service tests, follow these steps:

1. From the **Setup** menu, select **Add Targets**, then select **Add Targets Manually**.
2. In the Add Targets Manually page, select **Add Non-Host Targets by Specifying Target Monitoring Properties** option.
3. Select **Beacon** from the Target Type drop down list, select a Monitoring Agent and click **Add Manually**.
4. The Create Beacon page appears.

Figure 23–2 Create Beacon Page



Create Beacon

Select a Management Agent to enable its beacon functionality.

* Agent

* Name

You can name the beacon based on its geographic location.

Proxy Information

If the beacon will access the service through a firewall, you must specify proxy server settings.

Proxy Host

Proxy Port

Don't use Proxy for

Proxy Authentication Realm

Proxy Authentication Username

Proxy Authentication Password

Miscellaneous Information

HTTP Request Headers

Enable this feature to include an additional header in HTTP requests issued during execution of Web Transaction and HTTP Ping service tests. This HTTP request header supplies information to identify the te

Enable Message ID Request Header: No

This feature must be enabled to allow Real User Experience Insight (RUEI) monitoring of Web Transaction and HTTP Ping service tests.

Web Transaction (Browser)

For Windows agents, specify the account credentials to be used when launching a browser for web transaction playback.

Username

Password

5. Enter the following details:

   - Name: Name of the beacon being created.
   - Agent: Select the Management Agent on which the beacon will be running.
   - Proxy Information: If the beacon is accessing the service through a firewall, you must specify the proxy server settings as follows:
     - Proxy Host and Port: The name of the proxy server host and through which the beacon communicates.
     - Proxy Authentication Realm: The authentication realm (used for Basic and Digest authentication schemes) that is used to verify the credentials on the proxy server.
     - Proxy Authentication Username: The (fully qualified) username to be used for proxy server authentication.
     - Proxy Authentication Password: The accompanying password to be used for proxy server authentication.
   - Enable Message ID Request Header: Select the checkbox to include an additional header in HTTP requests issued when Web Transactions and HTTP Ping service tests are executed. This allows Real User Experience Insight (RUEI) monitoring of Web Transactions and HTTP Ping tests.
   - Web Transaction: For Windows agents, specify the account credentials to be used when launching a browser to playback a Web transaction.

   > **Note:** You can launch the Create Beacon option from the Services menu. From the **Services Features** menu, select **Beacons** and click **Add** to launch the Create Beacon page.

6. Click **Create** to create the beacon and return to the Beacon Home page. You can now use the beacon to monitor service tests.

7. From the Generic Service menu, select **Administration**, then select **Service Tests and Beacons**. You will see a list of service tests that have been enabled along with a list of beacons.

8. Select the service test to be monitored, then from the Beacons table, select the beacon that you have created. Indicate if it is a key beacon.
9. Click **Verify Service Test** to execute the service test by the selected beacon.

23.4.5.3 Configuring the Beacons

This section lists additional beacon related configuration tasks.

- **Configuring SSL Certificates for the Beacon**: When a beacon is used to monitor a URL over Secure Sockets Layer (SSL) HTTPS URL, the beacon must be configured to recognize the Certificate Authority that has been used by the Website where that URL resides.

  To use the SSL option with the Port Checker test, you may need to add additional certificates to the Management Agent's monitoring wallet. To add an additional certificate, follow these steps:

  1. Obtain the certificate, which is in `Base64encoded X.509 (.CER)` format, in the `b64SiteCertificate.txt` file. (The file name may be different in your configuration.) An example of the contents of the file is given below:

     ```
     ------BEGIN CERTIFICATE--------------
     MIIDBzCCAnCgAw...
     ...... base 64 certificate content .....
     ------END CERTIFICATE-----------------
     ```

     This file is stored in the Home directory of the Management Agent as `<AGENT_BASE>/agent_inst/sysman/config/b64InternetCertificate.txt` file.

  2. Create the `b64InternetCertificate.txt` file in the agent core and instance directory if it does not exist.

     ```
     <AGENT_BASE>/agent_inst/sysman/config/b64InternetCertificate.txt
     <AGENT_BASE>/core/12.1.0.2.0/sysman/config/b64InternetCertificate.txt
     ```

  3. Append the `Base64encoded X.509` certificate to the end of both `b64InternetCertificate.txt` files. Include both the `BEGIN` and `END CERTIFICATE` lines.
  4. Restart the Management Agent.

- **Configuring Dedicated Beacons**: Beacon functionality on an agent requires the the use of an internal Java VM. The use of a Java VM can increase the virtual memory size of the agent by several hundred megabytes. Because of memory constraints, it is preferable to create beacons only on agents that run on dedicated hosts. If you are running large numbers of tests (e.g., several hundred per minute) on a given beacon, you may also wish to install that beacon's agent on a dedicated host. To take full advantage of dedicated hardware, edit the agent's `$ORACLE_HOME/sysman/config/emd.properties` file. as follows:

  applicationmetadataquota: the disk quota in bytes for each application area

  – Set the property, `ThreadPoolModel=LARGE`. This allows the agent to simultaneously run many threads.

  – Set the property, `useAllCPUs=TRUE`. This allows the agent to run on multiple CPUs simultaneously.

  – The `applicationMetadataQuota_BEACON` property determines the total size that can be used to store ATS zip files. If you are using a ATS zip file or need to configure a large number of small ATS zip files on the beacon, you must specify a higher value for the `applicationMetadataQuota_BEACON` property.

  - @ This property determines the total size that the beacon can consume to store

    @ ATS zip files. If the user intends to use large ATS zip files or wishes to

    @ configure large number of small ATS zip files on a beacon then this property

    @ should be appropriately increased.

  - Append `-Xms512m -Xmx1024m` to the `agentJavaDefines` property. This increases the Java VM heap size to 1024 MB.

- **Configuring a Web Proxy for a Beacon**: Depending on your network configuration, the beacon may need to be configured to use a Web proxy. To configure the Web proxy for a beacon, search for the beacon in the All Targets page. Select the beacon you wish to configure and click **Configure**. Enter the properties for the Web proxy. For example, to set up `www-proxy.example.com` as the beacon's Web proxy, specify the values as the following:

```
Proxy Host: www-proxy.example.com
Proxy Port: 80
Don't use Proxy for: .example.com,.example1.com
```

> **Note:** You cannot play Siebel service tests and Web Transaction (Browser) service tests on the same machine.

23.4.5.4 Creating an ATS Service Test Using OATS Load Script

You can use the Oracle Application Test Suite (OATS) to define an Openscript Transaction Service Test. This test is used to enable beacon application transaction monitoring using Openscript load testing scripts. Openscript is a component of OATS and provides advanced capabilities to record and play back various types of Web transactions, such as web/HTTP, Oracle EBS/Forms, Oracle Fusion/ADF, Siebel, Adobe Flex, and so on.

By using ATS load scripts, you can:

- Reuse ATS testing scripts for production application transaction monitoring as part of application lifecycle management.
- Expand the beacon capabilities by:
  - Supporting complex application flows with mixed application types and protocols such as HTTP and Oracle Forms application in one flow.
  - Supporting protocol based Siebel application monitoring.
  - Providing Databank support.
  - Incorporating enhanced scripting and debugging features from Openscript.
  - Adding the latest script modules and features without updating Enterprise Manager.

Creating an ATS service test involves the following:

- Visit *http://www.oracle.com/technetwork/oem/app-test/index-084446.html* to download Openscript.
- Launch the installer and follow the steps to install Openscript.
- Record a new ATS transaction script by following these steps:

  - Launch Openscript and from the **File** menu, select **New**.
  - Select the type of script to be created and click **Next**. Some of the script types you can create are Adobe Flex, Oracle Fusion / ADF, Siebel, Database, Java Code Script, Web/HTTP and so on.
  - Select the location where the script is to be stored, enter a script name, and click **Finish**.
  - From the **View** menu, select **Openscript Preferences** to set the recording preferences.
  - Select **Record Category** and then select **HTTP Preferences**. Change the **Record Mode** from **Web** to **HTTP**. This ensures that scripts are played back correctly.
  - Select **Record** from the **Script** menu. The browser automatically opens when you start recording.
  - Load the web page where you want to start recording into the browser. Navigate the web site to record page objects, actions, and navigations. When you have finished navigating pages, close the browser and click **Stop**.
  - Select **Playback** from the **Script** menu to verify that the script has been properly recorded. Watch the application flow being played back in the play pane. Make sure the message log pane does not have any errors or failures. Save the script.
- After the script has been recorded, from the **File** menu, select **Export Script**.
  - Specify the location in which the script is to be saved. You can save the script in a repository or workspace.
  - Enter a name for the script and click **Finish**. A script bundle (.zip) is created. Make sure that the script bundle is self contained. See Creating a Self Contained Zip File.

  > **Note:** If the script file is very large, uncheck the **Recorded Data** option.

- Log into Enterprise Manager, upload the script bundle, and create an ATS service test. See Creating an ATS Service Test for details.

For more details on OATS, please refer to *Oracle® Functional Testing OpenScript User's Guide*.

23.4.5.4.1 Creating a Self Contained Zip File You must ensure that the zip file is self contained and contains the following:

- **<txn name>.jwg**: The archive file that contains the compiled script executable to be run by Execution Engine.
- **script.java**: The actual script Java source file.
- **<script name>-descriptor.xml** – Describes the step hierarchy
- **script.xml**: Describes the variables in the databank.
- **modules.properties**: Describes which internal modules are required for the engine.
- **Assets.xml**: Describes the dependent resources used by the root scripts including databank files, sub scripts, object libraries, and so on.

- **Databank Files**: The databank files used by the script while substituting different variable values.
- **Object Libraries**: The libraries that contain user-defined object identification rules and names. This is only applicable for functional testing scripts
- **Dependent Scripts**: A script can call out to other script.

23.4.5.4.2 Creating an ATS Service Test

To create an ATS service test, follow these steps:

> **Note:** To use the command line utility (EM CLI) to create and customize an ATS Test instance using the service test available in the repository, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

1. From the **Targets** menu, select **Services**, then from the **Create** menu, select **Generic Service - Test Based**.
2. Enter a name for the service and select a time zone.
3. Click **Next**. In the Create Generic Service: Availability page, select **Service Test**.
4. In the Create Generic Service: Service Test, select the **Test Type** as ATS Transaction.
5. Enter a name, description, and collection frequency for the service test.
6. In the ATS Zip Archive region, you can specify the location from which the ATS zip archive is to be imported. It can be imported from:
   - From Local Machine: Click **Browse** to select the zip file to be uploaded from your local machine.
   - From Test Repository: Select a zip file that is present in the test repository and click **Continue**. See Using the Test Repository for details.

   Click **Continue**. Based on the zip file uploaded, the ATS ZIP Archive section and Variables section are populated.
7. You will return to the ATS Service Test page where you can specify the following:
   - **Usage Options**: You can configure the script variable values by selecting the required usage option. You can either use the values recorded during the transaction or use the databank. A databank is an external CSV file that ATS scripts can refer to supply different input values over multiple iterations of the same script. For example, a login script can use a databank file, named `login_credential.csv`, to supply different login credentials during iteration.

     You can select:

     – **Use Recorded Values**: While playing back the transaction, the beacon uses the recorded values in the script.

     – **Use Values From EM Test Property**: You can specify values in the databank columns. These values are used by the beacon while playing back the script. This is useful if the same value is to be used for each variable. If variables defined as test properties, the value can be easily modified without having to modify script bundle or databank files.

     – **Loop Through All Databank Records**: While playing back the transaction, the beacon will go through each row in the script. For example, the first iteration will use the first rows of all the databanks. The second iteration will use the second rows of data and so on.

- **Encryption Password**: If you have configured ATS Openscript to encrypt script data (using the **Openscript View File > Openscript Preferences > Generic > Encryption**) option, when you create the scripts, you need to enter the same encryption password as specified in the ATS openscript, so that beacon can play back the script properly.
- **Default Playback Options**: The default playback options the beacon uses to play back the ATS Script.
- **Additional Playback Options**: If additional playback options have to be specified, you can specify them here.

23.4.5.4.3 Troubleshooting ATS Service Test Playback Issues

If the space quota for the beacon has been exhausted, the beacon cannot playback the recorded values in the ATS script and you may see the following error:

```
Beacon synchronization did not transfer the needed files to the
agent. Please check the agent log. File at: <directory>
```

To address this issue, the applicationMetadataQuota agent property must be set to a higher value in the emd.properties file. The default value is 500 MB but if there are several large files to be uploaded, this must be increased. After the property value has bee changed, you must restart the Management Agent.

Notes:

- The ATS files are present in the `/EMSTATE/sysman/ApplicationState/beacon` directory.
- File names have following naming convention `<Txn guid>_<beacon guid>.zip`.
- ATS related logs (`gcagent.log`, `gcagent_error.log`, `emagent.nohup`) are available in the `EMSTATE/sysman/log` folder

23.4.5.4.4 Databanking and Parameterization You can parameterize recorded script inputs to perform data driven testing. Examples of inputs that can be parameterized include user name, password on the login page, data entered in the search field, recorded navigations or user actions, and so on.

You can use databanks as the data source for parameterizing script inputs. Databanks are one or more external comma-separated value (CSV) or text (TXT) files that provide inputs to script parameters. Multiple Databank files can be attached to a single script and users can specify how OpenScript assigns data during script playback.

You can select data input values from an `external.csv` file and substitute the variable values with the values from the Databank. The field names are on the first line of the file separated by commas (no spaces). The field data is on subsequent lines separated by commas (different line for each record, no spaces around commas). An example is shown below:

```
FirstName,LastName,Mail,Phone
John,Smith,JohnS@company.com,x993
Mary,Ellen,MaryE@company.com,x742
```

To use the databank records, follow these steps:

1. Open or create a script project.

2. Configure the Databank to use with a script in the Assets Script Properties.
3. Select the script node where you want to use the Databank record.
4. Select the Script menu and then select **Other** from the Add sub menu.
5. Expand the General node and select **Get Next Databank Record**. Click **OK**.
6. Select Databank avitek alias to specify the Databank file from which the records are to be retrieved.
7. Click **OK**. A GetNextDatabankRecord: databank alias node will be added to the script. In the Java Code view, the `getDatabank("databank alias").getNextDataBankRecord()` method will be added to the script code as follows:

   ```
   getDatabank("avitek").getNextDatabankRecord();
   ```

After you have configured the databank for use with a script, you can map the databank files to specific script parameters. To map databank fields to script parameters, follow these steps:

1. Expand the [4] Oracle WebLogic Server - Medical Record Sample Application script tree node.
2. Right-click the usernameInput parameter and select **Substitute Variable**. The Substitute Variable window opens with the databank field names listed.
3. Select the Username field and click **Finish**. The parameter value changes to a databank variable in double braces `{{db.avitek.Username,fred#@golf.com}}`
4. Right-click the passwordInput parameter and select **Substitute Variable**. The Substitute Variable window opens with the databank field names listed.
5. Select the Password field and click Finish. The parameter value changes to a databank variable in double braces `{{db.avitek.Password,weblogic}}`
6. Save the script.

For more details on setting up the Databank, see the *Oracle® Functional Testing OpenScript User's Guide*.

Adding a Beacon Specific Databank File

You can use the `upload_ats_test_databank_file` emcli command to add a beacon specific databank file. The format of this command is given below:

```
emcli upload_ats_test_databank_file -name=<service_name>
-type=<service_type> -testname=<test_name> -testtype=<test_type>
-databankAlias=<databank alias> -input_file=databank:<input_
file> -beaconName=<beacon_name>
```

23.4.5.4.5 Parameterizing URLs

You can create variables to use for URLs in a script. If you need to change the base URL of a script, parametrizing the URLs provides a quick way to re-baseline a script to use a new URL.

To parameterize URLs, follow these steps:

1. After you have recorded your script, from the **Tools** menu, select **Parameterize URLs**.
2. Select the URL to parameterize and enter a variable name to use for the URL. Click **Next**.

3. Select or unselect the checkbox to specify the instances of the URL that are to be changed. Click **Finish**.
4. In the Java Code view, the getVariables().set("variable name", "value",scope); method will be added to the script code in the initialize() section as follows:

   ```
   getVariables().set("myServerVar", "http://myServer.com",
   Variables.Scope.GLOBAL);
   ```

5. Repeat these steps to parameterize other URLs in the script.

23.4.5.4.6 Success or Failure Validation You can perform text matching from TreeView and CodeView. For example, if you enter a string "hello" in a Google search window, the text matching is as follows:

```
web.document("/web:window[@index='0' or
@title='Google']/web:document[@index='0']").assertText("MatchTex
t", "hello", Source.DisplayContent, TextPresence.PassIfPresent,
MatchOption.Exact);
```

```
Source - enum - (Html,Display Content)
```

```
Html - Raw Html including Tags
```

```
Display Content - Html without tags
```

```
MatchOption - Not Case Sensitive
```

- **Exact - sensitive:** Matches any part of source string. For example, if the text entered is **abcdef**, if you enter **abc**, the string will match.
- **ExactEntireString:** Matches the exact source string.
- **RegEx - Not Case Sensitive**: Matches source string and sub-string. For example, if the text entered is **abcdef**, you can enter **a.*d**.
- **RegExEntireString**: Matches the entire source string only. For example, if the text entered is **abcdef**, you can enter **a.*f**.
- **Wildcard - wildcard pattern**: Matches source string and substring. For example, if the text entered is **abcdefghijklm**, you can enter **a?c*f**.
- **WildcardEntireString**: Matches the entire source string. For example, if the text entered is **abcdefghijklm**, you can enter **a*m**.

23.4.5.4.7 Using Beacon Override You can use the beacon override feature to specify different variable values for a test running on a different beacon. To do so, follow these steps:

1. Databank a script.
2. Select **Use EM Test Property** option.
3. Define beacon by specifying the sensitive and non-sensitive values as follows:

```
Databank_Alias>."<COLUMN_NAME>"="VALUE",<Databank_
Alias>."<COLUMN_NAME>"="VALUE",...
```

For example:

```
FusionCredentials."host"="fs-aufsn4x0cxf",FusionCredentials."hos
tlogin"="login-aufsn4x0cxf",FusionCredentials."username"="faadmi
n",FusionCredentials."password"="fusionfa1"
```

23.4.5.4.8 Updating the Databank File To update the ATS test script, follow these steps:

1. From the **Generic Service** menu, select **Administration**, then select **Service Tests and Beacons**.
2. From the Service Tests table, select ATS Transaction test type, and click **Edit**.
3. In the ATS Zip Archive region, click **Download**. Select the location where it is to be downloaded and click OK.
4. Edit the `.csv` file using a spreadsheet editor and save the changes.
5. Log into Enterprise Manager and navigate to the ATS Transaction Test page.
6. In the ATS Zip Archive region, click **Upload** to upload the updated file.

23.4.5.4.9 Using SLM Header for RUEI Integration If the ATS service test data is to be monitored by RUEI, you must specify the `x-oracle-slm-message-id` request header in the **Additional Playback Options** field. The format is in the form: `name1:value1;name2:value2;name3:value3`.

For example, `x-oracle-slm-message-id: bcn=<beacon_name>; svc=<service_name>;test=<test_ name>;step={{@getTopLevelStepName()}}`

23.4.6 Performance Metrics

Performance metrics are used to measure the performance of the service. If a service test has been defined for this service, then the response time measurements as a result of executing that service test can be used as a basis for the service's performance metrics. Alternatively, performance metrics from the underlying system components can also be used to determine the performance of the service.

Performance metrics to help you identify how well the service test is performing for each of the remote beacons. In general, the local beacon should have a very efficient and consistent response time because it is local to the Web application host. Remote beacons provide data to reflect the response time experienced by your application end users.

You can do the following:

- Add a performance metric for a service test. After selecting a metric, you can choose to:
  - Use the metric values from one beacon. Choose this option if you want the performance of the service to be based on the performance of one specific location.
  - Aggregate the metric across multiple beacons. Choose this option if you want to consider the performance from different locations. If you choose this option, you need to select the appropriate aggregation function:

Table 23–1 Beacon Aggregation Functions

Function	Description
Maximum	The maximum value of the metric from data collected across all beacons will be used. Use this function if you want to measure the worst performance across all beacons.
Minimum	The minimum value of the metric from data collected across all beacons will be used. Use this function if you want to measure the best performance across all beacons.
Average	The average value of the metric will be used. Use this function if you want to measure the 'average performance' across all beacons.

Table 23–1 (Cont.) Beacon Aggregation Functions

Function	Description
Sum	The sum of the metric values will be calculated. Use this function if you want to measure the sum of all response times across each beacon.

> **Note:** If you are configuring a Web transaction, you can specify the **Source** which can be transaction, step group or step. Based on this selection, the metric you add will be applicable at the transaction, step group, or step level.

- Add a performance metric for the underlying system components on which the service is hosted. After selecting a metric for a target, you can choose to:
  - Use the metric from a specific component. Choose this option if you want the performance of the service to be based on the performance of one specific system component. If you select this option, you can choose the Rule Based Target List.
  - Aggregate the metric across multiple components. Choose this option if you want to consider the performance from multiple components. If you choose this option, you need to select the appropriate aggregation function.

Table 23–2 System Aggregation Functions

Function	Description
Maximum	The maximum value of the metric across all components will be used as the value of this performance metric for the service.
Minimum	The minimum value of the metric across all components will be used as the value of this performance metric for the service.
Average	The average value of the metric across all components will be used.
Sum	The sum of values of metrics across all components will be calculated.

> **Note:** When a system is deleted, performance metrics associated with the system will not be collected.

- Edit a performance metric that has been defined. For service test-based performance metrics, you can modify the beacon function that should be used to calculate the metric values. For system-based performance metrics, you can modify the target type, metric, and whether the aggregation function should be used. You can also modify the Critical and Warning thresholds for the metric.
- Delete a performance metric that has been defined.

> **Note:** If you are defining performance metrics for an aggregate service, you can:
>
> - Add performance metrics from a single sub service.
> - Specify statistical aggregations of more than one metric.
>
> After selecting the metrics, you can set the thresholds to be used to trigger incidents, or remove metrics that are no longer required.

23.4.6.1 Rule Based Target List

The Rule Based Target List is applicable for system based performance metrics and direct members of system. You can define a rule that matches a system component you have selected. System components that match the user-provided rule will participate in the metric evaluation process. Later if any system component is added that matches this rule, this component will also participate in the metric evaluation process. If any system component that matches the rule is removed, that component will not participate in the metric evaluation process. The rule you define can be based on:

- All (All system components)
- Contains (Any system component that contains given criteria'
- Starts With (Any system component that starts with given criteria)
- Ends With (Any system component that ends with given criteria)
- Equals (Any system component that matches with given criteria)

23.4.6.2 Static Based Target List

In this case, the dependent targets that are selected will participate in the metric evaluation and the targets that are not selected will not be included.

23.4.7 Usage Metrics

Usage metrics are used to measure the user demand for the service. Usage metrics are collected based on the usage of the underlying system components on which the service is hosted. You can monitor the usage of a specific component or statistically calculate the average, minimum and maximum value from a set of components. For example, if you are defining an email service, which depends on an IMAP server, then you can use the 'Total Client Connections' metric of the IMAP server to represent usage of this email service. You can define usage metrics only for services that are associated with a system. You can do the following:

- Add a usage metric. After selecting a metric for a target, you can choose to:
  - Use the metric from a specific component. Use this option if you want to monitor the usage of a specific component.
  - Aggregate the metric across multiple components. Use this option if you want to statistically calculate the usage across multiple components. If you choose this option, you need select the appropriate aggregation function.

Table 23–3 Aggregation Functions - Usage Metrics

Function	Description
Maximum	The maximum value of the metric across all components will be used as the value of this usage metric for the service.
Minimum	The minimum value of the metric across all components will be used as the value of this usage metric for the service.
Average	The average value of the metric across all components will be used.
Sum	The sum of the values of metrics across all components will be calculated.

- Edit a usage metric that has been defined.
- Delete a usage metric that has been defined.

Note that only metrics from system targets can be added as usage metrics. Metrics from tests are not indicative of usage, and therefore cannot be added as usage metrics.

Note: If you are defining usage metrics for an aggregate service, you can

- Add usage metric from a single sub service.
- Specify statistical aggregations of more than one metric.

After selecting the usage metrics, you can set the threshold to be used to trigger incidents or remove metrics that are no longer required.

Rule Based Target List

The Rule Based Target List is applicable for system based performance metrics and direct members of system. You can define a rule that matches a system component you have selected. This enables you to promote performance metrics for evaluation. System components that match the user-provided rule will participate in the metric evaluation process. Later if any system component is added that matches this rule, this component will also participate in the metric evaluation process. If any system component that matches the rule is removed, that component will not participate in the metric evaluation process. The rule you define can be based on:

- All (All system components)
- Contains (Any system component that contains given criteria'
- Starts With (Any system component that starts with given criteria)
- Ends With (Any system component that ends with given criteria)
- Equals (Any system component that matches with given criteria)

23.5 Using the Transaction Recorder

You can record a transaction using an intuitive playback recorder that automatically records a series of user actions and navigation paths. You can play back transactions interactively, know whether it is internal or external to the data center, and understand the in-depth break-out of response times across all tiers of the Web application for quick diagnosis.

You must install the transaction recorder in your computer to record transactions. The transaction recorder is also used for playing back and tracing transactions. The transaction recorder is downloaded from the Enterprise Manager Cloud Control server the first time any of these actions is performed. The transaction recorder requires some Microsoft libraries to be installed in your computer. If these libraries are not present during installation, they are automatically downloaded and installed from the Microsoft site. Make sure that your computer has access to the Internet to download these files. After the installation has been completed, you may need to restart your computer to make the changes effective.

23.6 Setting Up and Using Service Level Agreements

A service level agreement (SLA) is a contract between a service provider and a customer on the expected quality of service for a specified business period. An SLA consists of one or more service level objectives (SLOs) for different business calendars and different service periods for which define the service levels to be provided.

Whether an SLA is satisfied or not is based on the evaluation of the underlying SLOs. Service level indicators (SLIs) allow SLOs to be quantified and measured. An SLO can have one or more SLIs.

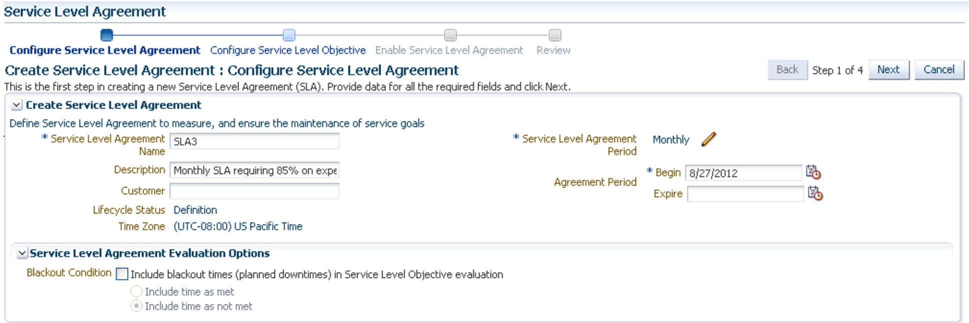
SLOs define the service level objectives to be provided. An SLO is a logical grouping of individual measurable Service Level Indicators (SLIs). For example, an SLO can define the percentage of time a service is available to the user, how well the service is performing in terms of response time or volume, and so on.

Service Level Indicators (SLIs) are quantifiable performance and usage metrics that can be used to evaluate the quality of a service.

To create an SLA, follow these steps:

1. Log in to Enterprise Manager as a user with `EM_ADMINISTRATOR` role.
2. From the **Targets** menu, select **Services**.
3. Click on a Generic Service target on the list. The Service Home page is displayed.
4. From the **Generic Service** menu, select **Service Level Agreement**, then select **Configuration**. The Service Level Agreement Configuration page appears.
5. On this page, you will see a list of all the SLAs defined for the selected service. Select an SLA from the list to view the details in the Service Level Agreement Details table. You can create an SLA or make a copy of an existing SLA (Create Like).
6. In the Service Level Agreement region, click **Create**. The Configure Service Level Agreement page appears.

Figure 23–3 Create Service Level Agreement: Configure Service Level Agreement


Service Level Agreement
Configure Service Level Agreement
Configure Service Level Objective
Enable Service Level Agreement
Review
Back
Step 1 of 4
Next
Cancel

Create Service Level Agreement : Configure Service Level Agreement

This is the first step in creating a new Service Level Agreement (SLA). Provide data for all the required fields and click Next.

Create Service Level Agreement

Define Service Level Agreement to measure, and ensure the maintenance of service goals

* Service Level Agreement Name: SLA3

Description: Monthly SLA requiring 85% on expe

Customer:

Lifecycle Status: Definition

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

* Service Level Agreement Period: Monthly

Agreement Period: * Begin 8/27/2012 Expire

Service Level Agreement Evaluation Options

Blackout Condition ☐ Include blackout times (planned downtimes) in Service Level Objective evaluation

○ Include time as met

● Include time as not met

Enter the following details:

- Name and description of the SLA.
- Name of the customer for whom the SLA is being created.
- The Lifecycle Status of the SLA. When an SLA is being created, it will be in the Definition Stage. For more details on the Lifecycle Status, see Lifecycle of an SLA.
- Specify the SLA Period. This is the contractual time period for which the SLA is determined and/or evaluated for compliance. (ie. quarterly, monthly, weekly SLA). Click the **Select** icon and select Monthly, Weekly, or Daily. Enter the Frequency which the SLA is to be evaluated and the date from which the SLA is to be evaluated. The SLA goals are reset when the SLA is evaluated.

For example, if you specify the SLA Evaluation Period as Monthly, Frequency as 12 and the date as 09/01/12, the SLA will be evaluated on that date followed 11 consecutive evaluations in the months of October, November, and so on.

- Specify the SLA Agreement Period. This is the **From** and **To Date** for which the recurring SLA periods are in effect. If you do not specify the **To Date** here, the SLA will have an Indefinite expiry date.
- An SLO may sometimes not be evaluated due to planned downtime or blackouts that have been scheduled for a service. In the Service Level Agreement Evaluation Options region, select the **Include blackout times (planned downtimes) in Service Level Objective evaluation** checkbox and specify whether the blackout times are to be included in the SLO evaluation. You can choose to:
  - Include time as met
  - Include time as not met
  - Exclude the blackout time during the overall computation of the SLO.

  For example, if the blackout or planned downtime for the week is 1 day, then the weekly availability is (7-1) / (7-1) days which is still 100% availability.

  By default, the **Include blackout times (planned downtimes) in Service Level Objective evaluation** option is not selected.

7. Click **Next**. In the Service Level Objectives page, define one or more SLOs that are to be part of the SLA. You can select the Evaluation Condition for the SLA which can be:
   - All Service Level Objectives must be met.
   - At least one Service Level Objective must be met.

   An SLA must have at least one SLO. More than one SLO can be active at any given time. You can either specify if all SLOs or at least one SLO should be met.
8. Click **Create** to define a new SLO. See Creating a Service Level Objective for details.
9. You can add more SLOs or edit the SLO you have defined. Click **Next**. In the Enable Service Level Agreement page, you can specify when the SLA is to be enabled. You can select:
   - Do Not Enable: If the SLA is not enabled, it will be in the Definition state and can be modified if required.
   - Enable Now: If the SLA is enabled, it cannot be modified as it will be in an Active state.
   - Enable Later: The SLA can be enabled later on a specified date.
10. Click **Next** , review details of the SLA, and click **Submit**. The SLA will be enabled on the specified date and you will return to the Service Level Agreement Configuration page.

23.6.1 Actionable Item Rules for SLAs

The table below shows a list of actions that can be performed on an SLA based on its status.

Status of SLA	Create Like	Edit	Enable	Disable	Delete
Definition	Yes	Yes	Yes	No	Yes
Scheduled	Yes	Yes	No	Yes	No
Active	Yes	No	No	Yes	No
Retired	Yes	No	No	No	Yes

- An SLA in a **Scheduled** or **Active** state cannot be directly deleted. You have to disable the SLA before you can delete it.
- When you edit an SLA in a **Scheduled** state, the status of the SLA changes to **Definition**.

23.6.2 Creating a Service Level Objective

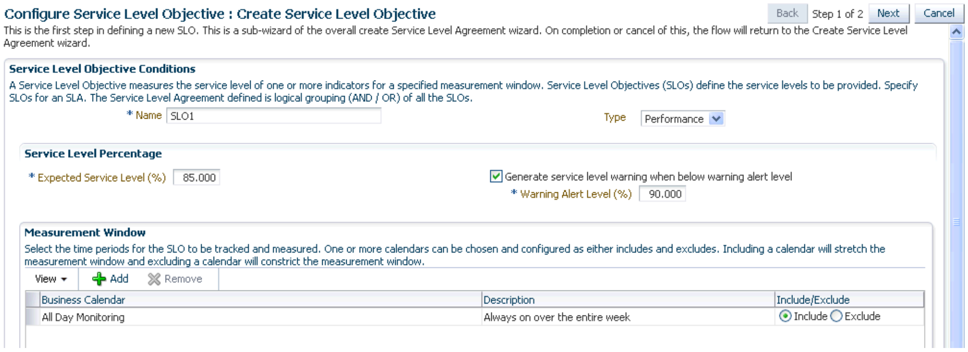
A Service Level Objective measures the service level of one or more indicators for a specified measurement window. Service Level Objectives (SLOs) define the service levels to be provided. You can specify if the SLA is considered to be satisfied if:

- All Service Level Objectives are met.
- At least one Service Level Objective is met.

To create an SLO, follow these steps:

1. Click **Create** in the Configure Service Level Objective page. The Create Service Level Objective page appears.

Figure 23–4 Create Service Level Objective



Configure Service Level Objective : Create Service Level Objective

This is the first step in defining a new SLO. This is a sub-wizard of the overall create Service Level Agreement wizard. On completion or cancel of this, the flow will return to the Create Service Level Agreement wizard.

Service Level Objective Conditions

A Service Level Objective measures the service level of one or more indicators for a specified measurement window. Service Level Objectives (SLOs) define the service levels to be provided. Specify SLOs for an SLA. The Service Level Agreement defined is logical grouping (AND / OR) of all the SLOs.

* Name: SLO1

Type: Performance

Service Level Percentage

* Expected Service Level (%): 85.000

☑ Generate service level warning when below warning alert level

* Warning Alert Level (%): 90.000

Measurement Window

Select the time periods for the SLO to be tracked and measured. One or more calendars can be chosen and configured as either includes and excludes. Including a calendar will stretch the measurement window and excluding a calendar will constrict the measurement window.

Business Calendar	Description	Include/Exclude
All Day Monitoring	Always on over the entire week	● Include ○ Exclude

2. Enter the following details:

   - Name of the SLO being defined.
   - Type of SLO: The SLO can be based on Availability or Performance metrics.
   - Expected Service Level%: This indicates the percentage of time the SLO conditions are met to ensure that the SLA is satisfied.
   - Warning Alert Level%: If the SLO conditions do not meet the specified threshold, a critical alert is generated.

     For example, if the Expected Service Level% is 90% and the Actual Service Level% is in the range of 90 to 99%, a Warning Alert is generated. If the Actual Service Level% is lesser than 90%, a Critical Alert is generated. This indicates that the SLA has been breached. If the Actual Service Level% is greater than 99%, it indicates that the SLA conditions have been satisfactorily met.

- Measurement Window: The time periods during which the SLO is in effect. A measurement window can have more than one time period assigned. For example, a measurement window can be configured as weekday peak hours which are Monday to Friday, from 9AM to 6PM and the weekend peak hours as 10AM to 2PM.

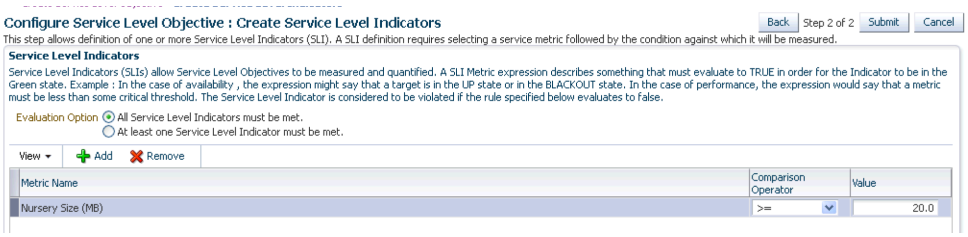
  While creating an SLO, you can choose more than one Business Calendar for an SLO. For example, suppose you want to evaluate each SLO from 8AM to 5PM except at lunch time (12PM to 1PM). You can create two measurement windows and exclude the lunch time from being measured.

  Another example of merging two measurement windows is when you want to combine weekly evaluation with calendar evaluation. If you want to evaluate an SLO every Monday and on the 15th of every month, you can create two monitoring windows and include these conditions in both the windows.

  By default, there are 3 predefined business calendars. You can also create your own calendar. See Defining Custom SLA Business Calendars for details.

3. Click **Next**. In the Create Service Level Indicators page, you can add one or more SLIs or conditions that allow the SLO to be measured.

Figure 23–5 Create Service Level Indicators



Configure Service Level Objective : Create Service Level Indicators

This step allows definition of one or more Service Level Indicators (SLI). A SLI definition requires selecting a service metric followed by the condition against which it will be measured.

Service Level Indicators

Service Level Indicators (SLIs) allow Service Level Objectives to be measured and quantified. A SLI Metric expression describes something that must evaluate to TRUE in order for the Indicator to be in the Green state. Example : In the case of availability , the expression might say that a target is in the UP state or in the BLACKOUT state. In the case of performance, the expression would say that a metric must be less than some critical threshold. The Service Level Indicator is considered to be violated if the rule specified below evaluates to false.

Evaluation Option ● All Service Level Indicators must be met.
○ At least one Service Level Indicator must be met.

Metric Name	Comparison Operator	Value
Nursery Size (MB)	>=	20.0

For example, if you are adding a performance SLI, you can specify that the Page Load Time should be less than or equal to 3 seconds. If this condition is not met, the SLI is considered to be violated. Specify the Evaluation Condition for the SLI:

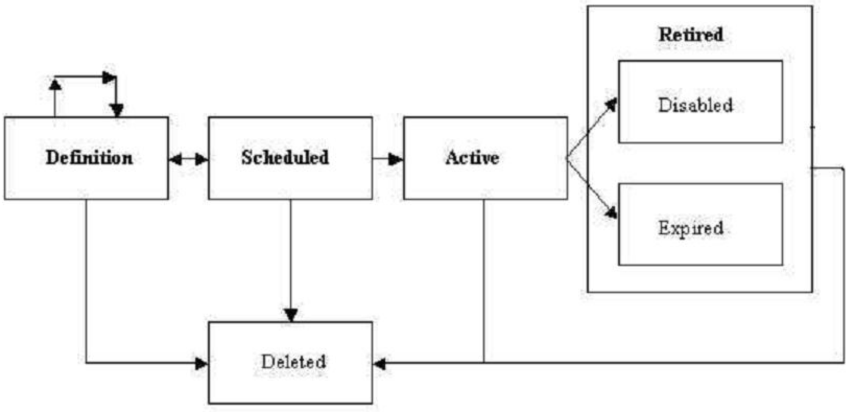
- All Service Level Indicators must be met.
- At least one Service Level Indicator must be met.

4. Click **Add** to add one or more metrics and specify the value and the evaluation condition. Click **Submit** to return to the Configure Service Level Objective page.

23.6.3 Lifecycle of an SLA

The following diagram shows the lifecycle of an SLA.

Figure 23–6 SLA Lifecycle



The SLA lifecycle consists of the following phases:

- Definition: This is the stage where the SLA is created and the SLOs are defined. You can configure or edit the SLA definition till the SLA is activated.
- Scheduled: This stage represents the period before the SLA is scheduled to go into effect at a future date.
- Active: This is the stage where the start date of a scheduled SLA is reached, or when the SLA is manually enabled.
- Retired: This is the stage when the SLA reaches the Expiry Date or the SLA is manually disabled.
- Disabled: An SLA can be manually disabled before it reaches the Expiry Date. Once an SLA is disabled, it cannot be reactivated. You must use the Create Like option to create a similar SLA and enable it.
- Expired: This is the stage where the SLA has reached the Expiry Date and is no longer active.
- Deleted: An SLA can be deleted if it is the Definition or Retired stage. An SLA that is an Active or Scheduled stage cannot be deleted.

23.6.4 Viewing the Status of SLAs for a Service

You can view the status of all SLAs for a service. To view the current status of the SLAs for a service, follow these steps:

1. From the **Targets** menu, select **Services**.
2. Click on a Generic Service target on the list. The Service Home page is displayed.
3. From the **Generic Service** menu, select **Service Level Agreement**, then select **Current Status**. The Service Level Agreement Current Status page appears.
4. This page shows a list of all the active SLAs that have been defined for this service. For each SLA, the SLA Status, SLA Evaluation Period, and the Service Level Objectives are displayed.
5. Select an SLA to view detailed information in the SLA. The following details are displayed:

- Tracking Status: This is the instant status of the SLI. For an Availability SLO, it is the status of the target. For a Performance SLO, it is the value of the Performance or Usage metric at a specific point in time.
- Service Level (%) : The percentage of time (from the beginning of the current evaluation period till the current date) the SLO conditions are met or the Tracking Status is **true**. If the Actual Service Level % is lesser than the Expected Service Level %, or the SLO conditions are met, the Service Level % graph is green.
- Type: This is the type of SLOs that have been defined for the SLA. This can be based on Availability or Performance metrics. An Availability SLO is based on the Response Metric [Service Target Availability]. It is specified in terms of the amount or percentage of time when the availability objective should be met. A Performance SLO gauges how well a service is performing. It includes measurements of speed and/or volume such as throughput or workload (ie. response times, transactions/hour). A Performance SLO can either be specified in terms of a set of SLIs, SLO conditions, and the amount or percentage of time when the objective should be met.
- SLO Violation: The violation allowances for each SLA evaluation period.
  - Total: The duration of the Evaluation Period * (Expected Service Level).
  - Actual: The time when the SLO is not met during the Evaluation Period.
  - Remaining: The time when the SLO could not be met without breaching the SLA. If the SLO is always met during the Evaluation Period, it indicates that there are no used allowances and the value in the Actual field will be 0.

23.6.5 Defining Custom SLA Business Calendars

Business Calendars are measurement windows that define a specific window of time in which the Service Level Objectives (SLO) are being measured. Out-of-the-box predefined business calendars are available. Apart from these, you can create custom business calendars. To create a custom business calendar, from the **Targets** menu, select **Services**. From the **Services Features** menu, select **Business Calendars**.

A list of business calendars that have been defined is displayed here. You can:

- **Create**: Click **Create** to set up a business calendar. The Add / Edit Business Calendar page is appears.
- **Create Like**: Select a calendar and click **Create Like** to make a copy of this calendar.
- **Edit**: Select a calendar, click **Edit** and make the necessary changes in the Add / Edit Business Calendar page.
- **Delete**: Select a calendar and click **Delete** to delete it. You cannot edit or delete a business calendar that is associated with one or more SLAs.
- **View Associated Service Level Agreements**: A business calendar can be used by one or more SLAs. Select a business calendar and click **View Associated Service Level Agreements** to view the SLAs that are associated with this calendar.

23.7 Using the Services Dashboard

The services dashboard provides a brief summary of all service related information in a single place. It provides a consolidated view of critical aspects of a service such as availability, performance, SLAs associated with the service, status of key system components, and so on.

23.7.1 Viewing the All Dashboards Page

To view the All Dashboards page, follow these steps:

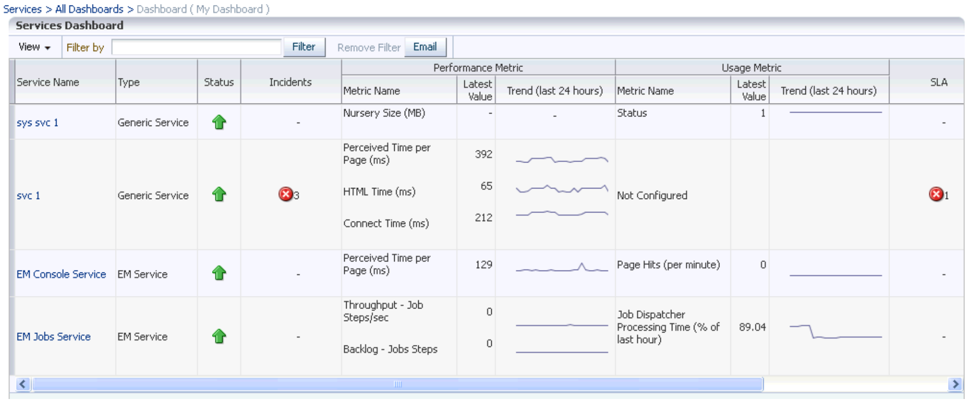
1. From the **Targets** menu, select **Services**.
2. From the **Services Features** menu, select **Dashboards**.
3. The All Dashboards page appears where you can see a list of all dashboards that have been created.
4. From the All Dashboards page, you can do the following:
   - **Create Dashboard**: Enter a unique name in the Dashboard Name field and a description, and click **Create Dashboard**. The newly added dashboard appears in the table. To create a dashboard, you must have an `EM_ADMINISTRATOR` role with **Create Services Dashboard** privilege.
   - **Customize Dashboard**: Select a dashboard from the list and click **Customize** and make the changes in the Edit Services Dashboard page. The dashboard can be customized only by the user who has created it.
   - **Delete**: Select a dashboard from the list and click **Delete**. The selected dashboard is deleted. The dashboard can be deleted only by the user who has created it.
5. Click on a Dashboard Name link to drill down to the Dashboard Details page.

23.7.2 Viewing the Dashboard Details Page

This page displays the following details:

- Service Name: Click on the link to drill down to the Service Details page.
- Incidents: Any incidents that have occurred.
- Performance / Usage Metric: The name of the performance and usage metrics available for the service and the latest value of each metric is displayed. The Trend charts show the metric trend over the last 24 hours. Click on the Trend chart to see a detailed view over the trend.
- SLA: Shows the number of enabled SLAs that are in Active, Critical or Warning state.
- Key Components: Shows the key targets that are up or available for this service.
- System Incidents: Any incidents that have occurred for the underlying systems of the service are displayed.

Figure 23–7 Services Dashboard



				Performance Metric			Usage Metric			
Service Name	Type	Status	Incidents	Metric Name	Latest Value	Trend (last 24 hours)	Metric Name	Latest Value	Trend (last 24 hours)	SLA
sys svc 1	Generic Service	⬆	-	Nursery Size (MB)	-	-	Status	1		-
svc 1	Generic Service	⬆	✖3	Perceived Time per Page (ms)	392		Not Configured			✖1
				HTML Time (ms)	65					
				Connect Time (ms)	212					
EM Console Service	EM Service	⬆	-	Perceived Time per Page (ms)	129		Page Hits (per minute)	0		-
EM Jobs Service	EM Service	⬆	-	Throughput - Job Steps/sec	0		Job Dispatcher Processing Time (% of last hour)	89.04		-
				Backlog - Jobs Steps	0					

You can filter the list of services that are listed in the dashboard. Specify a value in the Filter By field and click **Filter**. The filter will be applied on each row in all the services and the resulting list is displayed.

You can email a dashboard to one or more email addresses. Click Email and enter the email address and the subject of the dashboard. Click Send. This feature works only the htttp mode.

23.7.3 Customizing and Personalizing the Dashboard

You can customize a dashboard and make the changes available to all users. To customize a dashboard, select a row on the All Dashboards page and click **Customize**.

Note: The following privileges are required to cr

To add one or more services to the dashboard, click the Wrench icon. The Component Properties: Services Dashboard window appears. Select the type of service that you want to add to the dashboard and click **Search**. A list of services is displayed in the Available Targets table. Select one or more services that you want to add, move them to the Selected Targets table and click **Apply**. To add metrics to the respective services click on the Metrics tab and select the respective services to add metrics and click **OK**. The selected services and metrics now appear in the Services Dashboard table.

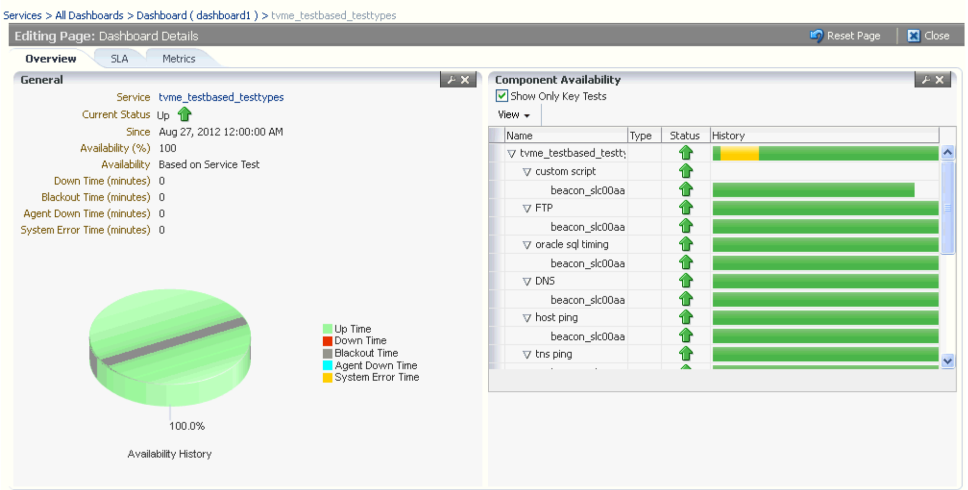
To delete a service target from the dashboard, select the row and click the Wrench icon. The Component Properties: Services Dashboard window appears. Deselect the services and metrics that are to be removed from the dashboard, click **Apply** and then click OK. To reset the changes you have made to the dashboard, click **Reset Page**. Any changes that have been made to the dashboard will be removed permanently. Click **Close** to exit the Edit mode.

You can make specific changes to a dashboard to suit your requirements. Click the **Personalize** icon and add or delete one ore more services from the dashboard. The changes that you make will be visible only to you and the other users cannot see the changes.

23.7.4 Viewing the Dashboard Service Details Page

This page shows detailed information for the selected service.

Figure 23–8 Dashboard Details Page



Service	tvme_testbased_testtypes
Current Status	Up ↑
Since	Aug 27, 2012 12:00:00 AM
Availability (%)	100
Availability	Based on Service Test
Down Time (minutes)	0
Blackout Time (minutes)	0
Agent Down Time (minutes)	0
System Error Time (minutes)	0

☑ Show Only Key Tests

Name	Type	Status	History
▽ tvme_testbased_testty		↑	
▽ custom script		↑	
beacon_slc00aa		↑	
▽ FTP		↑	
beacon_slc00aa		↑	
▽ oracle sql timing		↑	
beacon_slc00aa		↑	
▽ DNS		↑	
beacon_slc00aa		↑	
▽ host ping		↑	
beacon_slc00aa		↑	
▽ tns ping		↑	

It contains the following tabs:

- **Overview**: This tab provides a brief overview of the selected service. Click on the Service link to drill down to the Service Home page. It contains the following regions.
  - **General**: This region shows the name of the service, status, date from which the service is available, availability percentage, type of service (test or system based), down time, and error time. Click on the service name to drill down to the Service Home page.
  - **Component Availability**: This region shows the status of the components in the service. It shows the status of the component and the date from which the service has been Up. Select the Show Only Key Tests check box to view only the key service tests
- **SLA**: Shows a list of SLAs that have been enabled for this service. The name, status and the date from which the SLA is applicable is displayed. The SLA history over the last 7 days is also displayed.
- **Metrics**: This tab shows the performance and metrics charts that have been defined for this service. It also shows the incidents that have occured for the service and the underlying systems on which the service is based.

23.8 Using the Test Repository

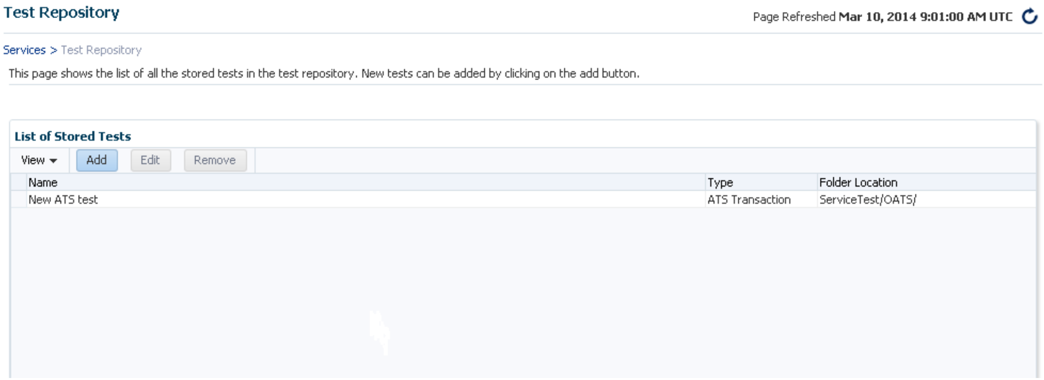
A test repository is a centralized location where you can maintain all the test scripts. To use the Test Repository, you should have pre-configured the OMS Software Library location. For more information, see Section 15.7.

The advantages of using a Test Repository include:

- Previously, a test could be created only in the context of a service. However, now, you have the flexibility of creating any number of test scripts outside the context of a service, and storing them in this centralized location called *Test Repository.* Uploading Test Scripts and Creating Services are now independent events. Once the test scripts are available in the repository, you can use them while creating your service.

- Previously, only the owner of the test script had the copy of the script. Now, with introduction of Test Repository, the scripts are maintained in a centralized location which allows all the users to access the scripts. At the time of creating a service, you can just import your scripts from the repository with the click of a button, thereby making the whole experience very user-friendly and quick.

> **Note:** Currently, there is support to store only the ATS test scripts in the central repository.



Test Repository

Page Refreshed **Mar 10, 2014 9:01:00 AM UTC**

Services > Test Repository

This page shows the list of all the stored tests in the test repository. New tests can be added by clicking on the add button.

List of Stored Tests

Name	Type	Folder Location
New ATS test	ATS Transaction	ServiceTest/OATS/

23.8.1 Viewing the Test Repository

To view the test scripts uploaded to the test repository, follow these steps:

1. From the **Targets** menu, select **Services**.
2. From the **Services Features** menu, select **Test Repository**.
3. The Test Repository page appears where you can see a list of all the tests that have been created.
4. From the Test Repository page, you can do the following:
   - **Adding Tests:** Click **Add**. In the Generic Information section, enter a unique test name. In the ATS Information section, click **Browse** to upload a test script from your local machine. Once you select a relevant file, the file name along with the step and module details are displayed. Click **Save** to save the script.
   - **Editing Tests:** Select the test, and click **Edit**. The ATS script cannot be modified within the Enterprise Manager Console. But you can download a previously uploaded script and import the zip file to ATS OpenScript. For more information on how to download and edit an ATS script, see Section 23.8.2.
   - **Removing Tests:** Select the test, and click Delete to delete the test script.
5. Click on a Test Name to view the details of the test in the Test Details table.

23.8.2 Editing an ATS Script

To download the script bundle and edit them, follow these steps:

- Click **Download** and save the zip file at the prompt.
- Launch OpenScript and from select File menu select Import Script to import the zip file to ATS OpenScript.

- After you have edited the script in ATS OpenScript, select **File**, then select **Export Script** to export the new script and save the zip file.
- Log into to Cloud Control, and navigate to the ATS Service Test page. Click **Upload** to upload the updated script file to Enterprise Manager.

23.9 Configuring Service Levels

A service level rule is defined as an assessment criteria used to determine service quality. It allows you to specify availability and performance criteria that your service must meet during business hours as defined in your Service Level Agreement. For example, e-mail service must be 99.99% available between 8am and 8pm, Monday through Friday.

A service level rule 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 rule is based on the following:

- **Business Hours:** Time range during which the service level should be calculated as specified in your Service Level Agreement.
- **Availability:** Allows you to specify when the service should be considered available. This will only affect the service level calculations and not the actual availability state displayed in the console. You can choose a service to be considered up when it is one or more of the following states:
  - Up: By default the service is considered to be Up or available.
  - Under Blackout: This option allows you to specify service blackout time (planned activity that renders the service as technically unavailable) as available service time.
  - Unknown: This option allows you to specify time that a service is unmonitored because the Management Agent is unavailable be counted as available service time.
- **Performance Criteria**: You can optionally designate poor performance of a service as a Service Level violation. For example, if your Website is up, but it takes 10 seconds to load a single page, your service may be considered unavailable.
- **Business Criteria:** Business criteria are useful in determining in the health of the business processes for a particular service. You can optionally define business metrics that can affect the Service Level. A Service Level violation occurs when a critical alert is generated for a specified business metric.

Note: The **Business Criteria** column is displayed only if one or more key business indicators are associated with the service. Refer to *Oracle Enterprise Manager Integration Guide*.

- **Actual Service Level:** This is calculated as percentage of time during business hours that your service meets the specified availability, performance, and business criteria.
- **Expected Service Level:** Denotes a minimum acceptable service level that your service must meet over any relevant evaluation period.

You can define only one service level rule for each service. The service level rule will be used to evaluate the **Actual Service Level** over a time period and compare it against the **Expected Service Level**.

23.9.1 Defining Service Level Rules

A Service Level Rule is defined as assessment criteria to measure Service quality. A Service Level Rule is based on the following:

- Time range for which the rule is applicable.
- Metrics that define the rule.
- The user expectation on these metrics values

The Expected Service Level is the expected quality for the service and is defined based on the time range and metrics of the Service Level Rule. For example, the Expected Service Level can be that the service is available 99% of the time during business hours.

When you create a service, the default service rule is applied to the service. However, you must edit the service level rule for each service to accurately define the assessment criteria that is appropriate for your service. To define a service level rule:

1. Click the **Targets** tab and **Services** subtab. The Services main page is displayed.
2. Click the service name link to go to the Service Home page.
3. In the Related Links section, click **Edit Service Level Rule**.
4. On the Edit Service Level Rule page, specify the expected service level and the actual service level and click **OK**. The expected service level specifies the percentage of time a service meets the performance, usage, availability, and business criteria defined in the Service Level Rule. The actual service level defines the baseline criteria used to define service quality and includes business hours, availability, performance criteria, usage criteria, and business criteria.

> **Note:** Any Super Administrator, owner of the service, or Enterprise Manager administrator with OPERATOR_TARGET target privileges can define or update the Service Level Rule.

23.9.2 Viewing Service Level Details

You can view service level information directly from the either of the following:

- **Enterprise Manager Cloud Control Console** -From any Service Home page, you can click on the Actual Service Level to drill down to the Service Level Details page. This page displays what Actual Service Level is achieved by the service over the last 24 hours/ 7 days / 31 days, compared to the Expected Service Level. In addition, details on service violation and time of each violation are presented in both graphical and textual formats.
- **Information Publisher** - Information Publisher provides an out-of-box report definition called the Services Dashboard that provides a comprehensive view of any service. From the Report Definition page, click on the **Services Monitoring Dashboard** report definition to generate a comprehensive view of an existing service. By default, the availability, performance, status, usage, business, and Service Level of the service are displayed. The Information Publisher also provides service-specific report elements that allow you to create your own custom report definitions. The following report elements are available:

- **Service Level Details**: Displays **Actual Service Level** achieved over a time-period and violations that affected it.
- **Service Level Summary**: Displays service level violations that occurred over selected time-period for a set of services.
- **Services Monitoring Dashboard**: Displays status, performance, usage, business, and service level information for a set of services.
- **Services Status Summary**: Information on one or more services' current status, performance, usage, business, and component statuses.

  Refer to the Online Help for more details on the report elements.

23.10 Configuring a Service Using the Command Line Interface

Using the Command Line Interface, you can define service targets, templates and set up incidents. EMCLI is intended for use by enterprise or system administrators writing scripts (shell/batch file, perl, tcl, php, etc.) that provide workflow in the customer's business process. EMCLI can also be used by administrators interactively, and directly from an operating system console. Refer to *Enterprise Manager Command Line Interface Guide* for details.

Samples EMCLI templates to create a Web transaction and an ATS service test are shown below.

Example 23–1 Web Transaction Service Test Template

```
<?xml version = '1.0' encoding = 'UTF-8'?> <transaction-template
template_type="generic_service" xmlns="template">
   <variables>
      <variable name="HOST1" value="linuxserver26.myco.com"/>
      <variable name="PORT1" value="5416"/>
      <variable name="PROTOCOL1" value="https"/>
   </variables>
   <transactions>
      <mgmt_bcn_transaction>
         <mgmt_bcn_txn_with_props>
            <mgmt_bcn_txn description="Test for checking the availability of EM
Console/Website" is_representative="true"
                          name="EM Console Service Test" monitoring="true" txn_
type="HTTP"/>
            <properties>
               <property name="readTimeout" num_value="120000.0" prop_type="2"
encrypt="false"/>
               <property name="Collection Interval" num_value="5.0" prop_type="2"
encrypt="false"/>
               <property name="certValidationMode" string_value="1" prop_type="1"
encrypt="false"/>
               <property name="maxDownloadSize" num_value="1.0E8" prop_type="2"
encrypt="false"/>
               <property name="sensitiveValuesProtection" string_value="0" prop_
type="1" encrypt="false"/>
               <property name="failureStringModes" string_value="regularText"
prop_type="1" encrypt="false"/>
               <property name="UserAgent" string_value="Mozilla/4.0
(compatible;MSIE 6.0; Windows NT 5.1) OracleEMAgentURLTiming/3.0" prop_type="1"
encrypt="false"/>
               <property name="successStringModes" string_value="regularText"
prop_type="1" encrypt="false"/>
               <property name="variablesModes" string_value="urlEncode" prop_
```

```
type="1" encrypt="false"/>
               <property name="content" string_value="0" prop_
type="1"encrypt="false"/>
               <property name="AcceptLanguage" string_value="en" prop_type="1"
encrypt="false"/>
               <property name="connectionTimeout" num_value="120000.0" prop_
type="2" encrypt="false"/>
               <property name="useCache" string_value="yes" prop_
type="1"encrypt="false"/>
               <property name="stringValidationMode" string_value="1" prop_
type="1" encrypt="false"/>
               <property name="granularity" string_value="transaction" prop_
type="1" encrypt="false"/>
               <property name="numThreads" num_value="4.0" prop_type="2"
encrypt="false"/>
               <property name="retries" num_value="1.0" prop_type="2"
encrypt="false"/>
               <property name="timeout" num_value="300000.0" prop_type="2"
encrypt="false"/>
               <property name="retryInterval" num_value="5000.0" prop_type="2"
encrypt="false"/>
            </properties>
            <per_bcn_properties/>
         </mgmt_bcn_txn_with_props>
         <steps_defn_with_props>
            <mgmt_bcn_step_with_props>
               <mgmt_bcn_step step_number="1" name="1.Access Logout page" step_
type="HTTP"/>
               <properties>
                  <property name="req_mode" num_value="1.0" prop_type="2"
encrypt="false"/>
                  <property name="http_method" string_value="G" prop_type="1"
encrypt="false"/>
                  <property name="url" string_
value="{PROTOCOL1}://{HOST1}:{PORT1}/em/console/logon/logoff?event=load" prop_
type="1" encrypt="false"/>
               </properties>
            </mgmt_bcn_step_with_props>
         </steps_defn_with_props>
         <stepgroups_defn/>
         <txn_thresholds>
            <mgmt_bcn_threshold warning_threshold="6000.0" warning_operator="0"
critical_threshold="12000.0" critical_operator="0" num_occurrences="1">
               <mgmt_bcn_threshold_key metric_name="http_response" metric_
column="avg_response_time"/>
            </mgmt_bcn_threshold>
            <mgmt_bcn_threshold warning_threshold="0.0" warning_operator="1"
critical_threshold="0.0" critical_operator="1" num_occurrences="1">
               <mgmt_bcn_threshold_key metric_name="http_response" metric_
column="status"/>
            </mgmt_bcn_threshold>
         </txn_thresholds>
         <step_thresholds/>
         <stepgroup_thresholds/>
      </mgmt_bcn_transaction>
   </transactions>
</transaction-template>
```

Example 23–2 ATS Service Test Template

```
<?xml version = '1.0' encoding = 'UTF-8'?>
<transaction-template template_type="generic_service" xmlns="template">
   <variables/>
   <transactions>
      <mgmt_bcn_transaction>
         <mgmt_bcn_txn_with_props>
            <mgmt_bcn_txn is_representative="true" name="ATS Page"
monitoring="true" txn_type="OATS"/>
            <properties>
               <property name="Collection Interval" num_value="5.0" prop_type="2"
encrypt="false"/>
               <property name="scriptDescription" string_value="[1] SignIn&#xA;[2]
Welcome&#xA;[3] Single Sign-Off&#xA;[4] Sign In" prop_type="1"encrypt="false"/>
               <property name="fileUploadTime" string_value="2012-08-0908:47:22.0"
prop_type="1" encrypt="false"/>
               <property name="OpenScriptJwgName" string_value="ATKHomepage.zip"
prop_type="1" encrypt="false"/>
               <property name="usageOptions" string_value="userDefined" prop_
type="1" encrypt="false"/>
               <property name="fileSize" string_value="41368" prop_type="1"
encrypt="false"/>
               <property name="beaconDistributionOverride" string_
value="AtsCredentials=1" prop_type="1" encrypt="false"/>
               <property name="FilePropertyValue" prop_type="7" encrypt="false"/>
               <property name="databankFilesJar" prop_type="7" encrypt="false"/>
               <property name="databankFiles" string_
value="AtsCredentials,AtsCredentials.csv,3;" prop_type="1" encrypt="false"/>
               <property name="granularity" string_value="transaction" prop_
type="1" encrypt="false"/>
               <property name="databankValues" string_
value="people.firstname=yang.,people.lastName=wang,middle.middlename_col=x." prop_
type="1" encrypt="false"/>
               <property name="modules" string_
value="oracle.oats.scripting.modules.utilities;version=2.4.0&#xA;oracle.oats.scrip
ting.modules.http;version=2.4.0&#xA;"
                         prop_type="1" encrypt="false"/>
               <property name="databankAliasMapping" string_
value="AtsCredentials=AtsCredentials.csv" prop_type="1" encrypt="false"/>
               <property name="defaultCLIOptions" string_
value="-dboptions*:1:FIRST_RECORD_ONLY -jwg ATKHomepage.jwg -noReport true" prop_
type="1"
                         encrypt="false"/>
            </properties>
            <per_bcn_properties/>
         </mgmt_bcn_txn_with_props>
         <steps_defn_with_props>
            <mgmt_bcn_step_with_props>
               <mgmt_bcn_step step_number="1" name="[1] Sign In" step_
type="OATS"/>
               <properties>
                  <property name="url" string_value="http:://www.test.com/test1"
prop_type="1" encrypt="false"/>
               </properties>
            </mgmt_bcn_step_with_props>
            <mgmt_bcn_step_with_props>
               <mgmt_bcn_step step_number="2" name="[2] Welcome" step_
type="OATS"/>
               <properties>
                  <property name="url" string_value="http:://www.test.com/test2"
```

```
prop_type="1" encrypt="false"/>
               </properties>
            </mgmt_bcn_step_with_props>
            <mgmt_bcn_step_with_props>
               <mgmt_bcn_step step_number="3" name="[3] Single Sign-Off" step_
type="OATS"/>
               <properties>
                  <property name="url" string_value="http:://www.test.com/test3"
prop_type="1" encrypt="false"/>
               </properties>
            </mgmt_bcn_step_with_props>
            <mgmt_bcn_step_with_props>
               <mgmt_bcn_step step_number="4" name="[4] Sign In" step_
type="OATS"/>
               <properties>
                  <property name="url" string_value="http:://www.test.com/test4"
prop_type="1" encrypt="false"/>
               </properties>
            </mgmt_bcn_step_with_props>
         </steps_defn_with_props>
         <stepgroups_defn/>
         <txn_thresholds>
            <mgmt_bcn_threshold warning_threshold="0.0" warning_operator="1"
critical_threshold="0.0" critical_operator="1" num_occurrences="1">
               <mgmt_bcn_threshold_key metric_name="openscript_response" metric_
column="status"/>
            </mgmt_bcn_threshold>
         </txn_thresholds>
         <step_thresholds/>
         <stepgroup_thresholds/>
      </mgmt_bcn_transaction>
   </transactions>
</transaction-template>
```

23.11 Troubleshooting Service Tests

This section lists some of the common errors you may encounter while using the Forms and the Web Transaction test type. The following topics are covered here:

- Verifying and Troubleshooting Forms Transactions
- Verifying and Troubleshooting Web Transactions

23.11.1 Verifying and Troubleshooting Forms Transactions

The section covers the following:

- Troubleshooting Forms Transaction Playback
- Troubleshooting Forms Transaction Recording

23.11.1.1 Troubleshooting Forms Transaction Playback

This section lists some of the common errors you may encounter while playing back a Forms transaction and provides suggestions to resolve these errors.

1. **Error Message:** Connection to Forms Server is lost. Possible version mismatch between `agentjars` and `formsjars`.

   Possible Cause: The transaction was recorded using an out-of-the-box Forms version.

Solution: Verify the version of the Forms Application that you are running by checking the version number in the About Oracle Forms Online Help. If this version is not supported, follow the steps listed under Error Message 2.

2. **Error Message:** Version Not Supported `<forms_version>`

   Possible Cause: The machine on which the beacon has been installed does not contain the necessary forms jar files.

   Solution: To resolve this error, follow these steps:

   1. Login to the system on which the Forms server has been installed. Locate the `frmall.jar` (if you are using Forms 10.1 or later) or `f90all.jar` (if are using Forms 9.0.4 or later) under the `$FORMS_HOME/forms/java` directory.
   2. Login to the system on which the beacon has been deployed and copy the jar file to the `$ORACLE_HOME/jlib/forms/<version>/` directory. The version you specify here should be the same as the version string in the error message. Make sure that the directory is empty before you copy over the jar file.

   If you are using Oracle Applications R12 and you encounter this error, follow these steps to resolve the error:

   1. Login to the system in which the Oracle Application server has been deployed. Locate the following files:

      ```
      $JAVA_TOP/oracle/apps/fnd/jar/fndforms.jar
      $JAVA_TOP/oracle/apps/fnd/jar/fndewt.jar
      ```

   2. Login to the system on which the beacon has been deployed and copy these files to the `$ORACLE_HOME/jlib/forms/apps/` directory. Make sure that the directory is empty before you copy over the jar files.

      > **Note:** You cannot monitor two deployments of Oracle Applications from the same beacon if different versions of Oracle Applications have been used.

3. **Error Message:** Forms URL is not pointing to the forms servlet.

   Possible Cause: When the Forms transaction was recorded, the location of the forms servlet could not be determined.

   Solution: Make sure that the Forms URL Parameter is pointing to the forms servlet. It should be `http://<hostname>:<port>/forms/frmservlet` for Forms10*g* or `http://<hostname>:<port>/forms/f90servlet` for Forms 9i. This parameter is automatically set by the Forms Transaction Recorder. But if it has not been set, you can locate the URL by following these steps:

   - Launch the Forms application.
   - View the source HTML file in the Forms launcher window.
   - Locate the `xsurl` variable. The URL is stored in this variable.

4. **Error Message**: Could not connect to `<machine name>`.

   Possible Cause: The machine on which the beacon has been installed cannot access the Forms Application.

   Solution: Make sure the machine on which the beacon has been installed can access the Forms Application and firewalls have been properly configured.

Support for playing back Forms transactions through proxy server is not available in this release.

5. **Error Message**: Invalid module path in the initial message.

   Possible Cause: The transaction may have been incorrectly recorded or may be corrupt.

   Solution: Try to record the transaction again.

6. **Error Message**: Cannot connect to login server.

   Possible Cause: This error may occur due the following reasons:

   - The Login URL that you have specified may be incorrect.
   - An invalid HTTPS certificate may have been provided for the login server.

   Solution:

   - Verify that the Login URL is correct.
   - If you are using HTTPS to connect to login server, make sure the certificate on the server is written for the login server machine itself. Make sure the SSL Certificate is imported into Agent and the CN of the certificate matches the host name of the login Server URL.

23.11.1.2 Troubleshooting Forms Transaction Recording

This section lists some troubleshooting steps that you can use when the Forms transaction cannot be recorded successfully.

1. Make sure that all your Internet Explorer instances are closed and no java runtime programs are open.
2. Start recording again with the java console open. You can view any exceptions or error messages displayed on the console.
3. You should now see the text "`Forms Transaction Recorder Version: <version number>`" on the console. If this text is displayed, proceed to step 5. If you do not see the text, check if the `formsRecorder.jar` has been copied to the Forms archive directory. You can perform this check using either of the following methods:

   1. Navigate to the Forms archive directory and check if the `formsRecorder.jar` file is present in the directory.
   2. Navigate to the **Enable Forms Transaction Monitoring** page, select the corresponding Forms server target and click **Configure**. Enter the host credentials to see if the Forms Transaction Recorder has already been configured on this Forms server. If the `formsRecorder.jar` is not present in the Forms archive directory, you need to configure your Forms server for transaction monitoring. After ensuring that the `formsRecorder.jar` is present in the archive directory of the Forms server, go back to **Step 1** and try recording again.

4. If you see an exception related to the java .policy file displayed on the java console, check the file to ensure that it has the required content and is in the right location. If any errors are found, you must fix these errors and try recording again.
5. If the recording still fails, check if the Enterprise Manager Certificate has been imported to the secure site.f the certificate has not been imported, you must import it and try recording again.

23.11.2 Verifying and Troubleshooting Web Transactions

This section lists some of the common errors you may encounter while recording and playing back Web Transactions.

1. **Scenario:** Verify Service Test displays: `Connection establishment timed out -- http://..../`

   Possible Cause: The beacon can only access that URL via a proxy server and it has not been configured.

   Solution: From the All Targets page, select the beacon, click **Configure** and set the beacon proxy setting.

2. **Scenario**: Verify Service Test displays: `Authorization Required -- https://...../`

   Possible Cause: The Basic Authentication information is not recorded automatically.

   Solution: To resolve this error, follow these steps:

   1. From the Service Tests and Beacons page, select the service test, click Edit.
   2. Make sure you enter all the Basic Authentication information: Username, Password, and Realm.

   Note: Realm usually appears above the Username label in the Browser's authorization dialog box.

   ---

3. **Scenario**: Verify Service Test displays `sun.security.validator.ValidatorException`: `No trusted certificate found -- https://....../.`

   Possible Cause: The beacon does not know about this SSL Certificate.

   Possible Solution: From the Service Tests and Beacons page, select the service test, and click **Edit**. Under **Advanced Properties**, and set **Authenticate SSL Certificates** to **No**.

4. **Scenario**: Verify Service Test displays: `Timeout of 300000 exceeded for https://....../ Response time = 3000000`

   Possible Cause: The test may be too complex to complete within the allotted time. Or, this may be an actual performance issue with the server.

   Possible Solution: From the Service Tests and Beacons page, select the service test, and click **Edit**. If this is not a server performance issue, under **Advanced Properties**, increase the **Timeout Value**.

5. Scenario: The Verify Service Test option reports that the service as down, but the Web application is up and you can successfully play back the Web transaction.

   Possible Cause: The Web application is only compatible with Internet Explorer or Mozilla-based browsers.

   Possible Solution: From the Service Tests and Beacons page, select the service test, and click **Edit**. Under **Advanced Properties**, set the **User Agent Header** as `Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) OracleEMAgentURLTiming/3.0.`

Note: For Enterprise Manager 10.2.0.4 and beyond, this User Agent Header is set automatically during Web transaction recording.

6. **Scenario**: Test Performance Page does not show any step metrics.

   Possible Cause: By default, only transaction-level metrics are collected.

   Possible Solution: From the Service Tests and Beacons page, select the service test, click **Edit**, and set **Data Granularity** to Step.

24

Introducing Enterprise Manager Support for SNMP

This chapter provides a brief overview of Enterprise Manager support for SNMP. It includes the following sections:

- Benefits of SNMP Support
- About the SNMP Management Station
- How Enterprise Manager Supports SNMP
- Sending SNMP Trap Notifications
- Monitoring External Devices Using SNMP
- About the Management Information Base (MIB)
- About Metric Extensions

The Simple Network Management Protocol (SNMP) is a protocol used for managing or monitoring devices, where many of these devices are network-type devices such as routers, switches, and so on. SNMP enables a single application to first retrieve information, then push new information between a wide range of systems independent of the underlying hardware.

Designed primarily for database, network, and system administrators, SNMP support integrates Enterprise Manager into a number of existing, widely-used management systems. Also, Enterprise Manager can extend its monitoring scope to devices that can be monitored using SNMP.

24.1 Benefits of SNMP Support

The primary benefits of SNMP support include the following:

- The monitoring of key Oracle products is quickly integrated into any management framework based upon SNMP.
- These Oracle products are located, identified, and monitored in real time across enterprise networks of any size.
- Administrators see standard Oracle icons that represent Oracle products in a network map. You can dynamically customize this map.
- Administrators see the current status of Oracle products, as shown by several status variables that are defined for each product in a management information base (MIB), or they can select which elements to view by their status.

- Administrators can anticipate exceptional conditions by defining thresholds and alerts, to respond to special situations as soon as they occur or to enable automatic responses.
- Administrators can store and analyze historical data that has been obtained through SNMP.
- Providers of management applications can easily build customized solutions for Oracle customers because SNMP is an open standard.

Strictly speaking, SNMP support is intended more for monitoring Oracle products than for managing them. SNMP support is invaluable for tracking the status of an entire network of Oracle applications — first, to verify normal operations, and second, to spot and react to potential problems as soon as they are detected. However, for purposes of investigating and solving some problems, other Oracle tools such as Oracle SQL *Plus Worksheet may be more appropriate. This is because SNMP support is designed to query status, but not to change system parameters, whereas other tools are designed to set or tune system parameters.

Note: Oracle SNMP is not supported on HP OpenVMS platform.

24.2 About the SNMP Management Station

The SNMP management station refers to a node from which managed elements are monitored using the SNMP protocol. Typically, it is a standalone workstation that is on the same network as the managed elements. While this book will consistently use the term SNMP management station, other terms used for it include management console, management system, or managing node.

Because most frameworks use SNMP as a basis for communication, Oracle products that support SNMP can be integrated into virtually every management framework. Third-party products such as CA Unicenter, HP OpenView, Tivoli NetView, Aprisma Spectrum, Sun Solstice, and Castle Rock SNMPc Network Manager provide SNMP Management Station functionality.

24.3 How Enterprise Manager Supports SNMP

Enterprise Manager supports SNMP by integrating with third-party management systems, sharing event information through SNMP traps and extending the monitoring scope of Enterprise Manager by monitoring new devices and targets using SNMP.

There are number of ways that Enterprise Manager uses SNMP as illustrated in Figure 24–1:

1. Sharing event information with third-party management systems by generating SNMP trap notifications from Enterprise Manager to an SNMP management station. For example, you can use SNMP to notify a third-party application that a selected metric has exceeded its threshold.

   This method supports SNMP version 1 (SNMPv1).

   For more information, see Section 24.4, "Sending SNMP Trap Notifications" and Chapter 4, "Using Notifications".

2. Extending the monitoring scope of Enterprise Manager to new entities by receiving SMNP traps or fetching SNMP data from or to the managed entity. By

developing a metadata plug-in to receive SNMP traps, you can enable Enterprise Manager to monitor a product capable of throwing SNMP traps.

This method supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2c), and SNMP version 3 (SNMPv3).

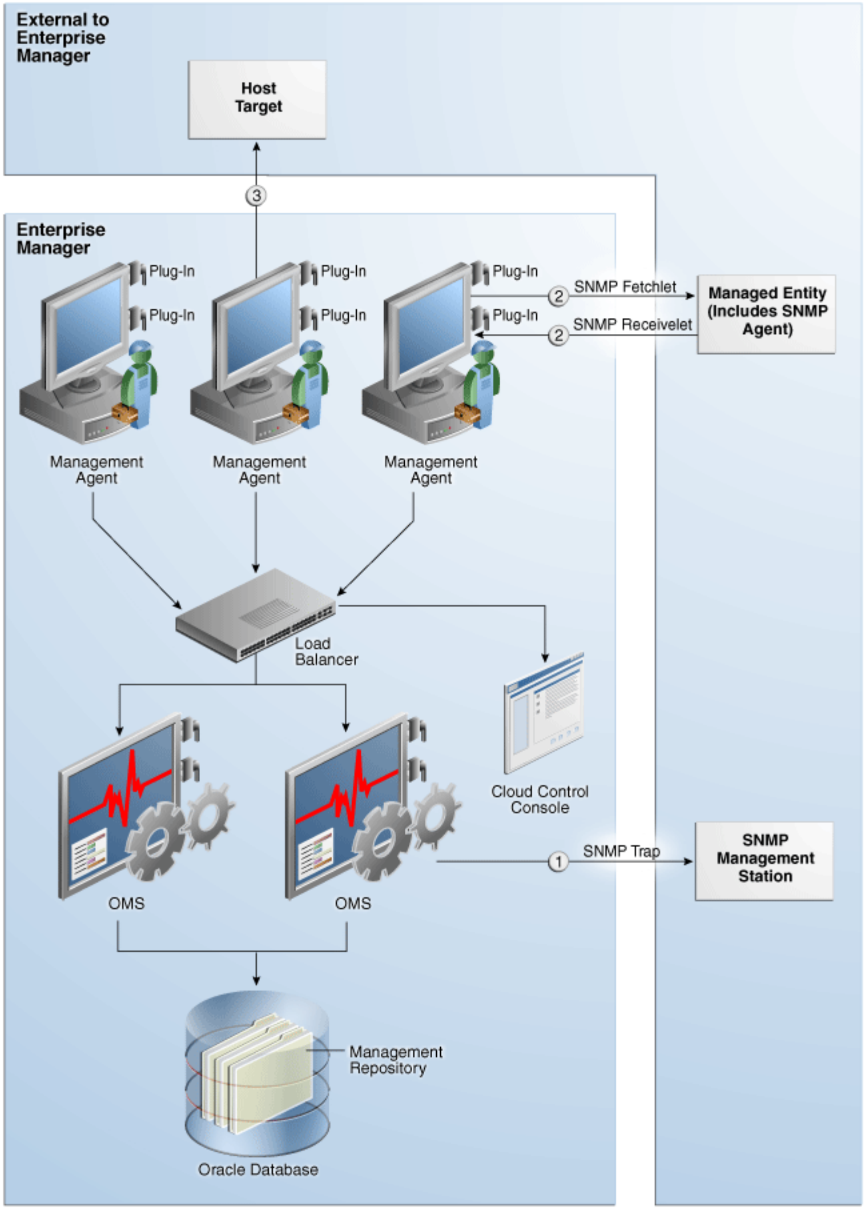
For more information, see Section 24.5, "Monitoring External Devices Using SNMP" and the *Oracle Enterprise Manager Cloud Control Extensibility Programmer's Reference*.

3. Creating new metrics to query SNMP agents by using SNMP adapters to allow Management Agents to query native SNMP agents on host targets for Management Information Base (MIB) variable information to be used as metric data.

   This method supports SNMP version 1 (SNMPv1), SNMP version 2 (SNMPv2c), and SNMP version 3 (SNMPv3).

   For more information, see Section 24.6, "About Metric Extensions" and Chapter 9, "Using Metric Extensions".

Figure 24–1 How Enterprise Manager Supports SNMP



24.4 Sending SNMP Trap Notifications

Using the Enterprise Manager notification system, you can share Enterprise Manager event information with other SNMP-enabled third-party applications through SNMP traps. Enterprise Manager supports the SNMPv1 protocol for sending traps. For example, you might want to send event information as traps to a third-party applications from Enterprise Manager when one of the following events takes place:

- a certain metric has exceeded a threshold (metric alert event)
- a target is down (target availability event)
- a job fails (job status change event)

Note: For a full list and description of Enterprise Manager event types, see Section 3.1.1, "Event Management".

Using SNMP traps with the notification system is a matter of:

1. Defining a notification method that uses an SNMP trap. For more information, see Section 4.5, "Sending SNMP Traps to Third Party Systems".
2. Assigning the notification method to a rule. You can edit an existing rule or create a new incident rule. For more information, see Section 3.2.4, "Setting Up Rule Sets".

24.4.1 About the Management Information Base (MIB)

While SNMP allows Enterprise Manager to send information to third-party SNMP-enabled applications, there might be situations where you want SNMP-enabled applications to obtain information from Enterprise Manager. This is accomplished with the help of MIB variables, and by signing up for SNMP traps. Details of the trap contents can be obtained from the MIB variables.

For more information about the MIB, see Section 4.6, "Management Information Base (MIB)" and Appendix A, "Interpreting Variables of the Enterprise Manager MIB".

Note: A valid Diagnostic Pack license is required to use the Enterprise Manager MIB variables.

24.5 Monitoring External Devices Using SNMP

It is often critical for an administrator to receive alerts from applications that are not managed by Enterprise Manager. Many of these applications can be configured to trigger SNMP traps when an alert condition takes place. You can receive these traps within Enterprise Manager and start monitoring those applications from Enterprise Manager. Having the capability to receive and analyze SNMP traps raised by such applications allows you extend Enterprise Manager's monitoring and alerting capabilities to these applications and reduce monitoring complexity in your IT environments.

You can configure Enterprise Manager to receive the SNMP traps raised by an application (not managed by Enterprise Manager) and display the traps as alerts in Enterprise Manager.

To receive these traps, you must develop a metadata plug-in to represent the managed entity. Then use an SNMP receivelet or SNMP fetchlet to receive or get monitoring data about that entity.

For more information about developing metadata plug-ins, see the *Oracle Enterprise Manager Cloud Control Extensibility Programmer's Reference*.

24.5.1 About SNMP Receivelets

While monitoring third-party entities in your managed environment, if the status of a third-party network element turns unavailable or if its metric severity conditions (metric thresholds) are met or exceeded, the SNMP Agent of that third-party network element sends a notification to the Management Agent. These notifications are in the form of SNMP traps that get triggered asynchronously upon reaching the performance thresholds, and without any requests from the Management Agent.

Since these traps are based on SNMP, the Management Agent uses SNMP Receivelets to receive and translate these SNMP traps into a form compatible with Oracle Management Service.

For more information about the SNMP receivelet, see the *Oracle Enterprise Manager Cloud Control Extensibility Programmer's Reference*.

24.5.2 About SNMP Fetchlets

Fetchlets are parameterized data access mechanisms available to map relevant data from a managed element into Enterprise Manager's metric format. In the standards area, Enterprise Manager currently uses SNMP Fetchlets to fetch information from SNMP-enabled entities within your managed environment.

The SNMP fetchlet queries the SNMP Agent for data about the managed entity as defined in the target type's Management Information Base (MIB). For more information about the MIB, see Section 24.4.1, "About the Management Information Base (MIB)" and Section 4.6, "Management Information Base (MIB)".

For more information about the SNMP fetchlet, see the *Oracle Enterprise Manager Cloud Control Extensibility Programmer's Reference*.

24.6 About Metric Extensions

Metric extensions provide you with the ability to extend Oracle's monitoring capabilities to monitor conditions specific to your IT environment. For example, you can create a new metric for a host target type. Use an SNMP Adapter to allow Enterprise Manager Management Agents to query native SNMP agents on target hosts for Management Information Base (MIB) variable information to be used as the metric data.

For more information about Metric Extensions and the SNMP Adapter, see Chapter 9, "Using Metric Extensions".

Part III

Security

This section contains the following chapter:

25 Configuring Security

For information about Enterprise Manager Cloud Control Security, see:

Oracle® Enterprise Manager Cloud Control Security Guide

12*c* Release 4 (12.1.0.4)

Part IV

Generating Reports

This section contains the following chapters:

26

Using Information Publisher

Information Publisher, Enterprise Manager’s reporting framework, makes information about your managed environment available to audiences across your enterprise. Strategically, reports are used to present a view of enterprise monitoring information for business intelligence purposes, but can also serve an administrative role by showing activity, resource utilization, and configuration of managed targets. IT managers can use reports to show availability of sets of managed systems. Executives can view reports on availability of applications (such as corporate email) over a period of time.

> **Note:** The Information Publisher (IP) reporting framework is still supported for Enterprise Manager 12c, however, new report development using this framework has been deprecated for Enterprise Manager 12c.

The reporting framework allows you to create and publish customized reports: Intuitive HTML-based reports can be published via the Web, stored, or e-mailed to selected recipients. Information Publisher comes with a comprehensive library of predefined reports that allow you to generate reports out-of-box without additional setup and configuration.

This chapter covers the following topics:

- About Information Publisher
- Out-of-Box Report Definitions
- Custom Reports
- Scheduling Reports
- Sharing Reports

26.1 About Information Publisher

Information Publisher provides powerful reporting and publishing capability. Information Publisher reports present an intuitive interface to critical decision-making information stored in the Management Repository while ensuring the security of this information by taking advantage of Enterprise Manager’s security and access control.

Information Publisher’s intuitive user-interface allows you to create and publish reports with little effort. The key benefits of using Information Publisher are:

- Provides a framework for creating content-rich, well-formatted HTML reports based on Management Repository data.

- Out-of-box reports let you start generating reports immediately without any system configuration or setup.
- Ability to schedule automatic generation of reports and store scheduled copies and/or e-mail them to intended audiences.
- Ability for Enterprise Manager administrators to share reports with the entire business community: executives, customers, and other Enterprise Manager administrators.

Information Publisher provides you with a feature-rich framework that is your central information source for your enterprise.

26.2 Out-of-Box Report Definitions

The focal point of Information Publisher is the report definition. A report definition tells the reporting framework how to generate a specific report by defining report properties such as report content, user access, and scheduling of report generation.

Information Publisher comes with a comprehensive library of predefined report definitions, allowing you to generate fully formatted HTML reports presenting critical operations and business information without any additional configuration or setup. .

Generating this HTML report involved three simple steps:

Step 1: Click **Availability History** (Group) in the report definition list.

Step 2: Select the group for which you want to run the report.

Step 3: Click **Continue** to generate the fully-formed report.

Supplied report definitions are organized by functional category with each category covering key areas.

To access the Information Publisher home page, from the **Enterprise** menu, choose **Reports** and then **Information Publisher**.

26.3 Custom Reports

Although the predefined report definitions that come with Information Publisher cover the most common reporting needs, you may want to create specialized reports. If a predefined report comes close to meeting your information requirements, but not quite, you can use Information Publisher's Create Like function to create a new report definition based on one of the existing reports definitions.

26.3.1 Creating Custom Reports

To create custom reports:

1. Choose whether to modify an existing report definition or start from scratch. If an existing report definition closely matches your needs, it is easy to customize it by using the Create Like function.
2. Specify name, category, and sub-category. Cloud Control provides default categories and sub-categories that are used for out-of-box reports. However, you can categorize custom reports in any way you like.
3. Specify any time-period and/or target parameters. The report viewer will be prompted for these parameters while viewing the report.

4. Add reporting elements. Reporting elements are pre-defined content building blocks, that allow you to add a variety of information to your report. Some examples of reporting elements are charts, tables, and images.
5. Customize the report layout. Once you have assembled the reporting elements, you can customize the layout of the report.

26.3.2 Report Parameters

By declaring report parameters, you allow the user to control what data is shown in the report. There are two types of parameters: target and time-period.

Example: If you are defining a report that will be used to diagnose a problem (such as a memory consumption report), the viewer will be able to see information for their target of interest.

By specifying the time-period parameter, the viewer will be able to analyze historical data for their period of interest.

Analyzing Historical Data

Information Publisher allows you to view reports for a variety of time-periods:

- Last 24 Hours/ 7 Days/ 31 Days
- Previous X Days/ Weeks/ Months/ Years (calendar units)
- This Week/ This Month/ This Year (this week so far)
- Any custom date range.

26.3.3 Report Elements

Report elements are the building blocks of a report definition. In general, report elements take parameters to generate viewable information. For example, the Chart from SQL element takes a SQL query to extract data from the Management Repository and a parameter specifying whether to display the data in the form of a pie, bar, or line chart. Report elements let you "assemble" a custom report definition using the Information Publisher user interface.

Information Publisher provides a variety of reporting elements. Generic reporting elements allow you to display any desired information, in the form of charts, tables or images. For example, you can include your corporate Logo, with a link to your corporate Web site. Monitoring elements show monitoring information, such as availability and alerts for managed targets. Service Level Reporting elements show availability, performance, usage and achieved service levels, allowing you to track compliance with Service Level Agreements, as well as share information about achieved service levels with your customers and business executives.

26.4 Scheduling Reports

Enterprise manager allows you to view reports interactively and/or schedule generation of reports on a flexible schedule. For example, you might want to generate an "Inventory Snapshot" report of all of the servers in your environment every day at midnight.

26.4.1 Flexible Schedules

Cloud Control provides the following scheduling options:

- One-time report generation either immediately or at any point in the future
- Periodic report generation
  - Frequency: Any number of Minutes/ Hours/ Days/ Weeks/ Months/ Years
  - You can generate copies indefinitely or until a specific date in the future.

26.4.2 Storing and Purging Report Copies

Enterprise Manager allows you to store any number of scheduled copies for future reference.

You can delete each stored copy manually or you can set up automated purging based on either the number of stored copies or based on retention time. For example, you can have Enterprise Manager purge all reports that are more than 90 days old.

26.4.3 E-mailing Reports

You can choose for scheduled reports to be e-mailed to any number of recipients. You can specify reply-to address and subject of the e-mail.

26.5 Sharing Reports

Information Publisher facilitates easy report sharing with the entire user community. Enterprise Manager administrators can share reports with other administrators and roles. However, there may be cases when you need to share reports with non-Enterprise Manager administrators, such as customers and/or business executives. To facilitate information sharing with these users, Enterprise Manager renders a separate reporting Web site that does not require user authentication.

Note: To ensure that no sensitive information is compromised, only Enterprise Manager administrators with a special system privilege are allowed to publish reports to the Enterprise Manager reports Web site.

Information Publisher honors Enterprise Manager roles and privileges, ensuring that only Enterprise Manager administrators can create reports on the information they are allowed to see.

When sharing reports, administrators have an option of allowing report viewers to see the report with the owner's privileges. For example, as a system administrator you might want to share a host’s performance information with a DBA using your server, but you do not want to grant the DBA any privileges on your host target. In this case, you could create a host performance report, and allow the DBA to view it with your privileges. This way, they only see the information you want them to see, without having access to the host homepage.

27 Creating Usage Tracking Reports

Usage Tracking Reports provides an overview of the Database features that are identified as being used by your organization.

> **Important:** Usage Tracking Reports are intended for informational purposes only and do not represent your license entitlements or requirements. To understand your license requirements, contact the License Management Services representative at:
>
> `http://www.oracle.com/us/corporate/license-management-services/index.html`

This chapter covers the following topics:

- Usage Tracking Reports
- Collecting Data for Database Usage Tracking
- Generating Database Usage Tracking Report
- Database Usage Tracking Summary Report
- Fusion Middleware Usage Tracking Summary Report

27.1 Usage Tracking Reports

Usage Tracking Reports are Oracle-supplied reports that are available with Oracle Business Intelligence Publisher (BI Publisher), the primary reporting system that provides a single, Web-based platform for authoring, managing, and delivering interactive reports and all types of highly formatted documents. The procedures detailed in this chapter assume that you have already integrated BI Publisher into Enterprise Manager. For instructions on integrating BI Publisher with Enterprise Manager, see "Integrating BI Publisher with Enterprise Manager" in the Oracle® Enterprise Manager Cloud Control Advanced Installation and Configuration Guide.

There are two Usage Tracking Reports:

- *Database Usage Tracking Summary Report* is a high level summary of the Database Version, Edition, licensable Options and Enterprise Management Pack usage.

  This report can be run and viewed online. The output report can be exported to PDF, RTF, Excel formats.

- *Database Usage Tracking Report* provides the above usage data in an exportable (csv) format. The exported data can be sent to Oracle License Management Services for further analysis to determine licensing requirements. Please contact the License Management Services representative at http://www.oracle.com/us/corporate/license-management-services/index.html to initiate an engagement.

This report cannot be run online and can only be scheduled. A single file for each database instance will be generated each time the report is scheduled to run. The format of the output files is comma separated values (CSV).

Creating Usage Tracking Reports consists of the following high-level tasks:

1. Setting up Database Usage Tracking credentials. (Required for both *Database Usage Tracking Summary Report* and *Database Usage Tracking Report*.)
2. Enabling the metric collection (via monitoring templates. (Required for both *Database Usage Tracking Summary Report* and *Database Usage Tracking Report*.)
3. Configuring the FTP Server (where reports are to be generated) in BI Publisher. (Not required for the Database Usage Tracking Summary Report.)
4. Generating the Usage Tracking Reports.

27.2 Collecting Data for Database Usage Tracking

Prior to producing the Database Usage Tracking Report, corresponding Metric Collections must be configured and enabled. This includes the following steps:

1. Setting Database Usage Tracking Credentials
2. Enabling or disabling (when the collection is finished) the Metric Collection. Depending on the preferences and available licensing, this can be done:
   - Using Monitoring Templates, from the OEM console, for the database targets which are licensed with Diagnostics Pack.
   - Using EM Command Line Interface (EM CLI), for any database target, regardless of the licensing.

There are two types of metric collections:

- Weekly metrics - to be collected once in 7 days: lms_wk_ci and lms_wk_ci_cdb
- Hourly metrics - to be collected every hour: lms_hr_ci and lms_hr_ci_cdb

  This collection must me enabled only when session information is needed, and should be carefully monitored because of the amount of data that can be generated.

For each of these two types, there are two different metric collections:

- For standard traditional database targets: lms_wk_ci and lms_hr_ci
- For Container Database (CDB) targets: lms_wk_ci_cdb and lms_hr_ci_cdb, which collect data from CDB$ROOT container and also from all the Pluggable Databases (PDBs)

27.2.1 Setting Database Usage Tracking Credentials

1. Log in to Enterprise Manager. From the **Setup** menu, select **Security** and then Monitoring Credentials.
2. Choose the desired database target from the list and click **Manage Monitoring Credentials**. The target Credential page displays.

3. Choose the target name from the list and click Set Credentials. The Enter Monitoring Credentials dialog displays.

4. Enter the requisite monitoring credentials and click **Save**.

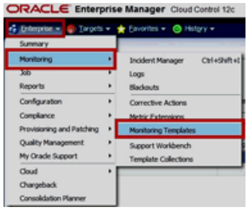
27.2.2 Enabling/Disabling the Metric Collection using Monitoring Templates

This method uses Monitoring Templates, a Diagnostics Pack feature, therefore can be used only on the database targets licensed with Diagnostics Pack.

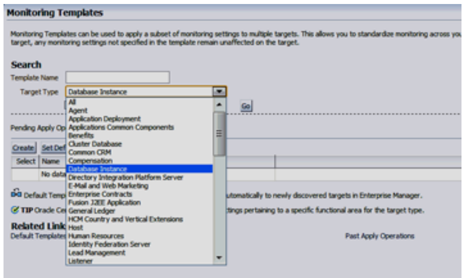
> **Note:** The use of monitoring templates for database targets is licensed under the Oracle Diagnostics Pack. You can also use the Enterprise Manager command line interface (EM CLI) to enable/disable metric collections which do not require an extra license.

Enabling the weekly metric collection:

1. From the **Enterprise** menu, select **Monitoring**, and then **Monitoring Templates**.



2. Choose **Database Instance** as target type, check **Display Oracle Certified Templates** and then click **Go**.

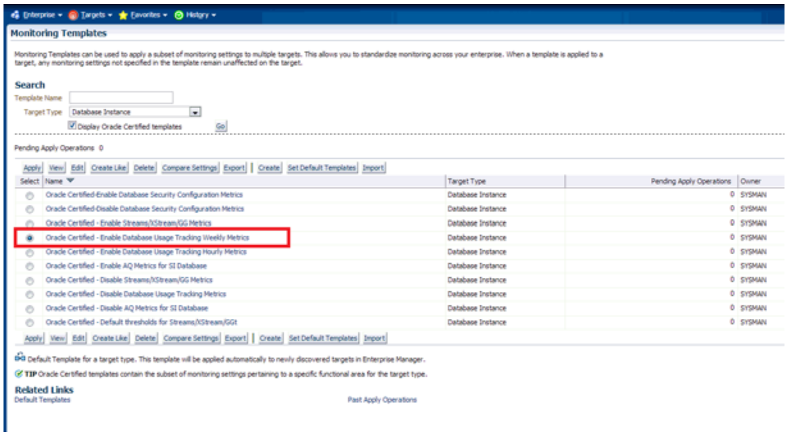


Monitoring Templates can be used to apply a subset of monitoring settings to multiple targets. This allows you to standardize monitoring across yo target, any monitoring settings not specified in the template remain unaffected on the target.

utomatically to newly discovered targets in Enterprise Manager.

tings pertaining to a specific functional area for the target type.

3. Chose **Oracle Certified - Enable Database Usage Tracking Weekly Metrics**, then click **Apply**.



Monitoring Templates can be used to apply a subset of monitoring settings to multiple targets. This allows you to standardize monitoring across your enterprise. When a template is applied to a target, any monitoring settings not specified in the template remain unaffected on the target.

Template Name

Target Type: Database Instance

☑ Display Oracle Certified templates

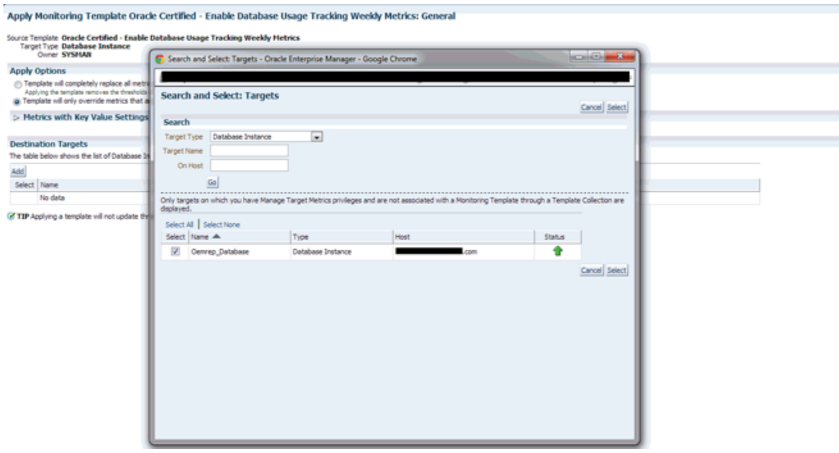
Pending Apply Operations 0

Select	Name	Target Type	Pending Apply Operations	Owner
○	Oracle Certified-Enable Database Security Configuration Metrics	Database Instance	0	SYSMAN
○	Oracle Certified-Disable Database Security Configuration Metrics	Database Instance	0	SYSMAN
○	Oracle Certified - Enable Streams/XStream/GG Metrics	Database Instance	0	SYSMAN
●	Oracle Certified - Enable Database Usage Tracking Weekly Metrics	Database Instance	0	SYSMAN
○	Oracle Certified - Enable Database Usage Tracking Hourly Metrics	Database Instance	0	SYSMAN
○	Oracle Certified - Enable AQ Metrics for SI Database	Database Instance	0	SYSMAN
○	Oracle Certified - Disable Streams/XStream/GG Metrics	Database Instance	0	SYSMAN
○	Oracle Certified - Disable Database Usage Tracking Metrics	Database Instance	0	SYSMAN
○	Oracle Certified - Disable AQ Metrics for SI Database	Database Instance	0	SYSMAN
○	Oracle Certified - Default thresholds for Streams/XStream/GGt	Database Instance	0	SYSMAN

Default Template for a target type. This template will be applied automatically to newly discovered targets in Enterprise Manager.

TIP Oracle Certified templates contain the subset of monitoring settings pertaining to a specific functional area for the target type.

4. From the new page, click **Add**. Choose the desired targets using check boxes and then click **Select**.



Apply Monitoring Template Oracle Certified - Enable Database Usage Tracking Weekly Metrics: General

Source Template **Oracle Certified - Enable Database Usage Tracking Weekly Metrics**
Target Type **Database Instance**
Owner **SYSMAN**

Apply Options

○ Template will completely replace all metr
Applying the template removes the thresholds
● Template will only override metrics that a

Destination Targets

The table below shows the list of Database In

Select	Name
	No data

TIP Applying a template will not update th

Search and Select: Targets - Oracle Enterprise Manager - Google Chrome

[redacted]

Search and Select: Targets

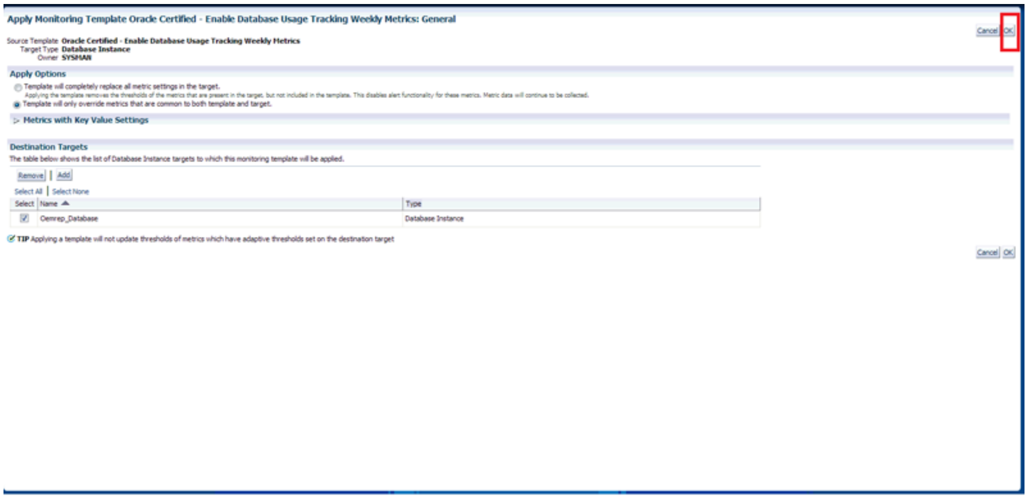
Search

Target Type: Database Instance
Target Name:
On Host:

Only targets on which you have Manage Target Metrics privileges and are not associated with a Monitoring Template through a Template Collection are displayed.

Select	Name	Type	Host	Status
☑	Oemrep_Database	Database Instance	[redacted].com	⬆

5. Click **OK** to finalize the changes.



Apply Monitoring Template Oracle Certified - Enable Database Usage Tracking Weekly Metrics: General

Source Template **Oracle Certified - Enable Database Usage Tracking Weekly Metrics**
Target Type **Database Instance**
Owner **SYSMAN**

Apply Options

○ Template will completely replace all metric settings in the target.
Applying the template removes the thresholds of the metrics that are present in the target, but not included in the template. This disables alert functionality for these metrics. Metric data will continue to be collected.
● Template will only override metrics that are common to both template and target.

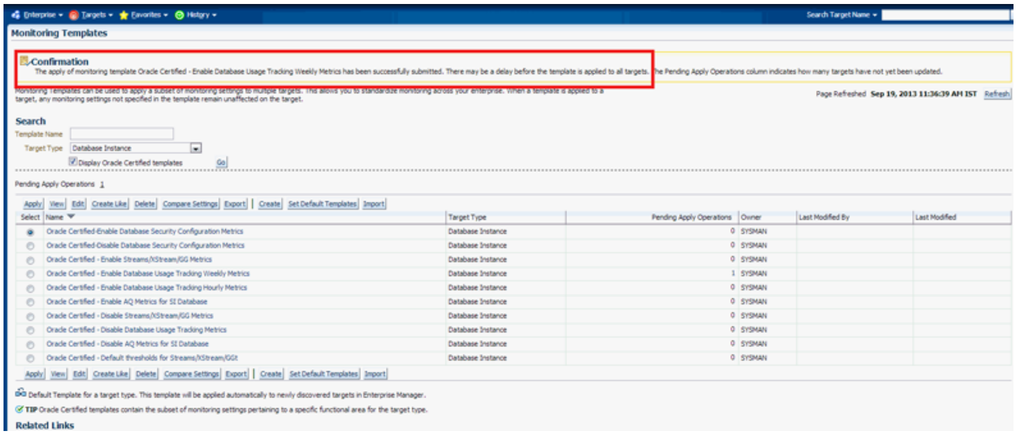
Destination Targets

The table below shows the list of Database Instance targets to which this monitoring template will be applied.

Select	Name	Type
☑	Oemrep_Database	Database Instance

TIP Applying a template will not update thresholds of metrics which have adaptive thresholds set on the destination target

6. Verify the confirmation message and **Pending Apply Operations** column that shows the number of targets that have not yet been updated. Make sure there are no ("0") pending apply operations.



Monitoring Templates

Confirmation
The apply of monitoring template Oracle Certifed - Enable Database Usage Tracking Weekly Metrics has been successfully submitted. There may be a delay before the template is applied to all targets. The Pending Apply Operations column indicates how many targets have not yet been updated.

Monitoring Templates can be used to apply a subset of monitoring settings to multiple targets. This allows you to standardize monitoring across your enterprise. When a template is applied to a target, any monitoring settings not specified in the template remain unaffected on the target.

Page Refreshed **Sep 19, 2013 11:36:39 AM IST**

Search

Template Name:
Target Type: Database Instance
☑ Display Oracle Certifed templates

Pending Apply Operations 1

Select	Name	Target Type	Pending Apply Operations	Owner	Last Modified By	Last Modified
●	Oracle Certified-Enable Database Security Configuration Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified-Disable Database Security Configuration Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Enable Streams/XStream/GG Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Enable Database Usage Tracking Weekly Metrics	Database Instance	1	SYSMAN		
○	Oracle Certified - Enable Database Usage Tracking Hourly Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Enable AQ Metrics for SI Database	Database Instance	0	SYSMAN		
○	Oracle Certified - Disable Streams/XStream/GG Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Disable Database Usage Tracking Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Disable AQ Metrics for SI Database	Database Instance	0	SYSMAN		
○	Oracle Certified - Default thresholds for Streams/XStream/GGt	Database Instance	0	SYSMAN		

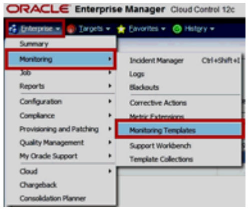
Default Template for a target type. This template will be applied automatically to newly discovered targets in Enterprise Manager.

TIP Oracle Certified templates contain the subset of monitoring settings pertaining to a specific functional area for the target type.

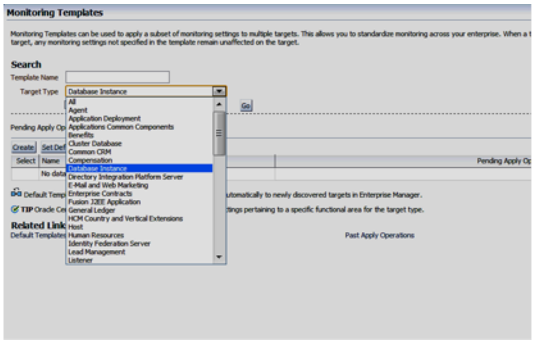
Related Links

Enabling the hourly metric collection:

1. From the **Enterprise** menu, select **Monitoring**, and then **Monitoring Templates**.



2. Choose **Database Instance** as the target type, check **Display Oracle Certified Templates** and click **Go**.


Monitoring Templates

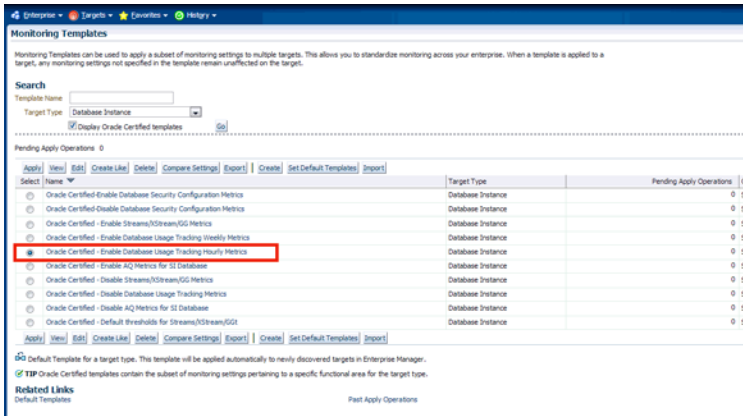
Monitoring Templates can be used to apply a subset of monitoring settings to multiple targets. This allows you to standardize monitoring across your enterprise. When a t target, any monitoring settings not specified in the template remain unaffected on the target.

Search

Template Name

Target Type: Database Instance

3. Choose **Oracle Certified - Enable Database Usage Tracking Hourly Metrics**, then click **Apply**.



Monitoring Templates

Monitoring Templates can be used to apply a subset of monitoring settings to multiple targets. This allows you to standardize monitoring across your enterprise. When a template is applied to a target, any monitoring settings not specified in the template remain unaffected on the target.

Search

Template Name

Target Type: Database Instance

☑ Display Oracle Certified templates Go

Pending Apply Operations 0

Apply | View | Edit | Create Like | Delete | Compare Settings | Export | Create | Set Default Templates | Import

Select	Name	Target Type	Pending Apply Operations
○	Oracle Certified-Enable Database Security Configuration Metrics	Database Instance	0
○	Oracle Certified-Disable Database Security Configuration Metrics	Database Instance	0
○	Oracle Certified - Enable Streams/XStream/GG Metrics	Database Instance	0
○	Oracle Certified - Enable Database Usage Tracking Weekly Metrics	Database Instance	0
●	Oracle Certified - Enable Database Usage Tracking Hourly Metrics	Database Instance	0
○	Oracle Certified - Enable AQ Metrics for SI Database	Database Instance	0
○	Oracle Certified - Disable Streams/XStream/GG Metrics	Database Instance	0
○	Oracle Certified - Disable Database Usage Tracking Metrics	Database Instance	0
○	Oracle Certified - Disable AQ Metrics for SI Database	Database Instance	0
○	Oracle Certified - Default thresholds for Streams/XStream/GGt	Database Instance	0

Apply | View | Edit | Create Like | Delete | Compare Settings | Export | Create | Set Default Templates | Import

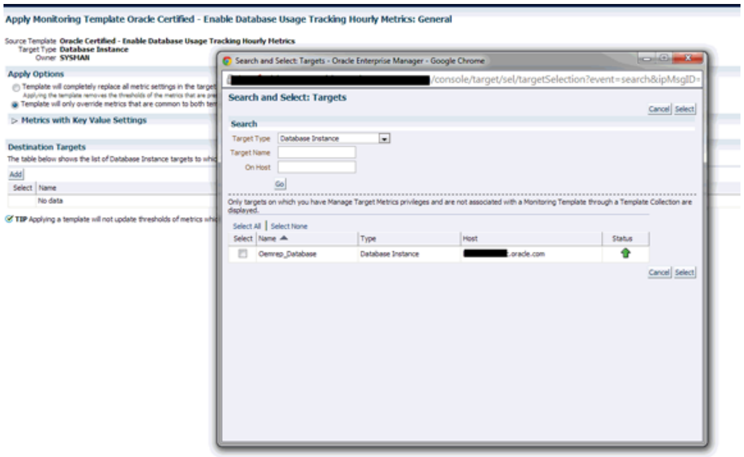
Default Template for a target type. This template will be applied automatically to newly discovered targets in Enterprise Manager.

TIP Oracle Certified templates contain the subset of monitoring settings pertaining to a specific functional area for the target type.

Related Links

Default Templates　Past Apply Operations

4. Click **Add** and then choose the desired targets.



Apply Monitoring Template Oracle Certified - Enable Database Usage Tracking Hourly Metrics: General

Source Template **Oracle Certified - Enable Database Usage Tracking Hourly Metrics**
Target Type **Database Instance**
Owner **SYSMAN**

Apply Options

○ Template will completely replace all metric settings in the target
Applying the template removes the thresholds of the metrics that are pre
● Template will only override metrics that are common to both tem

▷ **Metrics with Key Value Settings**

Destination Targets

The table below shows the list of Database Instance targets to whic

Add

Select	Name
	No data

TIP Applying a template will not update thresholds of metrics whi

Search and Select: Targets - Oracle Enterprise Manager - Google Chrome

[redacted]/console/target/sel/targetSelection?event=search&ipMsgID=

Search and Select: Targets

Cancel Select

Search

Target Type: Database Instance
Target Name:
On Host:
Go

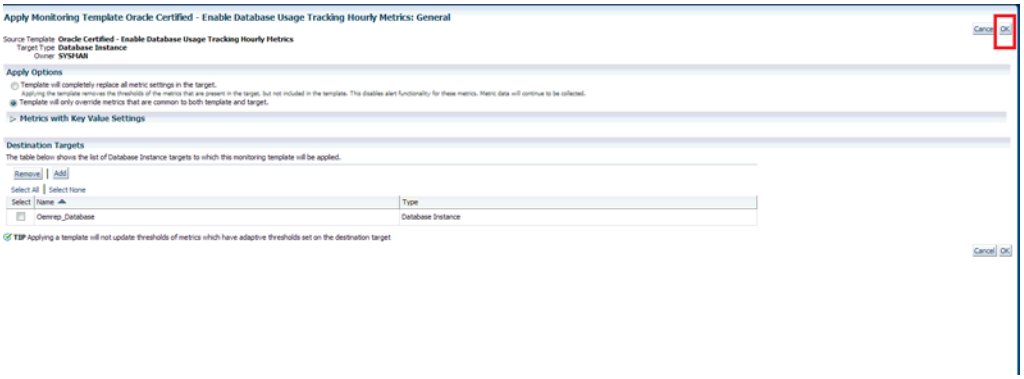
Only targets on which you have Manage Target Metrics privileges and are not associated with a Monitoring Template through a Template Collection are displayed.

Select All | Select None

Select	Name ▲	Type	Host	Status
□	Oemrep_Database	Database Instance	[redacted].oracle.com	⬆

Cancel Select

5. Click **OK** to finalize the changes.



Apply Monitoring Template Oracle Certified - Enable Database Usage Tracking Hourly Metrics: General

Cancel OK

Source Template **Oracle Certified - Enable Database Usage Tracking Hourly Metrics**
Target Type **Database Instance**
Owner **SYSMAN**

Apply Options

○ Template will completely replace all metric settings in the target.
Applying the template removes the thresholds of the metrics that are present in the target, but not included in the template. This disables alert functionality for these metrics. Metric data will continue to be collected.
● Template will only override metrics that are common to both template and target.

▷ **Metrics with Key Value Settings**

Destination Targets

The table below shows the list of Database Instance targets to which this monitoring template will be applied.

Remove | Add

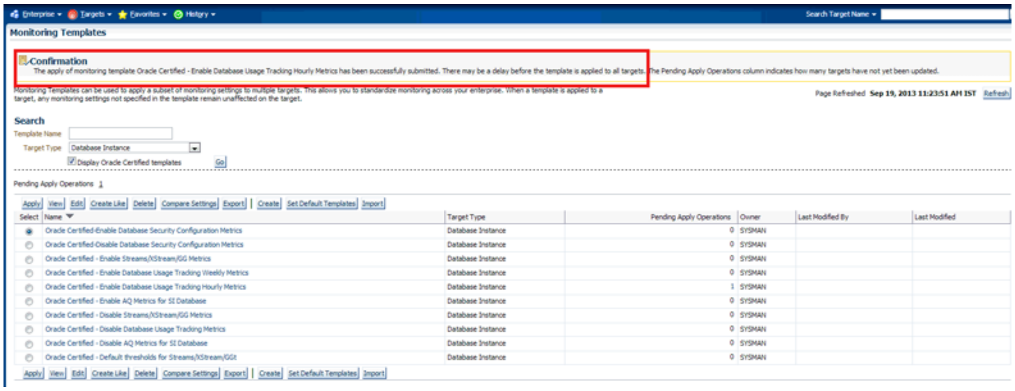
Select All | Select None

Select	Name ▲	Type
□	Oemrep_Database	Database Instance

TIP Applying a template will not update thresholds of metrics which have adaptive thresholds set on the destination target

Cancel OK

6. A confirmation message displays at the top of the page.



Monitoring Templates

Confirmation
The apply of monitoring template Oracle Certified - Enable Database Usage Tracking Hourly Metrics has been successfully submitted. There may be a delay before the template is applied to all targets. The Pending Apply Operations column indicates how many targets have not yet been updated.

Monitoring Templates can be used to apply a subset of monitoring settings to multiple targets. This allows you to standardize monitoring across your enterprise. When a template is applied to a target, any monitoring settings not specified in the template remain unaffected on the target.

Page Refreshed **Sep 19, 2013 11:23:51 AM IST** Refresh

Search

Template Name:
Target Type: Database Instance
☑ Display Oracle Certified templates Go

Pending Apply Operations 1

Apply | View | Edit | Create Like | Delete | Compare Settings | Export | Create | Set Default Templates | Import

Select	Name ▼	Target Type	Pending Apply Operations	Owner	Last Modified By	Last Modified
●	Oracle Certified-Enable Database Security Configuration Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified-Disable Database Security Configuration Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Enable Streams/XStream/GG Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Enable Database Usage Tracking Weekly Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Enable Database Usage Tracking Hourly Metrics	Database Instance	1	SYSMAN		
○	Oracle Certified - Enable AQ Metrics for SI Database	Database Instance	0	SYSMAN		
○	Oracle Certified - Disable Streams/XStream/GG Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Disable Database Usage Tracking Metrics	Database Instance	0	SYSMAN		
○	Oracle Certified - Disable AQ Metrics for SI Database	Database Instance	0	SYSMAN		
○	Oracle Certified - Default thresholds for Streams/XStream/GGt	Database Instance	0	SYSMAN		

Apply | View | Edit | Create Like | Delete | Compare Settings | Export | Create | Set Default Templates | Import

Disabling Usage Tracking Metric Collection:

1. Follow the steps 1 and 2 as show in the previous section.
2. In Step 3, choose **Oracle Certified - Disable Database Usage Tracking Metrics**, which disables both hourly and weekly collections.
3. Follow steps 4 to 6 from the previous section.

27.2.3 Enabling/Disabling the Metric Collection using the Command Line Interface

In the previous section, "Enabling/Disabling the Metric Collection using Monitoring Templates" on page 27-3, you performed these actions using the Enterprise Manager Cloud Control console for database targets licensed with Diagnostics Pack. However, you can also use the Enterprise Manager command line interface (EM CLI) to enable/disable metric collection from the operating system command line, in which case no extra licensing is required.

The following topics are covered in this section:

- Setting up EM CLI login
- Enabling/disabling the metric collection
- Using EM CLI to list all the database targets
- Using SQL to verify collection status

27.2.3.1 Setting up EM CLI login

Before running the EM CLI commands to enable/disable metric collection, the EM CLI login must be configured.This is typically done by specifying the URL, username, and password as shown in the following example:

```
emcli setup -url="https://jupiter.solarsystem.com:7799/em" -username=sysman
-password=manager -trustall
```

27.2.3.2 Enabling/disabling the metric collection

Metric collection is enabled/disabled using the EM CLI `modify_collection_schedule` verb. This verb is fully documented in the Oracle Enterprise Manager Command Line Interface Guide.

The following syntax must be use for Database Usage Tracking purposes:

```
emcli modify_collection_schedule
        -targetType="oracle_database"
        -targetNames="tname1;tname2;tname3;..."
        -collectionName="lms_wk_ci_cdb|lms_hr_ci_cdb|lms_wk_ci|lms_hr_ci"
        -freqType="HOUR|DAY|WEEKLY"
        -freqValue="1|7| MON|TUE|WED|THU|FRI|SAT|SUN"
        -collectionStatus="ENABLED|DISABLED"
        -preview="N"
```

Parameters

- **targetNames**

  The target name should be the same as exists in the repository. All of the targets should be the same target type you specified in the targetType parameter. Use a semicolon (;) to separate the names. Changes to the collection schedule will be executed for only valid target name and target type combinations. For example:`tname1;tname2;tname3`

- **collectionName**

  Name of one of the four metric collections predefined for Database Usage Tracking. "wk" indicates weekly collection while "hr" indicates the hourly collection. "_cdb" suffix indicates that the collection is to be applied only to CDB database targets.

  – lms_hr_ci_cdb and lms_wk_ci_cdb - must be applied to all CDB database targets (with PDBs)

  - lms_hr_ci and lms_wk_ci - must be applied to all the rest of database targets

- **freqType** and **freqValue**

  Indicate the frequency. These two parameters are not needed or ignored (if provided) in the case of collectionStatus="DISABLED".

  These parameters can be one of the following:

  - freqType=HOUR freqValue=1
  - freqType= DAYS freqValue=7
  - freqType=WEEKLY freqValue=MON (or any other weekday)

- **collectionStatus**

  Enables or disables the collection. The default is Enabled. If Disabled, freqType and freqValue are ignored.

Usage Examples

- Enabling weekly metrics on a CDB database target.

```
emcli modify_collection_schedule \
        -targetType="oracle_database" \
        -targetNames="targetdb3" \
        -collectionName="lms_wk_ci_cdb" \
        -freqType="DAY" \
        -freqValue="7" \
        -collectionStatus="ENABLED" \
        -preview="N"
```

  Note: On MS Windows, replace "\" with the Windows-specific command line continuation character: "^".

- Enabling weekly metrics on a multiple non-CDB database targets.

```
emcli modify_collection_schedule \
        -targetType="oracle_database" \
        -targetNames="targetdb1;targetdb2" \
        -collectionName="lms_wk_ci" \
        -freqType="WEEKLY" \
        -freqValue="SUN" \
        -collectionStatus="ENABLED" \
        -preview="N"
```

- Disabling weekly metrics on a CDB database target.

```
emcli modify_collection_schedule \
        -targetType="oracle_database" \
        -targetNames="targetdb3" \
        -collectionName="lms_wk_ci_cdb" \
        -collectionStatus="DISABLED" \
        -preview="N"
```

- Disabling weekly metrics on multiple non-CDB database targets.

```
emcli modify_collection_schedule \
        -targetType="oracle_database" \
        -targetNames="targetdb1;targetdb2" \
        -collectionName="lms_wk_ci" \
        -collectionStatus="DISABLED" \
        -preview="N"
```

- Enabling hourly metrics on a CDB database target.

  ```
  emcli modify_collection_schedule \
          -targetType="oracle_database" \
          -targetNames="targetdb3" \
          -collectionName="lms_hr_ci_cdb" \
          -freqType="DAY" \
          -freqValue="7" \
          -collectionStatus="ENABLED" \
          -preview="N"
  ```

- Enabling hourly metrics on a multiple non-CDB database targets.

  ```
  emcli modify_collection_schedule \
          -targetType="oracle_database" \
          -targetNames="targetdb1;targetdb2" \
          -collectionName="lms_hr_ci" \
          -freqType="WEEKLY" \
          -freqValue="SUN" \
          -collectionStatus="ENABLED" \
          -preview="N"
  ```

- Disabling hourly metrics on a CDB database target.

  ```
  emcli modify_collection_schedule \
          -targetType="oracle_database" \
          -targetNames="targetdb3" \
          -collectionName="lms_hr_ci_cdb" \
          -collectionStatus="DISABLED" \
          -preview="N"
  ```

- Disabling hourly metrics on multiple non-CDB database targets.

  ```
  emcli modify_collection_schedule \
          -targetType="oracle_database" \
          -targetNames="targetdb1;targetdb2" \
          -collectionName="lms_hr_ci" \
          -collectionStatus="DISABLED" \
          -preview="N"
  ```

27.2.3.3 Using EM CLI to list all the database targets

During the configuration process, it might be useful to list all the database targets in order to make sure that none are missed.

To list all database targets, run the following EM CLI command:

```
emcli get_targets -targets="oracle_database"
```

27.2.3.4 Using SQL to verify collection status

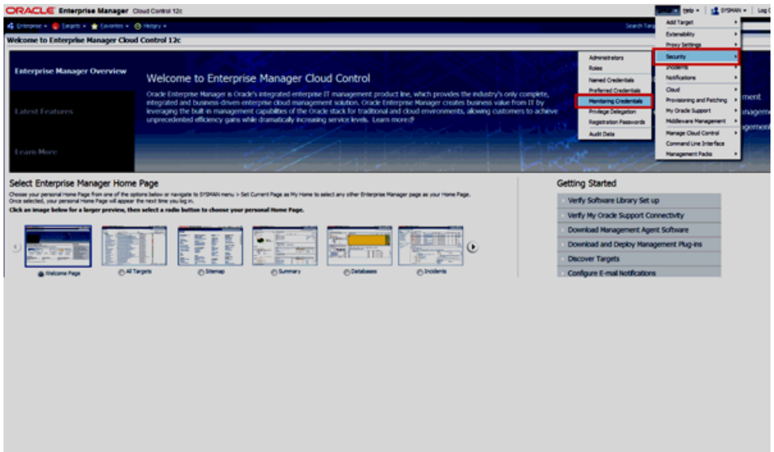
The following SQL query can be run on OEM Repository to list the collection status and schedules assigned to the database targets.

```
select
       t.TARGET_NAME,
       c.COLL_NAME,
       c.IS_ENABLED,
       c.SCHEDULE_EX
  from      SYSMAN.MGMT_TARGETS          t
  left join SYSMAN.MGMT_COLLECTIONS c on t.TARGET_GUID = c.OBJECT_GUID and c.COLL_
NAME like 'lms_%_ci%'
  where t.target_type = 'oracle_database'
```

```
order by t.TARGET_NAME, c.COLL_NAME;
```

27.2.4 Creating a Database Usage Tracking Report

1. Log in to Enterprise Manager. From the **Setup** menu, select **Security** and then **Monitoring Credentials**.



Welcome to Enterprise Manager Cloud Control

Oracle Enterprise Manager is Oracle's integrated enterprise IT management product line, which provides the industry's only complete, integrated and business-driven enterprise cloud management solution. Oracle Enterprise Manager creates business value from IT by leveraging the built-in management capabilities of the Oracle stack for traditional and cloud environments, allowing customers to achieve unprecedented efficiency gains while dramatically increasing service levels. Learn more

Select Enterprise Manager Home Page

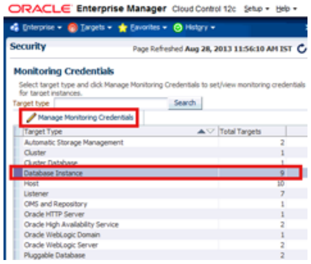
Choose your personal Home Page from one of the options below or navigate to SYSMAN menu > Set Current Page as My Home to select any other Enterprise Manager page as your Home Page. Once selected, your personal Home Page will appear the next time you log in.

Click an image below for a larger preview, then select a radio button to choose your personal Home Page.

Getting Started

- Verify Software Library Set up
- Verify My Oracle Support Connectivity
- Download Management Agent Software
- Download and Deploy Management Plug-ins
- Discover Targets
- Configure E-mail Notifications

2. Choose the **Database Instance** target type and click **Manage Monitoring Credentials**.


ORACLE Enterprise Manager Cloud Control 12c
Setup
Help
Enterprise
Targets
Favorites
History
Search
Manage Monitoring Credentials

Security

Page Refreshed **Aug 28, 2013 11:56:10 AM IST**

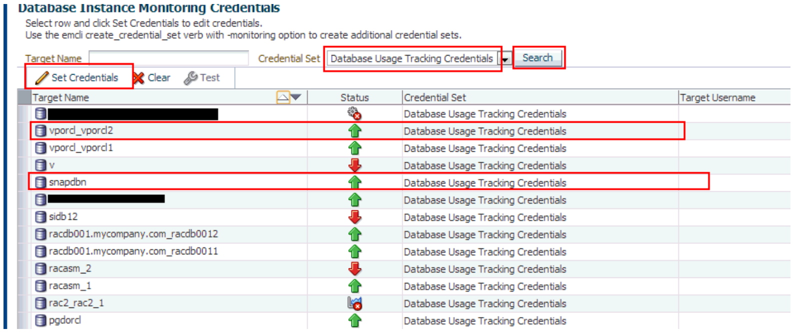
Monitoring Credentials

Select target type and click Manage Monitoring Credentials to set/view monitoring credentials for target instances.

Target type

Target Type	Total Targets
Automatic Storage Management	2
Cluster	1
Cluster Database	1
Database Instance	9
Host	10
Listener	7
OMS and Repository	1
Oracle HTTP Server	1
Oracle High Availability Service	2
Oracle WebLogic Domain	1
Oracle WebLogic Server	2
Pluggable Database	2

3. Select **Database Usage Tracking Credentials** entry in the Credential Set list and click **Search**.



Database Instance Monitoring Credentials

Select row and click Set Credentials to edit credentials.
Use the emcli create_credential_set verb with -monitoring option to create additional credential sets.

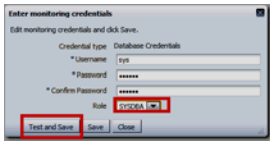
Target Name   Credential Set: Database Usage Tracking Credentials

Target Name	Status	Credential Set	Target Username
[redacted]		Database Usage Tracking Credentials	
vporcl_vporcl2	↑	Database Usage Tracking Credentials	
vporcl_vporcl1	↑	Database Usage Tracking Credentials	
v	↓	Database Usage Tracking Credentials	
snapdbn	↑	Database Usage Tracking Credentials	
[redacted]	↑	Database Usage Tracking Credentials	
sidb12	↓	Database Usage Tracking Credentials	
racdb001.mycompany.com_racdb0012	↑	Database Usage Tracking Credentials	
racdb001.mycompany.com_racdb0011	↑	Database Usage Tracking Credentials	
racasm_2	↓	Database Usage Tracking Credentials	
racasm_1	↑	Database Usage Tracking Credentials	
rac2_rac2_1		Database Usage Tracking Credentials	
pgdorcl	↑	Database Usage Tracking Credentials	

Click on the row for the desired target and then click **Set Credentials**.

> **Important:** This operation needs to be performed for all the Database Instances.

4. Enter the username and password for a database user with SYSDBA privilege.



Enter monitoring credentials

Edit monitoring credentials and click Save.

Credential type: Database Credentials

* Username: sys

* Password: •••••••

* Confirm Password: •••••••

Role: SYSDBA

5. Alternate method: Use the Enterprise Manager command line utility (EM CLI) to make the above settings as shown in the following examples.

Example 27–1 Multiple Targets

```
emcli set_monitoring_credential -target_names="testdb1;testdb2" -target_
type=oracle_database -set_name=DBCredsLMSMonitoring
-cred_type=DBCreds
-attributes="DBUserName:<USERNAME>;DBPassword:<PASSWORD>;DBRole:SYSDBA"
```

Example 27–2 Single Target

```
emcli set_monitoring_credential -target_name=Oemrep_Database -target_type=oracle_
database -set_name=DBCredsLMSMonitoring
-cred_type=DBCreds
-attributes="DBUserName:<USERNAME>;DBPassword:<PASSWORD>;DBRole:SYSDBA"
```

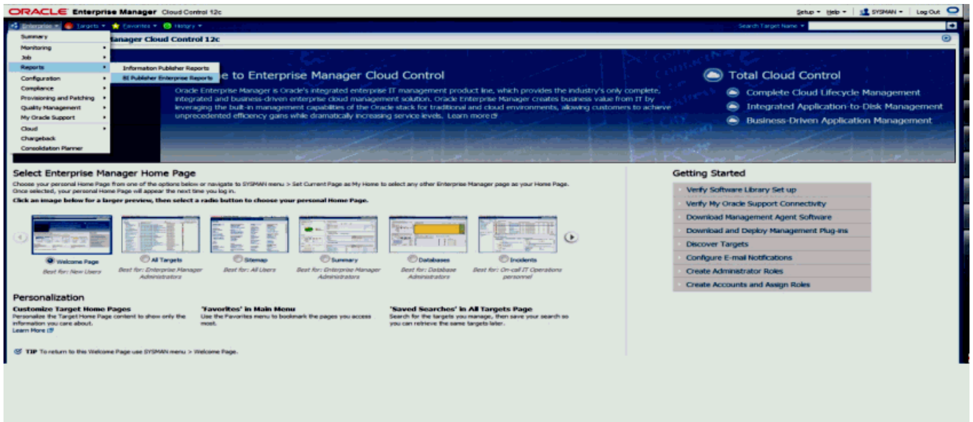
27.3 Generating Database Usage Tracking Report

Generating Database Usage Tracking Report consists of the following two steps:

1. Configuring Business Intelligence Publisher (BI Publisher) - setup the delivery destination of the output files (FTP server and folder)
2. Running Usage Tracking Report - produce the CSV files after the data is collected

27.3.1 Configuring Business Intelligence Publisher (BI Publisher)

1. From the **Enterprise** menu, select **Reports** and then **BI Publisher Enterprise Reports**.



Oracle Enterprise Manager is Oracle's integrated enterprise IT management product line, which provides the industry's only complete, integrated and business-driven enterprise cloud management solution. Oracle Enterprise Manager creates business value from IT by leveraging the built-in management capabilities of the Oracle stack for traditional and cloud environments, allowing customers to achieve unprecedented efficiency gains while dramatically increasing service levels. Learn more

Choose your personal Home Page from one of the options below or navigate to SYSMAN menu > Set Current Page as My Home to select any other Enterprise Manager page as your Home Page. Once selected, your personal Home Page will appear the next time you log in.

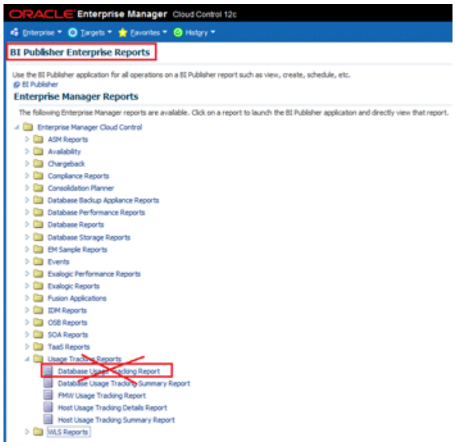
Click an image below for a larger preview, then select a radio button to choose your personal Home Page.

TIP To return to this Welcome Page use SYSMAN menu > Welcome Page.

ORACLE Enterprise Manager Cloud Control 12c
Setup
Help
SYSMAN
Log Out
Enterprise
Targets
Favorites
History
Search Target Name
Summary
Monitoring
Job
Reports
Configuration
Compliance
Provisioning and Patching
Quality Management
My Oracle Support
Cloud
Chargeback
Consolidation Planner
Information Publisher Reports
BI Publisher Enterprise Reports
Manager Cloud Control 12c
e to Enterprise Manager Cloud Control
Total Cloud Control
Complete Cloud Lifecycle Management
Integrated Application-to-Disk Management
Business-Driven Application Management
Select Enterprise Manager Home Page
Welcome Page
Best for: New Users
All Targets
Best for: Enterprise Manager Administrators
Sitemap
Best for: All Users
Summary
Best for: Enterprise Manager Administrators
Databases
Best for: Database Administrators
Incidents
Best for: On-call IT Operations personnel
Personalization
Customize Target Home Pages
Personalize the Target Home Page content to show only the information you care about.
Learn More
'Favorites' in Main Menu
Use the Favorites menu to bookmark the pages you access most.
'Saved Searches' in All Targets Page
Search for the targets you manage, then save your search so you can retrieve the same targets later.
Getting Started
Verify Software Library Set up
Verify My Oracle Support Connectivity
Download Management Agent Software
Download and Deploy Management Plug-ins
Discover Targets
Configure E-mail Notifications
Create Administrator Roles
Create Accounts and Assign Roles

2. Click on **BI Publisher Enterprise Reports Web Application** to navigate to the Oracle BI Publisher URL. Log in to BI Publisher using the same credentials used to Log in to Enterprise Manager.

Important: Do NOT click on the **Database Usage Tracking Report** shown at the bottom of the page. The online execution of this *Usage Tracking Report* has been disabled.



BI Publisher Enterprise Reports

Use the BI Publisher application for all operations on a BI Publisher report such as view, create, schedule, etc.

BI Publisher

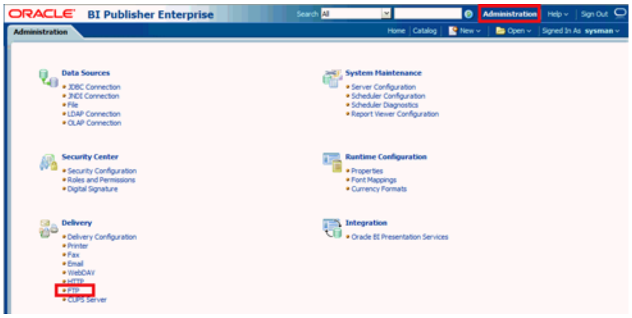
Enterprise Manager Reports

The following Enterprise Manager reports are available. Click on a report to launch the BI Publisher application and directly view that report.

- Enterprise Manager Cloud Control
  - ASM Reports
  - Availability
  - Chargeback
  - Compliance Reports
  - Consolidation Planner
  - Database Backup Appliance Reports
  - Database Performance Reports
  - Database Reports
  - Database Storage Reports
  - EM Sample Reports
  - Events
  - Exalogic Performance Reports
  - Exalogic Reports
  - Fusion Applications
  - IDM Reports
  - OSB Reports
  - SOA Reports
  - TaaS Reports
  - Usage Tracking Reports
    - Database Usage Tracking Report
    - Database Usage Tracking Summary Report
    - FMW Usage Tracking Report
    - Host Usage Tracking Details Report
    - Host Usage Tracking Summary Report
  - WLS Reports

3. Set up the delivery destination.

   Click on the **Administration** tab on the top right corner of the page. Then select **FTP** under **Delivery** as shown below:



Data Sources
- JDBC Connection
- JNDI Connection
- File
- LDAP Connection
- OLAP Connection

System Maintenance
- Server Configuration
- Scheduler Configuration
- Scheduler Diagnostics
- Report Viewer Configuration

Security Center
- Security Configuration
- Roles and Permissions
- Digital Signature

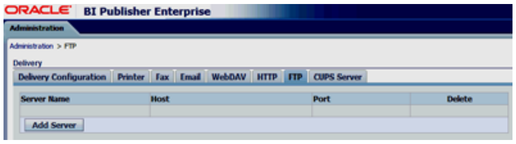
Runtime Configuration
- Properties
- Font Mappings
- Currency Formats

Delivery
- Delivery Configuration
- Printer
- Fax
- Email
- WebDAV
- HTTP
- FTP
- CUPS Server

Integration
- Oracle BI Presentation Services

4. Add an FTP Server:

   Click **Add Server.**



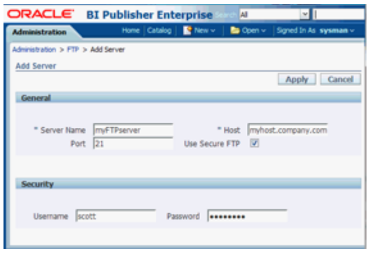
Server Name	Host	Port	Delete

Enter the following fields for the FTP server:

Server Name -	Example : myFTPserver (any name of your choice)
Host -	Example : myhost.company.com
Port -	Example : 22

Select "Use Secure FTP" check box to enable secure FTP (SFTP)

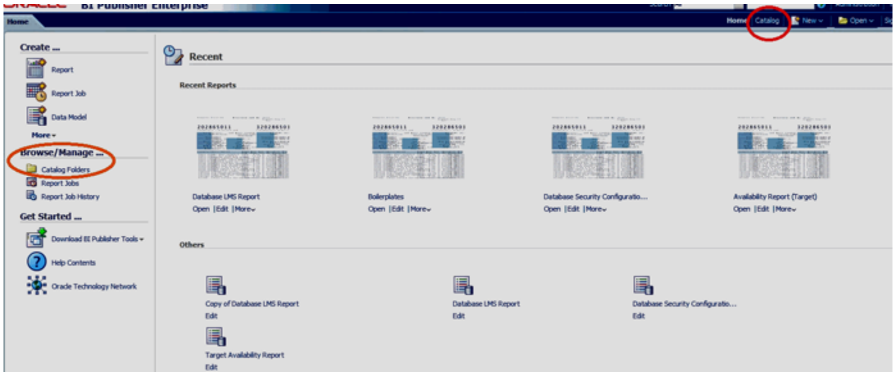
Enter a username and password to connect to the host


ORACLE BI Publisher Enterprise
Administration
Home | Catalog | New | Open | Signed In As sysman
Administration > FTP > Add Server
Add Server
Apply
Cancel
General
Security

* Server Name: myFTPserver
* Host: myhost.company.com
Port: 21
Use Secure FTP: ☑
Username: scott
Password: ********

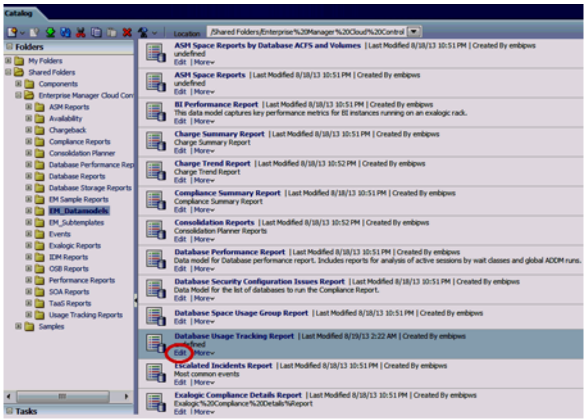
5. Configure the data model with the FTP server configured above in step 4.

   Click on **Catalog Folders** or alternatively the **Catalog** menu as shown in the following graphic.



   Select **Shared Folders**, then select **Enterprise Manager Cloud Control** and then **EM_Datamodels**

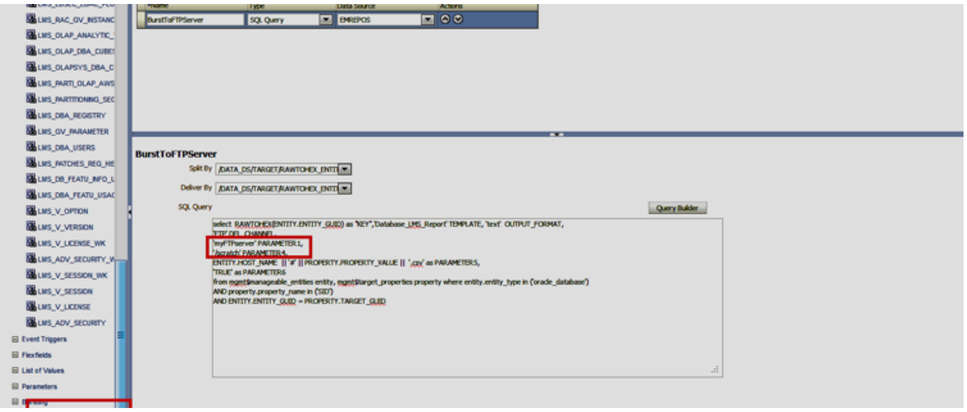
   Scroll to **Database Usage Tracking Report** and click **Edit**.



   On the bottom of the left list, select **Bursting**, and then **BurstToFTPserver**.

   In the **SQL Query** area, update the query as show below:

   - "myFTPserver" (configured in step 4) as the value for the PARAMETER1 column.
   - The output directory (absolute path of the directory on the disk) as the value for the PARAMETER4 column.



Name	Type	Data Source
BurstToFTPServer	SQL Query	EMREPOS

BurstToFTPServer

Split By /DATA_DS/TARGET/RAWTOHEX_ENTI

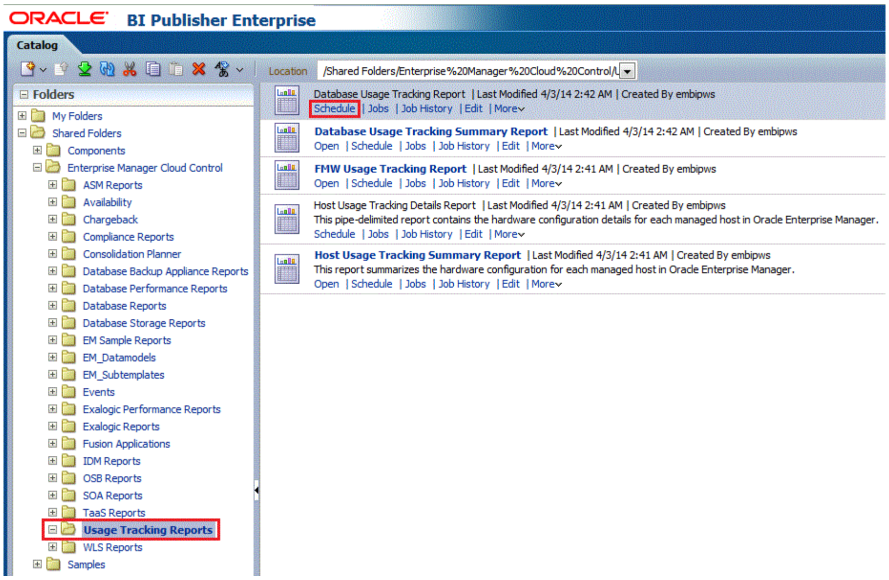
Deliver By /DATA_DS/TARGET/RAWTOHEX_ENTI

SQL Query

```
select RAWTOHEX(ENTITY.ENTITY_GUID) as "KEY",'Database_LMS_Report' TEMPLATE, 'text' OUTPUT_FORMAT,
'FTP' DEL_CHANNEL,
'myFTPserver' PARAMETER1,
'/scratch' PARAMETER4,
ENTITY.HOST_NAME || '#' || PROPERTY.PROPERTY_VALUE || '.csv' as PARAMETER5,
'TRUE' as PARAMETER6
from mgmt$manageable_entities entity, mgmt$target_properties property where entity.entity_type in ('oracle_database')
AND property.property_name in ('SID')
AND ENTITY.ENTITY_GUID = PROPERTY.TARGET_GUID
```

27.3.2 Running Usage Tracking Reports:

1. From the **Catalog** menu, select **Shared Folders**, then select **Enterprise Manager Cloud Control,** then **Usage Tracking Reports**, then **Database Usage Tracking Report**, and finally **Schedule**.



Location /Shared Folders/Enterprise%20Manager%20Cloud%20Control/U

Database Usage Tracking Report | Last Modified 4/3/14 2:42 AM | Created By embipws
Schedule | Jobs | Job History | Edit | More

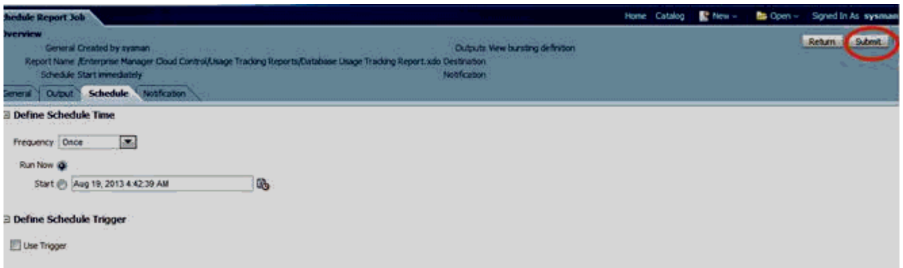
Database Usage Tracking Summary Report | Last Modified 4/3/14 2:42 AM | Created By embipws
Open | Schedule | Jobs | Job History | Edit | More

FMW Usage Tracking Report | Last Modified 4/3/14 2:41 AM | Created By embipws
Open | Schedule | Jobs | Job History | Edit | More

Host Usage Tracking Details Report | Last Modified 4/3/14 2:41 AM | Created By embipws
This pipe-delimited report contains the hardware configuration details for each managed host in Oracle Enterprise Manager.
Schedule | Jobs | Job History | Edit | More

Host Usage Tracking Summary Report | Last Modified 4/3/14 2:41 AM | Created By embipws
This report summarizes the hardware configuration for each managed host in Oracle Enterprise Manager.
Open | Schedule | Jobs | Job History | Edit | More

2. Make sure that, in the Schedule tab, the frequency is set to **Once** and **Run Now** is selected. Click **Submit**.



Overview

General Created by sysman

Report Name /Enterprise Manager Cloud Control/Usage Tracking Reports/Database Usage Tracking Report.xdo

Schedule Start immediately

Outputs View bursting definition

Destination

Notification

Define Schedule Time

Frequency Once

Run Now ●

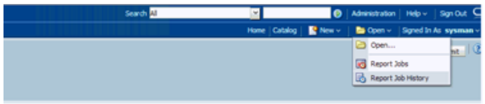
Start ○ Aug 19, 2013 4:42:39 AM

Define Schedule Trigger

□ Use Trigger

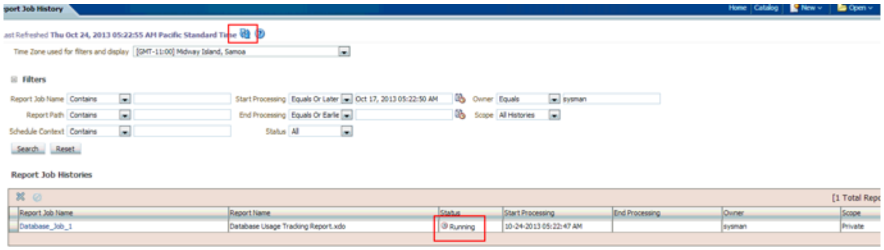
3. In the popup window, enter a job name to uniquely identify the job later.

   The status of the submitted job can be monitored in "Report Job History" page as shown below.



Errors (if any) in the metric collection are displayed at the bottom of each report that gets generated for an instance.

Use the refresh button highlighted in the screen shot (job_running.png) to refresh the status of the job



ast Refreshed Thu Oct 24, 2013 05:22:55 AM Pacific Standard Time

Time Zone used for filters and display [GMT-11:00] Midway Island, Samoa

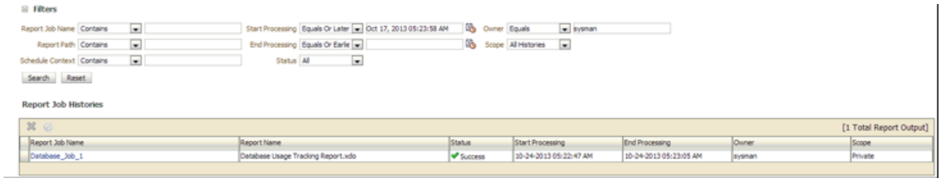
Report Job Name: Contains
Report Path: Contains
Schedule Context: Contains
Start Processing: Equals Or Later Oct 17, 2013 05:22:50 AM
End Processing: Equals Or Earlie
Status: All
Owner: Equals sysman
Scope: All Histories

Report Job Histories

[1 Total Repo

Report Job Name	Report Name	Status	Start Processing	End Processing	Owner	Scope
Database_Job_1	Database Usage Tracking Report.xdo	Running	10-24-2013 05:22:47 AM		sysman	Private

Wait until the status of the job changes from *Running* to *Success*.



Report Job Name: Contains
Report Path: Contains
Schedule Context: Contains
Start Processing: Equals Or Later Oct 17, 2013 05:23:58 AM
End Processing: Equals Or Earlie
Status: All
Owner: Equals sysman
Scope: All Histories

Report Job Histories

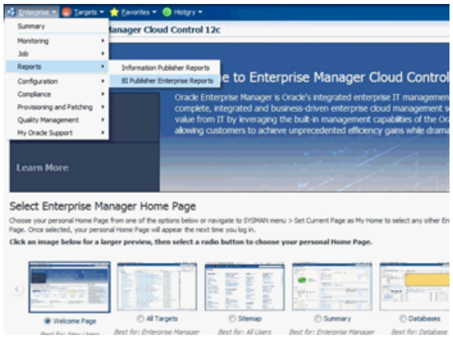
[1 Total Report Output]

Report Job Name	Report Name	Status	Start Processing	End Processing	Owner	Scope
Database_Job_1	Database Usage Tracking Report.xdo	✓ Success	10-24-2013 05:22:47 AM	10-24-2013 05:23:05 AM	sysman	Private

27.4 Database Usage Tracking Summary Report

Follow steps 1, 2 described in "Database Usage Tracking Report" if they have not already been done.

1. Set up Database Usage Tracking credentials.
2. Enable the metric collection.
3. Once logged into Enterprise Manager, from the **Enterprise** menu, select **Reports** and then **BI Publisher Reports**.



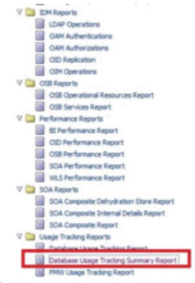
Oracle Enterprise Manager is Oracle's integrated enterprise IT managemen complete, integrated and business-driven enterprise cloud management s value from IT by leveraging the built-in management capabilities of the Or allowing customers to achieve unprecedented efficiency gains while drama

Select Enterprise Manager Home Page

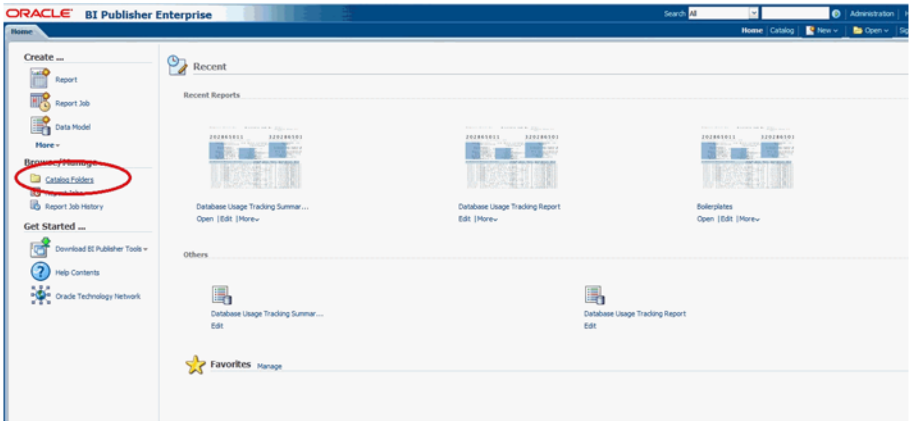
Choose your personal Home Page from one of the options below or navigate to SYSMAN menu > Set Current Page as My Home to select any other En Page. Once selected, your personal Home Page will appear the next time you log in.

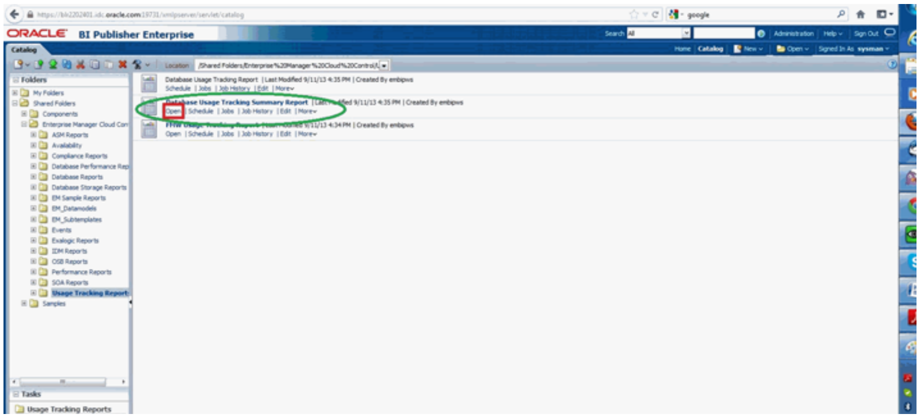
Click an image below for a larger preview, then select a radio button to choose your personal Home Page.

4. Click on **Database Usage Tracking Summary Report** in the tree. You will be prompted to log in to BI Publisher for the first time.



5. The report can also be viewed by logging in to BI Publisher.

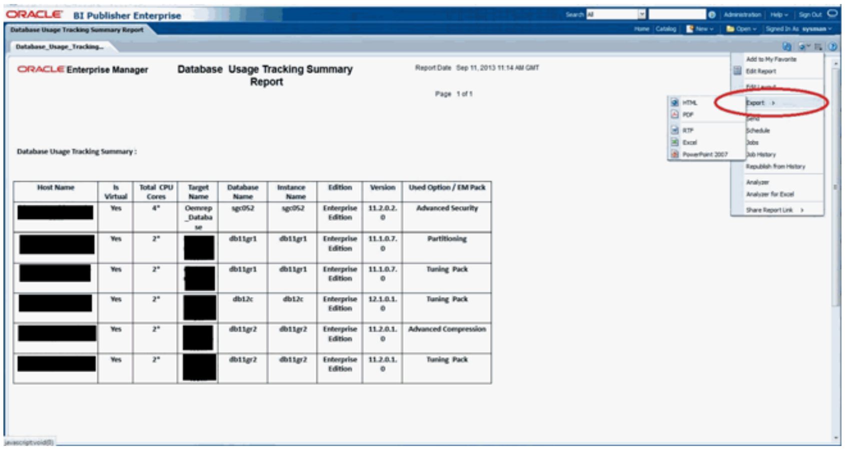




Database Usage Tracking Report | Last Modified 9/11/13 4:35 PM | Created By embipws
Schedule | Jobs | Job History | Edit | More

Database Usage Tracking Summary Report | Last Modified 9/11/13 4:35 PM | Created By embipws
Open | Schedule | Jobs | Job History | Edit | More

FMW Usage Tracking Report | Last Modified 9/11/13 4:34 PM | Created By embipws
Open | Schedule | Jobs | Job History | Edit | More



ORACLE Enterprise Manager

Database Usage Tracking Summary Report

Report Date Sep 11, 2013 11:14 AM GMT

Page 1 of 1

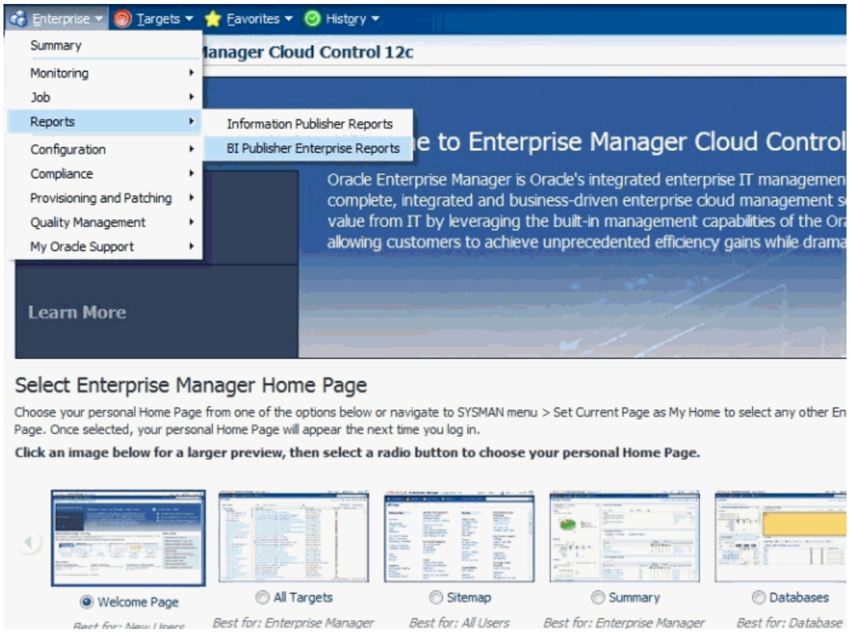
Database Usage Tracking Summary :

Host Name	Is Virtual	Total CPU Cores	Target Name	Database Name	Instance Name	Edition	Version	Used Option / EM Pack
[redacted]	Yes	4*	Oemrep _Database	sgc052	sgc052	Enterprise Edition	11.2.0.2.0	Advanced Security
[redacted]	Yes	2*	[redacted]	db11gr1	db11gr1	Enterprise Edition	11.1.0.7.0	Partitioning
[redacted]	Yes	2*	[redacted]	db11gr1	db11gr1	Enterprise Edition	11.1.0.7.0	Tuning Pack
[redacted]	Yes	2*	[redacted]	db12c	db12c	Enterprise Edition	12.1.0.1.0	Tuning Pack
[redacted]	Yes	2*	[redacted]	db11gr2	db11gr2	Enterprise Edition	11.2.0.1.0	Advanced Compression
[redacted]	Yes	2*	[redacted]	db11gr2	db11gr2	Enterprise Edition	11.2.0.1.0	Tuning Pack

27.5 Fusion Middleware Usage Tracking Summary Report

> **Note:** The Fusion Middleware Usage Tracking Summary Report contains data that is collected when the Enterprise Manager Fusion Middleware Plug-in is installed. There are no steps required to enable the Fusion Middleware metric collection.

1. Once logged in to Enterprise Manager, from the **Enterprise** menu, select **Reports**, and then **BI Publisher Reports**.



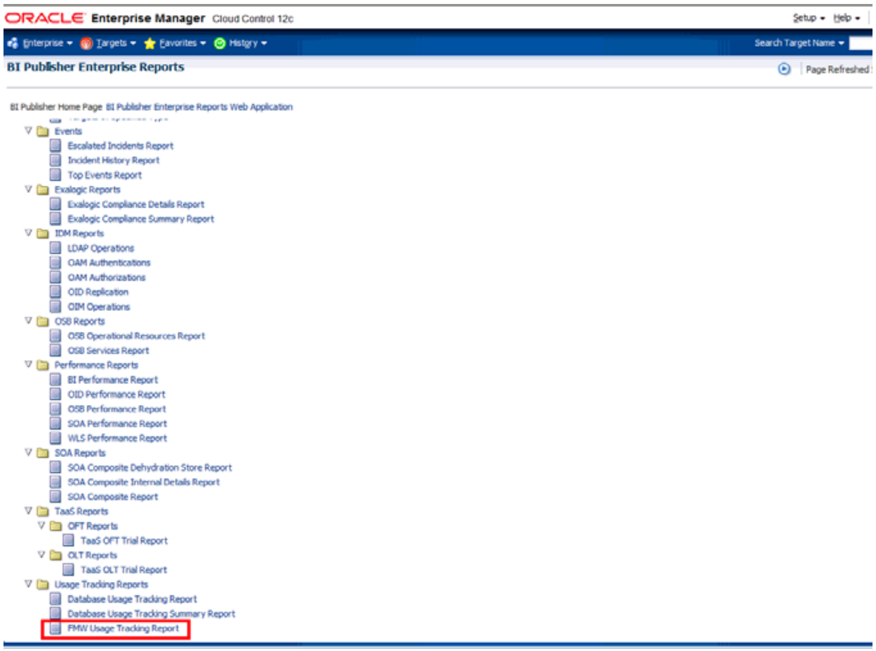
Oracle Enterprise Manager is Oracle's integrated enterprise IT managemen complete, integrated and business-driven enterprise cloud management s value from IT by leveraging the built-in management capabilities of the Ora allowing customers to achieve unprecedented efficiency gains while drama

Select Enterprise Manager Home Page

Choose your personal Home Page from one of the options below or navigate to SYSMAN menu > Set Current Page as My Home to select any other En Page. Once selected, your personal Home Page will appear the next time you log in.

Click an image below for a larger preview, then select a radio button to choose your personal Home Page.

2. Click on **FMW Usage Tracking Report** in the tree. You will be prompted to login to BI Publisher for the first time.

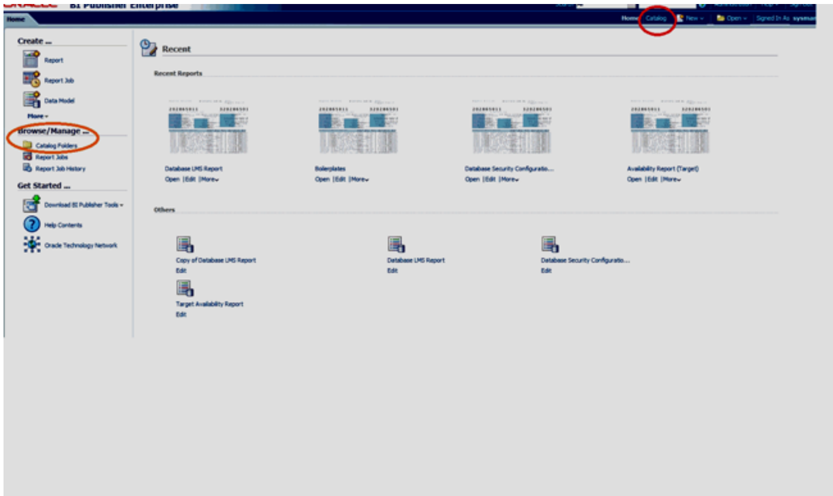

ORACLE Enterprise Manager Cloud Control 12c
Setup
Help
Enterprise
Targets
Favorites
History
Search Target Name
BI Publisher Enterprise Reports
Page Refreshed

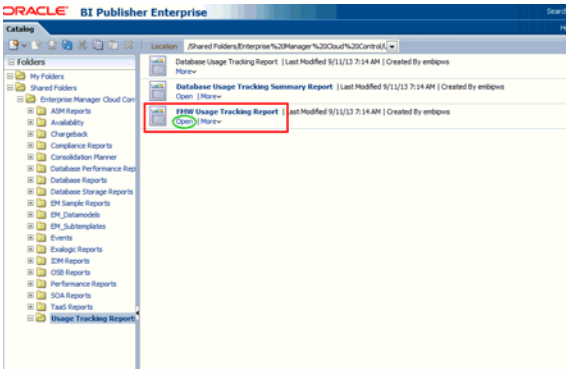
BI Publisher Home Page BI Publisher Enterprise Reports Web Application

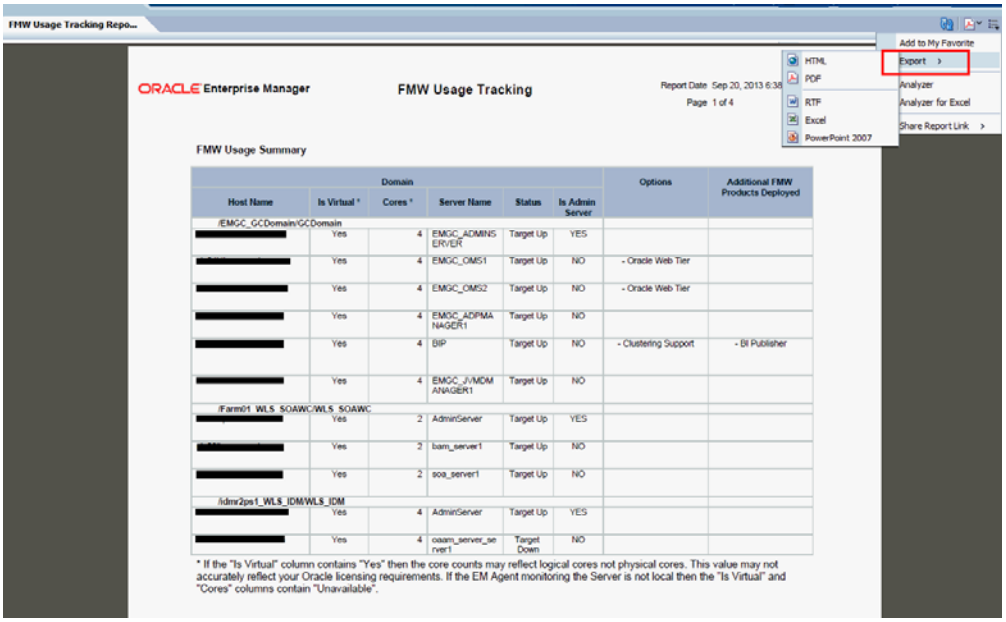
- Events
  - Escalated Incidents Report
  - Incident History Report
  - Top Events Report
- Exalogic Reports
  - Exalogic Compliance Details Report
  - Exalogic Compliance Summary Report
- IDM Reports
  - LDAP Operations
  - OAM Authentications
  - OAM Authorizations
  - OID Replication
  - OIM Operations
- OSB Reports
  - OSB Operational Resources Report
  - OSB Services Report
- Performance Reports
  - BI Performance Report
  - OID Performance Report
  - OSB Performance Report
  - SOA Performance Report
  - WLS Performance Report
- SOA Reports
  - SOA Composite Dehydration Store Report
  - SOA Composite Internal Details Report
  - SOA Composite Report
- TaaS Reports
  - OFT Reports
    - TaaS OFT Trial Report
  - OLT Reports
    - TaaS OLT Trial Report
- Usage Tracking Reports
  - Database Usage Tracking Report
  - Database Usage Tracking Summary Report
  - FMW Usage Tracking Report

3. The report can also be viewed by logging in to BI Publisher.

   Click on **Catalog Folders** or the **Catalog** Menu as shown.




ORACLE BI Publisher Enterprise
Catalog
Location /Shared Folders/Enterprise%20Manager%20Cloud%20Control/
Folders
My Folders
Shared Folders
Enterprise Manager Cloud Con
ASM Reports
Availability
Chargeback
Compliance Reports
Consolidation Planner
Database Performance Rep
Database Reports
Database Storage Reports
EM Sample Reports
EM_Datamodels
EM_Subtemplates
Events
Exalogic Reports
IDM Reports
OSB Reports
Performance Reports
SOA Reports
TaaS Reports
Usage Tracking Report
Database Usage Tracking Report | Last Modified 9/11/13 7:14 AM | Created By embipws
Database Usage Tracking Summary Report | Last Modified 9/11/13 7:14 AM | Created By embipws
FMW Usage Tracking Report | Last Modified 9/11/13 7:14 AM | Created By embipws
Open | More



FMW Usage Tracking

Report Date Sep 20, 2013 6:38

Page 1 of 4

FMW Usage Summary

Domain						Options	Additional FMW Products Deployed
Host Name	Is Virtual *	Cores *	Server Name	Status	Is Admin Server		
/EMGC_GCDomain/GCDomain							
[redacted]	Yes	4	EMGC_ADMINSERVER	Target Up	YES		
[redacted]	Yes	4	EMGC_OMS1	Target Up	NO	- Oracle Web Tier	
[redacted]	Yes	4	EMGC_OMS2	Target Up	NO	- Oracle Web Tier	
[redacted]	Yes	4	EMGC_ADPMANAGER1	Target Up	NO		
[redacted]	Yes	4	BIP	Target Up	NO	- Clustering Support	- BI Publisher
[redacted]	Yes	4	EMGC_JVMDMANAGER1	Target Up	NO		
/Farm01_WLS_SOAWC/WLS_SOAWC							
[redacted]	Yes	2	AdminServer	Target Up	YES		
[redacted]	Yes	2	bam_server1	Target Up	NO		
[redacted]	Yes	2	soa_server1	Target Up	NO		
/idmr2ps1_WLS_IDM/WLS_IDM							
[redacted]	Yes	4	AdminServer	Target Up	YES		
[redacted]	Yes	4	oaam_server_server1	Target Down	NO		

* If the "Is Virtual" column contains "Yes" then the core counts may reflect logical cores not physical cores. This value may not accurately reflect your Oracle licensing requirements. If the EM Agent monitoring the Server is not local then the "Is Virtual" and "Cores" columns contain "Unavailable".

27.6 Host Usage Tracking Reports

The Host Usage Tracking Reports provides an overview of the Host processor information. This is to be used for informational purposes only and this does not represent your license entitlement or requirement. Please contact the License Management Services representative at

http://www.oracle.com/us/corporate/license-management-services/index.html to understand your license requirements.

Two reports namely "Host Usage Tracking Summary Report" and "Host Usage Tracking Details Report" have been added.

- "Host Usage Tracking Summary Report" is a high level summary of the processor information on the Host system.

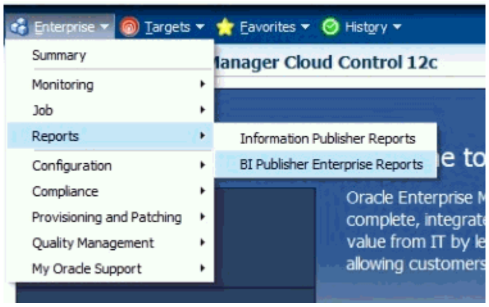
  This report can be run and viewed online. The output report can be exported to PDF, RTF, Excel formats.

- "Host Usage Tracking Details Report" provides the above usage data in an exportable format. The exported data can be sent to Oracle License Management Services for further analysis to determine licensing requirements. Please contact the License Management Services representative at http://www.oracle.com/us/corporate/license-management-services/index.html to initiate an engagement.

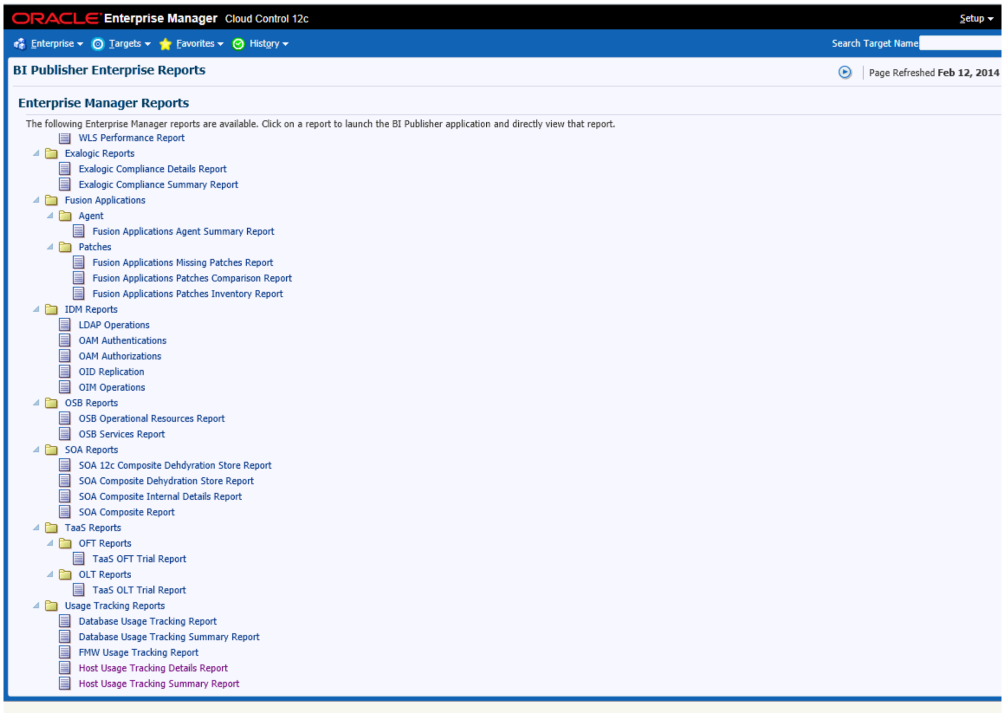
  A single file with each managed host's processor information is created. The format of the output files is limited to a pipe delimited file.

27.6.1 Host Usage Tracking Summary Report

1. Once logged into Enterprise Manager, from the **Enterprise** menu, select **Reports** and then **BI Publisher Reports**.



2. In the tree list, click "Host Usage Tracking Summary Report" .You will be prompted to log into BI Publisher for the first time.



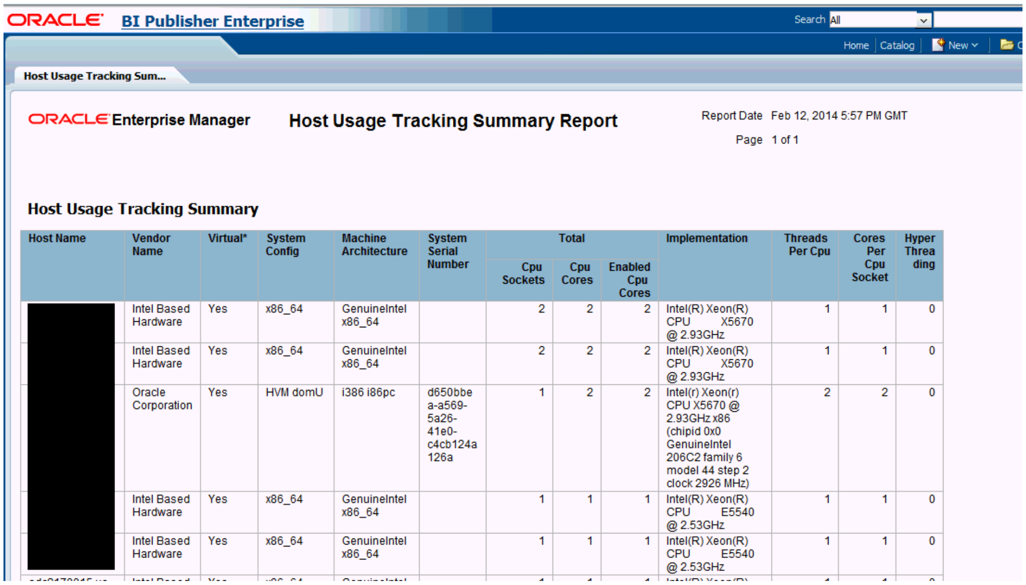
BI Publisher Enterprise Reports

Page Refreshed **Feb 12, 2014**

Enterprise Manager Reports

The following Enterprise Manager reports are available. Click on a report to launch the BI Publisher application and directly view that report.

- WLS Performance Report
- Exalogic Reports
  - Exalogic Compliance Details Report
  - Exalogic Compliance Summary Report
- Fusion Applications
  - Agent
    - Fusion Applications Agent Summary Report
  - Patches
    - Fusion Applications Missing Patches Report
    - Fusion Applications Patches Comparison Report
    - Fusion Applications Patches Inventory Report
- IDM Reports
  - LDAP Operations
  - OAM Authentications
  - OAM Authorizations
  - OID Replication
  - OIM Operations
- OSB Reports
  - OSB Operational Resources Report
  - OSB Services Report
- SOA Reports
  - SOA 12c Composite Dehdyration Store Report
  - SOA Composite Dehydration Store Report
  - SOA Composite Internal Details Report
  - SOA Composite Report
- TaaS Reports
  - OFT Reports
    - TaaS OFT Trial Report
  - OLT Reports
    - TaaS OLT Trial Report
- Usage Tracking Reports
  - Database Usage Tracking Report
  - Database Usage Tracking Summary Report
  - FMW Usage Tracking Report
  - Host Usage Tracking Details Report
  - Host Usage Tracking Summary Report



ORACLE BI Publisher Enterprise
Search All
Home
Catalog
New
Host Usage Tracking Sum...
ORACLE Enterprise Manager

Host Usage Tracking Summary Report

Report Date Feb 12, 2014 5:57 PM GMT

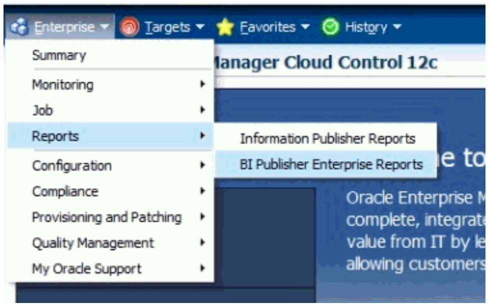
Page 1 of 1

Host Usage Tracking Summary

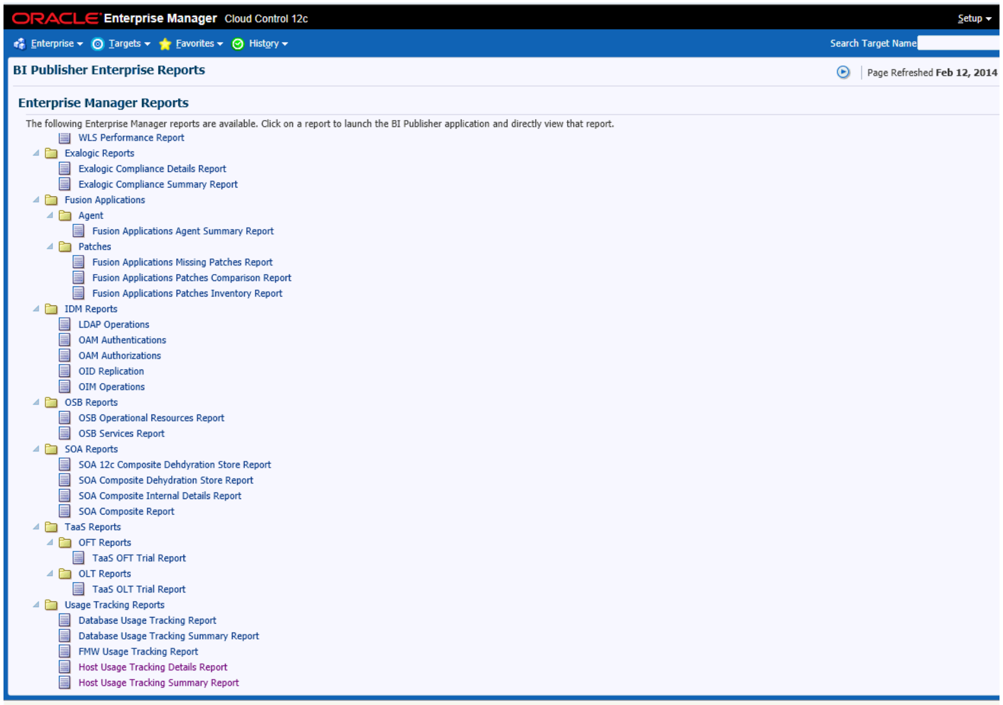
Host Name	Vendor Name	Virtual*	System Config	Machine Architecture	System Serial Number	Total			Implementation	Threads Per Cpu	Cores Per Cpu Socket	Hyper Threading
						Cpu Sockets	Cpu Cores	Enabled Cpu Cores				
[redacted]	Intel Based Hardware	Yes	x86_64	GenuineIntel x86_64		2	2	2	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz	1	1	0
[redacted]	Intel Based Hardware	Yes	x86_64	GenuineIntel x86_64		2	2	2	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz	1	1	0
[redacted]	Oracle Corporation	Yes	HVM domU	i386 i86pc	d650bbea-a569-5a26-41e0-c4cb124a126a	1	2	2	Intel(r) Xeon(r) CPU X5670 @ 2.93GHz x86 (chipid 0x0 GenuineIntel 206C2 family 6 model 44 step 2 clock 2926 MHz)	2	2	0
[redacted]	Intel Based Hardware	Yes	x86_64	GenuineIntel x86_64		1	1	1	Intel(R) Xeon(R) CPU E5540 @ 2.53GHz	1	1	0
[redacted]	Intel Based Hardware	Yes	x86_64	GenuineIntel x86_64		1	1	1	Intel(R) Xeon(R) CPU E5540 @ 2.53GHz	1	1	0

27.6.2 Host Usage Tracking Details Report

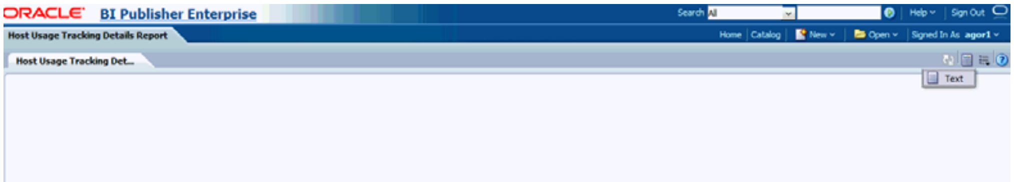
1. Once logged into Enterprise Manager, from the **Enterprise** menu, select **Reports** and then **BI Publisher Reports**.



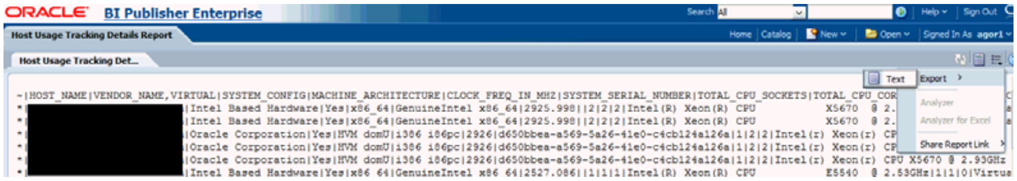
2. In the tree list click "Host Usage Tracking Details Report". You will be prompted to login to BI Publisher for the first time.


ORACLE Enterprise Manager Cloud Control 12c
Setup
Enterprise
Targets
Favorites
History
Search Target Name
BI Publisher Enterprise Reports
Page Refreshed Feb 12, 2014
Enterprise Manager Reports
The following Enterprise Manager reports are available. Click on a report to launch the BI Publisher application and directly view that report.
WLS Performance Report
Exalogic Reports
Exalogic Compliance Details Report
Exalogic Compliance Summary Report
Fusion Applications
Agent
Fusion Applications Agent Summary Report
Patches
Fusion Applications Missing Patches Report
Fusion Applications Patches Comparison Report
Fusion Applications Patches Inventory Report
IDM Reports
LDAP Operations
OAM Authentications
OAM Authorizations
OID Replication
OIM Operations
OSB Reports
OSB Operational Resources Report
OSB Services Report
SOA Reports
SOA 12c Composite Dehdyration Store Report
SOA Composite Dehydration Store Report
SOA Composite Internal Details Report
SOA Composite Report
TaaS Reports
OFT Reports
TaaS OFT Trial Report
OLT Reports
TaaS OLT Trial Report
Usage Tracking Reports
Database Usage Tracking Report
Database Usage Tracking Summary Report
FMW Usage Tracking Report
Host Usage Tracking Details Report
Host Usage Tracking Summary Report

3. Click the "View" icon in the upper-right corner and click "Text".

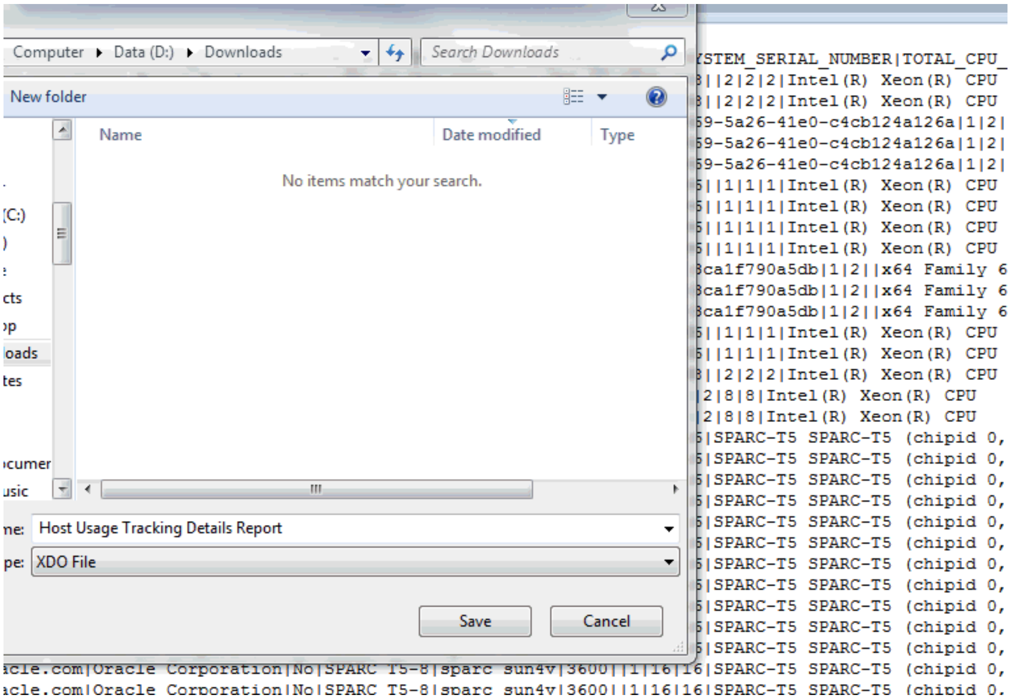

ORACLE BI Publisher Enterprise
Search All
Help
Sign Out
Host Usage Tracking Details Report
Home
Catalog
New
Open
Signed In As agor1
Host Usage Tracking Det...
Text

4. Click the "Actions" icon in the upper-right corner and select "Export" then "Text"



```
~|HOST_NAME|VENDOR_NAME,VIRTUAL|SYSTEM_CONFIG|MACHINE_ARCHITECTURE|CLOCK_FREQ_IN_MHZ|SYSTEM_SERIAL_NUMBER|TOTAL_CPU_SOCKETS|TOTAL_CPU_COR
*[redacted]|Intel Based Hardware|Yes|x86_64|GenuineIntel x86_64|2925.998||2|2|2|Intel(R) Xeon(R) CPU          X5670  @ 2.
*          |Intel Based Hardware|Yes|x86_64|GenuineIntel x86_64|2925.998||2|2|2|Intel(R) Xeon(R) CPU          X5670  @ 2.
*          |Oracle Corporation|Yes|HVM domU|i386 i86pc|2926|d650bbea-a569-5a26-41e0-c4cb124a126a|1|2|2|Intel(r) Xeon(r) CP
*          |Oracle Corporation|Yes|HVM domU|i386 i86pc|2926|d650bbea-a569-5a26-41e0-c4cb124a126a|1|2|2|Intel(r) Xeon(r) CP
*          |Oracle Corporation|Yes|HVM domU|i386 i86pc|2926|d650bbea-a569-5a26-41e0-c4cb124a126a|1|2|2|Intel(r) Xeon(r) CPU X5670 @ 2.93GHz
*          |Intel Based Hardware|Yes|x86 64|GenuineIntel x86 64|2527.086||1|1|1|Intel(R) Xeon(R) CPU          E5540  @ 2.53GHz|1|1|0|Virtua
```

5. Select "Save"



ne: Host Usage Tracking Details Report

pe: XDO File

```
YSTEM_SERIAL_NUMBER|TOTAL_CPU_
3||2|2|2|Intel(R) Xeon(R) CPU
3||2|2|2|Intel(R) Xeon(R) CPU
59-5a26-41e0-c4cb124a126a|1|2|
59-5a26-41e0-c4cb124a126a|1|2|
59-5a26-41e0-c4cb124a126a|1|2|
5||1|1|1|Intel(R) Xeon(R) CPU
5||1|1|1|Intel(R) Xeon(R) CPU
5||1|1|1|Intel(R) Xeon(R) CPU
5||1|1|1|Intel(R) Xeon(R) CPU
3ca1f790a5db|1|2||x64 Family 6
3ca1f790a5db|1|2||x64 Family 6
3ca1f790a5db|1|2||x64 Family 6
5||1|1|1|Intel(R) Xeon(R) CPU
5||1|1|1|Intel(R) Xeon(R) CPU
3||2|2|2|Intel(R) Xeon(R) CPU
|2|8|8|Intel(R) Xeon(R) CPU
|2|8|8|Intel(R) Xeon(R) CPU
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
5|SPARC-T5 SPARC-T5 (chipid 0,
acle.com|Oracle Corporation|No|SPARC T5-8|sparc sun4v|3600||1|16|16|SPARC-T5 SPARC-T5 (chipid 0,
acle.com|Oracle Corporation|No|SPARC T5-8|sparc sun4v|3600||1|16|16|SPARC-T5 SPARC-T5 (chipid 0,
```

Part V

Accessing Enterprise Manager via Mobile Devices

This section contains the following chapter:

28

Remote Access To Enterprise Manager

This chapter describes how to set up and use an iDevice to remotely connect to Enterprise Manager for the purpose of managing incidents and problems in Cloud Control.

The chapter also explains how to connect to the Enterprise Manager desktop version directly from the Safari browser.

The following sections describe setup and use of Cloud Control Mobile:

To use your iDevice to connect directly to the desktop version, see Section 28.9, "Connecting to Enterprise Manager Desktop Version."

28.1 Reviewing System Requirements

Cloud Control Mobile can be deployed to the following Enterprise Manager Cloud Control 12c minimum configurations:

- A new installation of the Enterprise Manager Cloud Control 12c (12.1.0.1) patched release (released February 2012 or later)
- An existing Enterprise Manager Cloud Control 12c (12.1.0.1) installation with Bundle Patch 1 (BP1) applied

Additional requirements are as follows:

- iDevice (iPhone, iPod touch, or iPad) running iOS 4.2.x or later
- A Wi-Fi or 3G connection to a network that has access to Enterprise Manager (Cloud Control Mobile supports connections over VPN)
- An Apple account with which to download the app from the iTunes App Store

28.2 Performing Initial Setup

Initial setup involves the following tasks:

- Connect to a Wi-Fi or 3G network
- Install and configure VPN
- Download the Cloud Control Mobile app and sync with your iDevice
- Add a Cloud Control URL to connect to the installed Enterprise Manager

28.3 Connecting the First Time

When you first install the app, there is no default Enterprise Manager connection, so you must supply a Cloud Control URL. There are two ways to do this:

- Use the iDevice Settings app
- Launch the Cloud Control Mobile app

In either case, first log in to VPN if required before proceeding with the instructions below. Without the VPN connection, the login screen will not appear.

iDevice Settings

Define a default Cloud Control URL as follows:

1. Tap the Settings icon on the Home screen.
2. Tap Cloud Control in the apps list.
3. On the Cloud Control screen, enter a name to identify the site and type the Cloud Control URL to which to connect. The URL should be of the form:

   ```
   https://www.yoursite.com/em
   ```

4. Tap **Settings** to store the information and return to the list of apps.

You can now launch the Cloud Control Mobile app to log in.

Initial App Launch

Define a default Cloud Control URL as follows:

1. Tap the Cloud Control Mobile icon on the Home screen.
2. On the Add Site screen, enter a name to identify the site and type the Cloud Control URL to which to connect. The URL should be of the form:

   ```
   https://www.yoursite.com/em
   ```

   Before you can type in the name field you may first have to clear the field by tapping the X at the right.
3. Tap **Done** to store the information.
4. Tap **Done** on the Sites screen. Note that you also have the option to add additional sites before exiting this screen.
5. Tap **Settings** on the Sites navigation bar to close the Sites list screen.
6. Tap **Save** on the Settings navigation bar to complete the action.

Proceed with the login.

28.4 Encountering the Login Screen

You encounter the login screen under the following conditions:

- After supplying a default Cloud Control URL upon initial launch
- Anytime you subsequently launch the app
- When you change the default site
- When you log out

Tap the **Settings** icon to see a list of sites or to change the default login site. See Section 28.5, "Managing Settings" for more information.

Specify your credentials and tap **Login**; the Incident Manager opens, displaying the my open incidents and problems view.

If your Enterprise Manager installation does not have a site certificate signed by a valid certificate authority, an alert overlays the login screen noting an invalid certificate. You have the option to continue with the login or change the URL to which you are trying to connect.

Note: If your installed Enterprise Manager uses single sign-on, the SSO process supplants site login. Upon completion of single sign-on, the workflow proceeds to the my open incidents and problems view.

28.5 Managing Settings

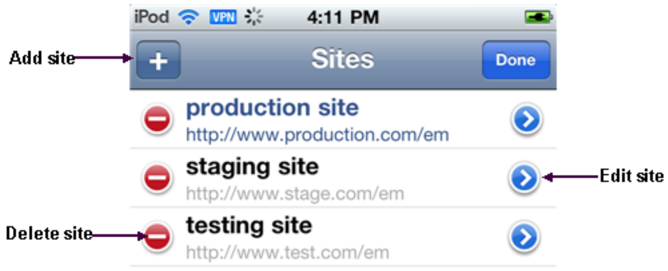
Cloud Control Mobile has its own settings interface apart from the iDevice Settings app that you use to manage all apps.

In managing Cloud Control Mobile app settings, you perform the following actions:

- Add a site
- Edit a site
- Delete a site
- Change the default site

Each action starts with the same basic steps:

1. Tap the actions icon on the right of the navigation bar.
2. Tap **Settings** in the action sheet.
3. Tap the Edit Sites table row.
4. Tap **Edit**. The Sites management screen appears:



production site
http://www.production.com/em

staging site
http://www.stage.com/em

testing site
http://www.test.com/em

Then proceed as described below for each individual action.

Add a Site

1. Tap the + sign on the left of the Sites navigation bar.

2. Type a name and a URL for the site to be added.
3. Tap **Done** on the Add Site navigation bar to close the screen.
4. Tap **Done** on the Sites navigation bar to exit edit mode.
5. Tap **Settings** on the Sites navigation bar to close the Sites list screen.
6. Tap **Save** on the Settings navigation bar to complete the action.

Edit a Site

1. Tap the blue arrow to the right of the URL to be edited.
2. Change the values as appropriate.
3. Tap **Done** on the Edit Site navigation bar to close the screen.
4. Tap **Done** on the Sites navigation bar to exit edit mode.
5. Tap **Settings** on the Sites navigation bar to close the Sites list screen.
6. Tap **Save** on the Sites navigation bar to complete the action.

Delete a Site

1. Tap the red circle to the left of the URL to be deleted.
2. Tap **Delete** that appears on the right in the table row.
3. Tap **Done** on the Sites navigation bar to close the screen.
4. Tap **Settings** on the Sites navigation bar to close the Sites list screen.
5. Tap **Save** on the Settings navigation bar to complete the action.

Change the Default Site

1. Tap the site to be the new default. The check mark to the right in the table row confirms your selection.
2. Tap **Settings** to close the Sites list screen.
3. Tap **Save** to complete the action.
4. After a brief moment, the Login screen appears. Specify credentials to log in to the new site.

Note that you also can change the default site in iDevice Settings for Cloud Control.

28.6 Using Cloud Control Mobile in Incident Manager

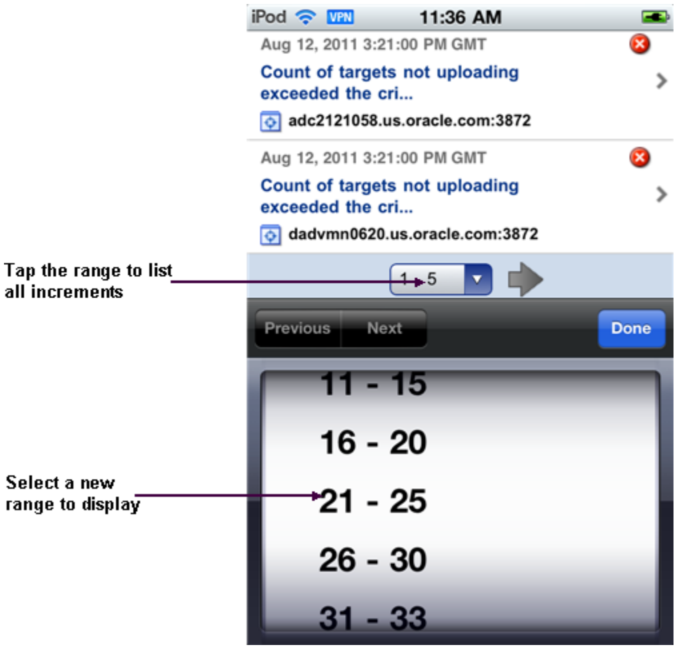
Connecting to Cloud Control remotely, you can do the following in Incident Manager:

- View your open incidents and problems; drill down to incident and problem details, including associated updates and events
- See the list of incidents for a given problem; link to these incidents and their details
- Acknowledge incidents and problems
- Manage incident and problem workflow for better tracking (change status, assign owner, escalate, and so forth)
- See who has been notified about an issue and what comments have been added by administrators

In addition, The FAQ that follows may help in understanding differences, subtleties, and nuances between the mobile app and its desktop counterpart.

How do I view more issues?

The app displays five rows at a time. Use the next and previous controls at the bottom of the display to scroll the list. Or tap the number range itself (1 - 5) to pick from a list of increments.



Aug 12, 2011 3:21:00 PM GMT

Count of targets not uploading exceeded the cri...

adc2121058.us.oracle.com:3872

Aug 12, 2011 3:21:00 PM GMT

Count of targets not uploading exceeded the cri...

dadvmn0620.us.oracle.com:3872

Tap the range to list all increments

Select a new range to display

How do I view issue details?

Simply tap the line that identifies the incident or problem. On the Details screen, you can continue to drill down to updates and events as well as expand the summary description.

Are the views the same in the mobile app as in the desktop version?

Yes, except for event-related views (standard or custom), which are not available in the app. Any custom views created in the desktop version augment the list of standard views.

Can I refresh the view?

Yes, just tap the refresh icon on the left of the navigation bar. When you do, the timestamp reflects the date and time of the refresh.

Can I view target details?

Yes, first drill down to incident details, then tap the target name to jump to target details. Tap **Incident** to return to the incident details.

Can I set search criteria or create a custom view?

No, you cannot set search criteria or create a custom view in the mobile app, but you can create and manage views in the desktop version, which are then available in the mobile app.

Can I invoke the incident rules feature?

No, but you can receive notifications generated by incident rules on your mobile device, provided your Enterprise Manager account has the appropriate notification preferences.

Can I connect to My Oracle Support?

If a problem has an assigned SR number, you can click the number to view the SR details in the My Oracle Support (MOS) Mobile app.

Can I access guided resolution information and diagnostics?

No.

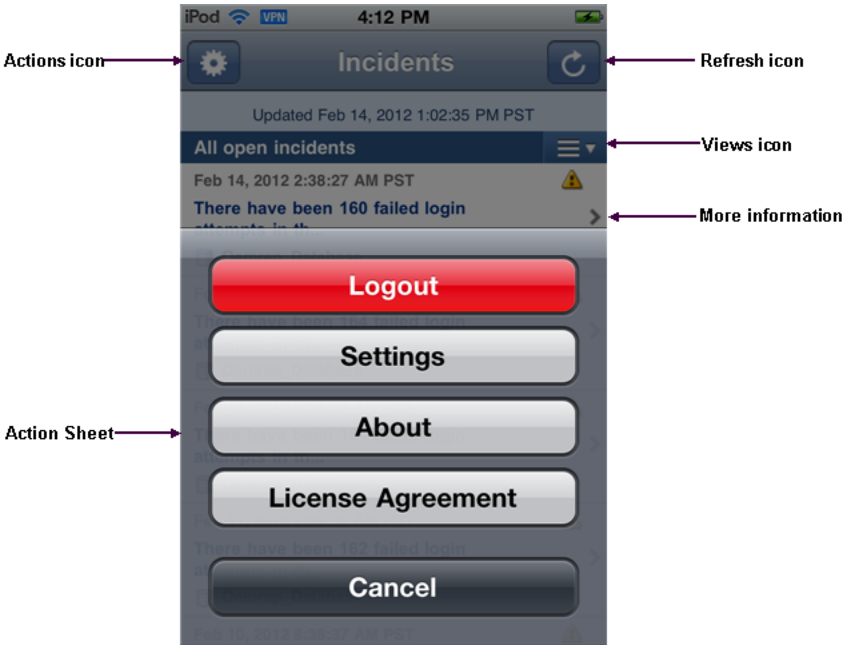
Do all iDevices work the same way with the mobile app?

Pretty much. The one difference you will note on an iPad is that if you tap a link to an issue or a target in an external source such as Safari or an e-mail message, Safari launches, pointing to the relevant page in the desktop version, where you are greeted with the usual Cloud Control login screen. With the other devices, tapping a link in an external source launches the mobile app.

28.7 Working in Cloud Control Mobile

This section covers the following operational tasks in Cloud Control Mobile:

- Viewing Incidents and Problems
- Changing Views
- Performing Actions



Updated Feb 14, 2012 1:02:35 PM PST

All open incidents

Feb 14, 2012 2:38:27 AM PST

There have been 160 failed login

28.7.1 Viewing Incidents and Problems

Although navigation is intuitive, the following sections offer guidance on viewing incidents and problems. As the interactions are slightly different, there is a separate section for each type of issue.

Viewing Incidents

Use the following guidelines as you view incidents in the list:

- An arrow on the right indicates availability of additional information.
- Tap anywhere in the incident row to drill down to incident details.
- The summary appears at the top. As summaries can be lengthy, you may need to tap the opening lines of the summary to view the complete summary. Tap **Incident** to return to incident details.
- Problem ID in incident details is a link to problem details. If you follow the link, tap **Incidents** there to return to the starting point; that is, the original list view where you first opened the incident.
- In the incident details view, target name is a link to target details. Tap **Incident** there to return to incident details.
- Tracking information appears below target name in the incident details view.
- Scroll down in incident details and tap **All Updates** to see the equivalent of the **Updates** tab in the desktop version. Tap **Incident** there to return to incident details.
- Scroll further and tap **Event List** to see the equivalent of the **Events** tab in the desktop version. Tap **Incident** there to return to incident details.

Viewing Problems

Use the following guidelines as you view problems in the list:

- An arrow on the right indicates availability of additional information.
- Tap anywhere in the problem row to drill down to problem details.
- The summary appears at the top. As summaries can be lengthy, you may need to tap the opening lines of the summary to view the complete summary. Tap **Problem** to return to problem details.
- If the problem has an SR number assigned, tap the number to log in to the My Oracle Support (MOS) Mobile app using your MOS credentials. You can then view the SR details and take appropriate action. Go to the Home screen and tap the Cloud Control Mobile app icon to return to problem details.
- In the problem details view, target name is a link to target details. Tap **Problem** there to return to problem details.
- Tracking information appears below target name in the problem details view.
- Scroll down in problem details and tap **All Updates** to see the equivalent of the **Updates** tab in the desktop version. Tap **Problem** there to return to problem details.
- Scroll further to see additional details such as first and last incident and number of incidents in which the problem has occurred.
- Scroll further and tap **Incident List** to see the equivalent of the **Incidents** tab in the desktop version. Tap **Problem** there to return to problem details.
- Each incident summary in the list is a link to the details of the incident. If you follow the link, tap **Incidents** there to return to the starting point; that is, the original list view where you first opened the issue.

28.7.2 Changing Views

When you first log in, the my open incidents and problems view appears by default. You can change the view as follows:

1. Open the Views menu by tapping the views icon (three horizontal lines to the right of the current views title).
2. Tap the view you want. The check mark to the right confirms your selection.
3. Tap **Incidents** to display the new view.

28.7.3 Performing Actions

You can perform the following actions while viewing incident or problem details:

- Acknowledge the issue
- Manage the workflow of the issue

To acknowledge an incident or problem:

1. While viewing the details, tap **Actions**.
2. Tap **Acknowledge** in the action sheet.

   A message confirms the update on the Details screen.

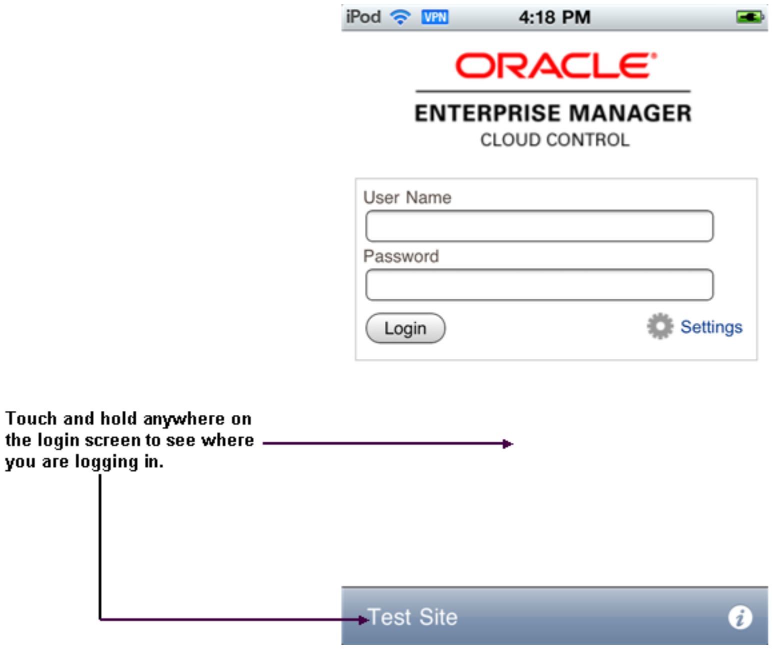
Note that the Acknowledge action may not appear in the action sheet for a variety of reasons; for example, the issue has already been acknowledged or closed, or you do not have the right permissions to acknowledge the issue.

To manage the workflow of an incident or problem for better tracking:

1. While viewing the details, tap **Actions**.
2. Tap **Manage** in the action sheet.
3. Complete the Manage dialog the same as you would in the desktop version. The only thing missing is the ability to add styles and formatting to the comment.
4. Tap **Save** to complete the action.

28.8 Learning Tips and Tricks

Use a touch-and-hold gesture at any time within the app to display on the bottom of the screen the current site to which you are logged in or about to log in. If the site name is unavailable, the URL appears. With the site identity displayed, tap the information icon on the right to access the Settings screen, where you can manage your sites and change the default site. Repeat the touch-and-hold gesture to remove the site display from the bottom of the screen.



If you have logged out of the app and find that you are stuck on a page trying to return to Cloud Control Mobile, you have a couple of options to resolve the issue:

- Open iDevice Settings and change the Cloud Control default URL.
- Force quit the app and restart Cloud Control Mobile. For example, press and hold the On/Off button on top of the device until the power off slider appears, and then press the Home button until the app closes.

28.9 Connecting to Enterprise Manager Desktop Version

With Enterprise Manager Cloud Control 12*c* (12.1.0.2), you can log in to the desktop version of Enterprise Manager using Safari on your iDevice, provided your iDevice is on the same network as Enterprise Manager. If you are remote, you may need to establish a VPN connection.

1. Connect to a WiFi or 3G network.
2. Establish a VPN connection if necessary.
3. Open Safari and specify an Enterprise Manager URL.
4. Enter login credentials to access Cloud Control.

With Cloud Control open on your iDevice, you have access to the full feature set. Consider the following as you navigate around the interface:

- Practice gestures to get a sense of how to zoom on a piece of screen real estate.
- Be patient when tapping menu selections; it does not necessarily occur instantaneously.
- Touch and hold a selection to open a context (right-click) menu. This gesture too requires some practice to develop the right sensitivity.
- Not all pages render precisely.
- Pages that have Flex/Flash effects will not render at all.

Note: If you connect to the desktop version of Enterprise Manager through Safari, be sure to set the Safari AutoFill Names and Passwords configuration setting to OFF. Otherwise, the login credentials can be saved to the local store, where they are susceptible to apps scanning for sensitive data.

Part VI

Configuring Enterprise Manager for High Availability

The Enterprise Manager High Availability section has been moved to the Oracle® Enterprise Manager Cloud Control Advanced Installation and Configuration Guide.

Part VII

Appendixes

This part contains the following appendixes:

A

Interpreting Variables of the Enterprise Manager MIB

Enterprise Manager Cloud Control can send SNMP traps to third-party, SNMP-enabled applications. Details of the trap contents can be obtained from the management information base (MIB) variables. This appendix provides information to help you interpret the variables of the private Oracle Enterprise Manager MIB.

For information about the format of MIB variable descriptions, see Section 4.6.3, "Reading the MIB Variable Descriptions".

This appendix contains the following sections:

- oraEMNGEvent
- oraEM4AlertTable
- oraEM4JobAlertTable

Note: SNMP trap notification methods created from the Cloud Control 12*c* console send the new oraEMNGEvent trap.

SNMP trap notification methods created before Enterprise Manager Release 12*c* send oraEM4Alert and oraEM4JobAlert traps. After upgrading to Enterprise Manager Release 12*c*, existing methods from earlier releases continue to deliver the old traps for backward compatibility.

A.1 oraEMNGEvent

The following sections describe the SNMP traps sent from SNMP trap notification methods created from the Cloud Control 12*c* console.

Table A–1 oraEMNGEvent Variables and Corresponding Object IDs

Variable Name	Object ID
oraEMNGEventIndex	1.3.6.1.4.1.111.15.3.1.1.1.1
oraEMNGEventNotifType	1.3.6.1.4.1.111.15.3.1.1.2.1
oraEMNGEventMessage	1.3.6.1.4.1.111.15.3.1.1.3.1
oraEMNGEventMessageURL	1.3.6.1.4.1.111.15.3.1.1.4.1
oraEMNGEventSeverity	1.3.6.1.4.1.111.15.3.1.1.5.1
oraEMNGEventSeverityCode	1.3.6.1.4.1.111.15.3.1.1.6.1

Table A–1 (Cont.) oraEMNGEvent Variables and Corresponding Object IDs

Variable Name	Object ID
oraEMNGEventRepeatCount	1.3.6.1.4.1.111.15.3.1.1.7.1
oraEMNGEventActionMsg	1.3.6.1.4.1.111.15.3.1.1.8.1
oraEMNGEventOccurrenceTime	1.3.6.1.4.1.111.15.3.1.1.9.1
oraEMNGEventReportedTime	1.3.6.1.4.1.111.15.3.1.1.10.1
oraEMNGEventCategories	1.3.6.1.4.1.111.15.3.1.1.11.1
oraEMNGEventCategoryCodes	1.3.6.1.4.1.111.15.3.1.1.12.1
oraEMNGEventType	1.3.6.1.4.1.111.15.3.1.1.13.1
oraEMNGEventName	1.3.6.1.4.1.111.15.3.1.1.14.1
oraEMNGAssocIncidentId	1.3.6.1.4.1.111.15.3.1.1.15.1
oraEMNGAssocIncidentOwner	1.3.6.1.4.1.111.15.3.1.1.16.1
oraEMNGAssocIncidentAcked	1.3.6.1.4.1.111.15.3.1.1.17.1
oraEMNGAssocIncidentStatus	1.3.6.1.4.1.111.15.3.1.1.18.1
oraEMNGAssocIncidentPriority	1.3.6.1.4.1.111.15.3.1.1.19.1
oraEMNGAssocIncidentEscLevel	1.3.6.1.4.1.111.15.3.1.1.20.1
oraEMNGEventTargetName	1.3.6.1.4.1.111.15.3.1.1.21.1
oraEMNGEventTargetNameURL	1.3.6.1.4.1.111.15.3.1.1.22.1
oraEMNGEventTargetType	1.3.6.1.4.1.111.15.3.1.1.23.1
oraEMNGEventHostName	1.3.6.1.4.1.111.15.3.1.1.24.1
oraEMNGEventTargetOwner	1.3.6.1.4.1.111.15.3.1.1.25.1
oraEMNGEventTgtLifeCycleStatus	1.3.6.1.4.1.111.15.3.1.1.26.1
oraEMNGEventTargetVersion	1.3.6.1.4.1.111.15.3.1.1.27.1
oraEMNGEventUserDefinedTgtProp	1.3.6.1.4.1.111.15.3.1.1.28.1
oraEMNGEventSourceObjName	1.3.6.1.4.1.111.15.3.1.1.29.1
oraEMNGEventSourceObjNameURL	1.3.6.1.4.1.111.15.3.1.1.30.1
oraEMNGEventSourceObjType	1.3.6.1.4.1.111.15.3.1.1.31.1
oraEMNGEventSourceObjSubType	1.3.6.1.4.1.111.15.3.1.1.32.1
oraEMNGEventSourceObjOwner	1.3.6.1.4.1.111.15.3.1.1.33.1
oraEMNGEventCAJobName	1.3.6.1.4.1.111.15.3.1.1.34.1
oraEMNGEventCAJobStatus	1.3.6.1.4.1.111.15.3.1.1.35.1
oraEMNGEventCAJobOwner	1.3.6.1.4.1.111.15.3.1.1.36.1
oraEMNGEventCAJobStepOutput	1.3.6.1.4.1.111.15.3.1.1.37.1
oraEMNGEventCAJobType	1.3.6.1.4.1.111.15.3.1.1.38.1
oraEMNGEventRuleSetName	1.3.6.1.4.1.111.15.3.1.1.39.1
oraEMNGEventRuleName	1.3.6.1.4.1.111.15.3.1.1.40.1
oraEMNGEventRuleOwner	1.3.6.1.4.1.111.15.3.1.1.41.1
oraEMNGEventSequenceId	1.3.6.1.4.1.111.15.3.1.1.42.1
oraEMNGEventRCADetails	1.3.6.1.4.1.111.15.3.1.1.43.1

Table A–1 (Cont.) oraEMNGEvent Variables and Corresponding Object IDs

Variable Name	Object ID
oraEMNGEventContextAttrs	1.3.6.1.4.1.111.15.3.1.1.44.1
oraEMNGEventUserComments	1.3.6.1.4.1.111.15.3.1.1.45.1
oraEMNGEventUpdates	1.3.6.1.4.1.111.15.3.1.1.46.1
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1
oraEMNGEventTypeAttr3	1.3.6.1.4.1.111.15.3.1.1.63.1
oraEMNGEventTypeAttr4	1.3.6.1.4.1.111.15.3.1.1.64.1
oraEMNGEventTypeAttr5	1.3.6.1.4.1.111.15.3.1.1.65.1
oraEMNGEventTypeAttr6	1.3.6.1.4.1.111.15.3.1.1.66.1
oraEMNGEventTypeAttr7	1.3.6.1.4.1.111.15.3.1.1.67.1
oraEMNGEventTypeAttr8	1.3.6.1.4.1.111.15.3.1.1.68.1
oraEMNGEventTypeAttr9	1.3.6.1.4.1.111.15.3.1.1.69.1
oraEMNGEventTypeAttr10	1.3.6.1.4.1.111.15.3.1.1.70.1
oraEMNGEventTypeAttr11	1.3.6.1.4.1.111.15.3.1.1.71.1
oraEMNGEventTypeAttr12	1.3.6.1.4.1.111.15.3.1.1.72.1
oraEMNGEventTypeAttr13	1.3.6.1.4.1.111.15.3.1.1.73.1
oraEMNGEventTypeAttr14	1.3.6.1.4.1.111.15.3.1.1.74.1
oraEMNGEventTypeAttr15	1.3.6.1.4.1.111.15.3.1.1.75.1
oraEMNGEventTypeAttr16	1.3.6.1.4.1.111.15.3.1.1.76.1
oraEMNGEventTypeAttr17	1.3.6.1.4.1.111.15.3.1.1.77.1
oraEMNGEventTypeAttr18	1.3.6.1.4.1.111.15.3.1.1.78.1
oraEMNGEventTypeAttr19	1.3.6.1.4.1.111.15.3.1.1.79.1
oraEMNGEventTypeAttr20	1.3.6.1.4.1.111.15.3.1.1.80.1
oraEMNGEventTypeAttr21	1.3.6.1.4.1.111.15.3.1.1.81.1
oraEMNGEventTypeAttr22	1.3.6.1.4.1.111.15.3.1.1.82.1
oraEMNGEventTypeAttr23	1.3.6.1.4.1.111.15.3.1.1.83.1
oraEMNGEventTypeAttr24	1.3.6.1.4.1.111.15.3.1.1.84.1
oraEMNGEventTypeAttr25	1.3.6.1.4.1.111.15.3.1.1.85.1

A.1.1 oraEMNGEventIndex

Syntax

Integer

Access

Read-only

Status

Mandatory

Description

The index of a particular event, unique only at the moment an event is generated.

A.1.2 oraEMNGEventNotifType

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The notification type. Possible values are:

- NOTIF_NORMAL
- NOTIF_RETRY
- NOTIF_DURATION
- NOTIF_REPEAT
- NOTIF_CA
- NOTIF_RCA

A.1.3 oraEMNGEventMessage

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The message associated with this event.

A.1.4 oraEMNGEventMessageURL

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The Enterprise Manager Cloud Control console URL for the event message. It is populated for events with severities other than INFORMATIONAL. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.5 oraEMNGEventSeverity

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The severity of the event, such as Fatal, Critical, Warning, Advisory, Information, or Clear.

A.1.6 oraEMNGEventSeverityCode

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The internal code of the severity, such as Fatal, Critical, Warning, Advisory, Informational, or Clear.

A.1.7 oraEMNGEventRepeatCount

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The repeat notification counter for the event.

A.1.8 oraEMNGEventActionMsg

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The action message for this event.

A.1.9 oraEMNGEventOccurrenceTime

Syntax
DisplayString

Access
read-only

Status
Mandatory

Explanation
The time when this event occurred (optional). This is only populated for events that have an occurrence time.

A.1.10 oraEMNGEventReportedTime

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The time when this event was reported.

A.1.11 oraEMNGEventCategories

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The list of categories to which this event belongs. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.12 oraEMNGEventCategoryCodes

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The list of internal category codes to which this event belongs. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.13 oraEMNGEventType

Syntax
DisplayString

Access

Read-only

Status

Mandatory

Explanation

The name of the event type to which this event belongs.

Available Event Types

- metric_alert
- target_availability
- job_status_change
- metric_error
- user_reported
- cs_core
- sla_alert
- mext_update
- selfupdate
- cs_rule_violation

A.1.14 oraEMNGEventName

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The name of this event.

A.1.15 oraEMNGAssocIncidentId

Syntax

DisplayString

Access

Read-only

Status
Mandatory

Explanation
The ID of the associated incident with the event (optional).

A.1.16 oraEMNGAssocIncidentOwner

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
Owner of the associated incident with the event (optional).

A.1.17 oraEMNGAssocIncidentAcked

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
Acknowledged status of the associated incident with the event. 1 indicates acknowledged. 0 indicates unacknowledged.

A.1.18 oraEMNGAssocIncidentStatus

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation

The status of the associated incident with the event.

A.1.19 oraEMNGAssocIncidentPriority

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The priority of the associated incident with the event.

A.1.20 oraEMNGAssocIncidentEscLevel

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The escalation level of the associated incident with the event.

A.1.21 oraEMNGEventTargetName

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The name of the target to which this event applies. Populated for events that are about a target only.

A.1.22 oraEMNGEventTargetNameURL

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The Enterprise Manager Console URL of the target to which this event applies. Populated for events that are about a target only. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.23 oraEMNGEventTargetType

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The type of the target to which this event applies. Populated for events that are about a target only.

A.1.24 oraEMNGEventHostName

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The name of the host on which this event originated. Populated for events that are about a target only.

A.1.25 oraEMNGEventTargetOwner

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The primary administrator of the target on which this event originated. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.26 oraEMNGEventTgtLifeCycleStatus

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The life cycle status of the target on which this event originated.

A.1.27 oraEMNGEventTargetVersion

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The version of the target on which this event originated.

A.1.28 oraEMNGEventUserDefinedTgtProp

Syntax
DisplayString

Access
read-only

Status
Mandatory

Explanation
The user defined target properties [name,value pair list] of the associated target with this event. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.29 oraEMNGEventSourceObjName

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The name of the source object to which this event belongs to. Populated for events that are about a non-target object only, such as Jobs.

A.1.30 oraEMNGEventSourceObjNameURL

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
Enterprise Manager Console URL for the source object to which this event belongs. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.31 oraEMNGEventSourceObjType

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The type of the source object to which this event belongs.

A.1.32 oraEMNGEventSourceObjSubType

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The subtype of the source object to which this event belongs. (Optional). This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.33 oraEMNGEventSourceObjOwner

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The primary administrator of the source object to which this event belongs. (Optional). This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.34 oraEMNGEventCAJobName

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The name of the corrective action job associated with this event.

A.1.35 oraEMNGEventCAJobStatus

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The status of the corrective action job associated with this event.

A.1.36 oraEMNGEventCAJobOwner

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The owner of the corrective action job associated with this event.

A.1.37 oraEMNGEventCAJobStepOutput

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The job step output from the corrective action job associated with this event.

A.1.38 oraEMNGEventCAJobType

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The job type from the corrective action job associated with this event.

A.1.39 oraEMNGEventRuleSetName

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The name of the ruleset that caused this notification. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.40 oraEMNGEventRuleName

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The name of the rule within the ruleset that caused this notification.

A.1.41 oraEMNGEventRuleOwner

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
The owner of the ruleset that caused this notification.

A.1.42 oraEMNGEventSequenceId

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation
An Enterprise Manager-generated identifier that uniquely identifies the current issue until it is cleared.

A.1.43 oraEMNGEventRCADetails

Syntax
DisplayString

Access
Read-only

Status
Mandatory

Explanation

Root Cause Analysis information associated with this event if it exists.

A.1.44 oraEMNGEventContextAttrs

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The context attributes associated with this event. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.45 oraEMNGEventUserComments

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The user comments associated with this event. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.46 oraEMNGEventUpdates

Syntax

DisplayString

Access

Read-only

Status

Mandatory

Explanation

The updates associated with this event. This variable is empty if the trap size exceeds the configured SNMP packet size.

A.1.47 oraEMNGEventTypeAttr(1-71)

The following tables list oraEMNGEventType MIB variables 1 through 71. Each table categorizes the MIB variables by specific event type.

Table A–2 Metric Alert Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Metric GUID	A unique ID for the metric.
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	Severity GUID	A unique ID for the alert record.
oraEMNGEventTypeAttr3	1.3.6.1.4.1.111.15.3.1.1.63.1	Cycle GUID	A unique ID for the alert cycle.
oraEMNGEventTypeAttr4	1.3.6.1.4.1.111.15.3.1.1.64.1	Collection Name	The name of the collection collecting the metric.
oraEMNGEventTypeAttr5	1.3.6.1.4.1.111.15.3.1.1.65.1	Metric Group	The name of the metric.
oraEMNGEventTypeAttr6	1.3.6.1.4.1.111.15.3.1.1.66.1	Metric	The name of the metric column.
oraEMNGEventTypeAttr7	1.3.6.1.4.1.111.15.3.1.1.67.1	Metric Description	A brief description of the metric.
oraEMNGEventTypeAttr8	1.3.6.1.4.1.111.15.3.1.1.68.1	Metric value	The value of the metric when the event triggered.
oraEMNGEventTypeAttr9	1.3.6.1.4.1.111.15.3.1.1.69.1	Key Value	The monitored object for the metric corresponding to the Metric Alert event.
oraEMNGEventTypeAttr10	1.3.6.1.4.1.111.15.3.1.1.70.1	Key Column 1	Key Column 1
oraEMNGEventTypeAttr11	1.3.6.1.4.1.111.15.3.1.1.71.1	Key Column 1 Value	The value of Key Column 1.
oraEMNGEventTypeAttr12	1.3.6.1.4.1.111.15.3.1.1.72.1	Key Column 2	Key Column 2
oraEMNGEventTypeAttr13	1.3.6.1.4.1.111.15.3.1.1.73.1	Key Column 2 Value	The value of Key Column 2.
oraEMNGEventTypeAttr14	1.3.6.1.4.1.111.15.3.1.1.74.1	Key Column 3	Key Column 3
oraEMNGEventTypeAttr15	1.3.6.1.4.1.111.15.3.1.1.75.1	Key Column 3 Value	The value of Key Column 3.
oraEMNGEventTypeAttr16	1.3.6.1.4.1.111.15.3.1.1.76.1	Key Column 4	Key Column 4
oraEMNGEventTypeAttr17	1.3.6.1.4.1.111.15.3.1.1.77.1	Key Column 4 Value	The value of Key Column 4.
oraEMNGEventTypeAttr18	1.3.6.1.4.1.111.15.3.1.1.78.1	Key Column 5	Key Column 5
oraEMNGEventTypeAttr19	1.3.6.1.4.1.111.15.3.1.1.79.1	Key Column 5 Value	The value of Key Column 5.
oraEMNGEventTypeAttr20	1.3.6.1.4.1.111.15.3.1.1.80.1	Key Column 6	Key Column 6
oraEMNGEventTypeAttr21	1.3.6.1.4.1.111.15.3.1.1.81.1	Key Column 6 Value	The value of Key Column 6.
oraEMNGEventTypeAttr22	1.3.6.1.4.1.111.15.3.1.1.82.1	Key Column 7	Key Column 7
oraEMNGEventTypeAttr23	1.3.6.1.4.1.111.15.3.1.1.83.1	Key Column 7 Value	The value of Key Column 7.
oraEMNGEventTypeAttr24	1.3.6.1.4.1.111.15.3.1.1.84.1	Number of keys	The number of key metric columns in the metric.

Table A–3 Target Availability Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Availability status	The current availability status of the target.
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	Severity GUID	The GUID of the severity record associated with this availability status.
oraEMNGEventTypeAttr3	1.3.6.1.4.1.111.15.3.1.1.63.1	Availability Sub-status	The sub-status of a target for the current status.
oraEMNGEventTypeAttr4	1.3.6.1.4.1.111.15.3.1.1.64.1	Transition Severity	The severity that resulted in the target's status change to the current availability status.
oraEMNGEventTypeAttr5	1.3.6.1.4.1.111.15.3.1.1.65.1	Response metric GUID	The Metric GUID of response metric.
oraEMNGEventTypeAttr6	1.3.6.1.4.1.111.15.3.1.1.66.1	Severity GUID of the first severity in the availability cycle	The GUID of the first severity record in this availability cycle.

Table A–4 Job Status Change Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Execution ID	The unique ID of the job execution.
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	Job Status	The status of the job execution.
oraEMNGEventTypeAttr3	1.3.6.1.4.1.111.15.3.1.1.63.1	Execution Log	The job output of the last step executed.
oraEMNGEventTypeAttr4	1.3.6.1.4.1.111.15.3.1.1.64.1	Job Status Code	The execution status code of job execution.
oraEMNGEventTypeAttr5	1.3.6.1.4.1.111.15.3.1.1.65.1	State Change ID	The unique ID of the last status change.

Table A–5 Compliance Standard Rule Violation Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Root Compliance Standard	The root compliance standard node display name.
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	Root Compliance Standard Version	The root compliance standard version.
oraEMNGEventTypeAttr3	1.3.6.1.4.1.111.15.3.1.1.63.1	Root Compliance Standard Author	The author of the root compliance standard.
oraEMNGEventTypeAttr4	1.3.6.1.4.1.111.15.3.1.1.64.1	Parent Compliance Standard	The parent compliance standard node display name.

Table A–5 (Cont.) Compliance Standard Rule Violation Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr5	1.3.6.1.4.1.111.15.3.1.1.65.1	Compliance Standard Version	The compliance standard version.
oraEMNGEventTypeAttr6	1.3.6.1.4.1.111.15.3.1.1.66.1	Parent Compliance Standard Author	The author of a parent compliance standard.
oraEMNGEventTypeAttr7	1.3.6.1.4.1.111.15.3.1.1.67.1	Root Target Name	The root target name.
oraEMNGEventTypeAttr8	1.3.6.1.4.1.111.15.3.1.1.68.1	Root Target Type	The root target type.
oraEMNGEventTypeAttr9	1.3.6.1.4.1.111.15.3.1.1.69.1	Rule Name	The rule display name

Table A–6 Compliance Standard Score Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Root Compliance Standard	The root compliance standard node display name.
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	Root Compliance Standard Author	The author of the root compliance standard.
oraEMNGEventTypeAttr3	1.3.6.1.4.1.111.15.3.1.1.63.1	Root Compliance Standard Version	The version of the root compliance standard.
oraEMNGEventTypeAttr4	1.3.6.1.4.1.111.15.3.1.1.64.1	Compliance Standard	The compliance standard node display name.
oraEMNGEventTypeAttr5	1.3.6.1.4.1.111.15.3.1.1.65.1	Compliance Standard Version	The version of a compliance standard.
oraEMNGEventTypeAttr6	1.3.6.1.4.1.111.15.3.1.1.66.1	Compliance Standard Author	The author of a compliance standard.
oraEMNGEventTypeAttr7	1.3.6.1.4.1.111.15.3.1.1.67.1	Root Target Name	The root target name.
oraEMNGEventTypeAttr8	1.3.6.1.4.1.111.15.3.1.1.68.1	Root Target Type	The root target type.
oraEMNGEventTypeAttr10	1.3.6.1.4.1.111.15.3.1.1.70.1	Warning Threshold	The warning threshold of a compliance score.
oraEMNGEventTypeAttr9	1.3.6.1.4.1.111.15.3.1.1.69.1	Compliance Score	The compliance score.
oraEMNGEventTypeAttr11	1.3.6.1.4.1.111.15.3.1.1.71.1	Critical Threshold	The critical threshold of a compliance score.

Table A–7 Metric Error Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Metric Group	The name of the metric.
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	Collection Name	The name of the collection collecting the metric.

Table A–8 Metric Extension Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Metric Extension Version attribute	The version of the metric extension.

Table A–9 Self-update Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Type	Type
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	Description	Description
oraEMNGEventTypeAttr3	1.3.6.1.4.1.111.15.3.1.1.63.1	Version	Version
oraEMNGEventTypeAttr4	1.3.6.1.4.1.111.15.3.1.1.64.1	Status	Status

Table A–10 Service Level Agreement Alert Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Service Level Agreement Name	Service Level Agreement Name
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	Service Level Objective Name	Service Level Objective Name
oraEMNGEventTypeAttr3	1.3.6.1.4.1.111.15.3.1.1.63.1	Service Level Objective Type	The type of the Service Level Objective which will be either Performance or Availability
oraEMNGEventTypeAttr4	1.3.6.1.4.1.111.15.3.1.1.64.1	Value at Event Triggered	The value at Event Triggered
oraEMNGEventTypeAttr5	1.3.6.1.4.1.111.15.3.1.1.65.1	Customer Name	Customer Name

Table A–11 User-reported Event Type

Variable Name	OID Number	Event Type Attribute	Description
oraEMNGEventTypeAttr1	1.3.6.1.4.1.111.15.3.1.1.61.1	Name	The name describing the nature of the issue.
oraEMNGEventTypeAttr2	1.3.6.1.4.1.111.15.3.1.1.62.1	key	The optional key describing a sub-component within the target that this event is about.

A.2 oraEM4AlertTable

The oraEM4AlertTable describes the SNMP traps sent from Oracle Enterprise Manager for both metric severity alerts and policy violations.

Table A–12 lists the variables of the oraEM4AlertTable and their corresponding Object IDs.

Table A–12 oraEM4AlertTable Variables and Corresponding Object IDs

Variable Name	Object ID
oraEM4AlertTargetName	1.3.6.1.4.1.111.15.1.1.1.2.1
oraEM4AlertTargetType	1.3.6.1.4.1.111.15.1.1.1.3.1
oraEM4AlertHostName	1.3.6.1.4.1.111.15.1.1.1.4.1
oraEM4AlertMetricName	1.3.6.1.4.1.111.15.1.1.1.5.1
oraEM4AlertKeyName	1.3.6.1.4.1.111.15.1.1.1.6.1
oraEM4AlertKeyValue	1.3.6.1.4.1.111.15.1.1.1.7.1
oraEM4AlertTimeStamp	1.3.6.1.4.1.111.15.1.1.1.8.1
oraEM4AlertSeverity	1.3.6.1.4.1.111.15.1.1.1.9.1
oraEM4AlertMessage	1.3.6.1.4.1.111.15.1.1.1.10.1
oraEM4AlertRuleName	1.3.6.1.4.1.111.15.1.1.1.11.1
oraEM4AlertRuleOwner	1.3.6.1.4.1.111.15.1.1.1.12.1
oraEM4AlertMetricValue	1.3.6.1.4.1.111.15.1.1.1.13.1
oraEM4AlertContext	1.3.6.1.4.1.111.15.1.1.1.14.1
oraEM4AlertCycleGuid	1.3.6.1.4.1.111.15.1.1.1.15.1
oraEM4AlertRepeatCount	1.3.6.1.4.1.111.15.1.1.1.16.1
oraEM4AlertUDTargetProperties	1.3.6.1.4.1.111.15.1.1.1.17.1
oraEM4AlertAck	1.3.6.1.4.1.111.15.1.1.1.18.1
oraEM4AlertAckBy	1.3.6.1.4.1.111.15.1.1.1.19.1
oraEM4AlertNotifType	1.3.6.1.4.1.111.15.1.1.1.20.1
oraEM4AlertViolationGuid	1.3.6.1.4.1.111.15.1.1.1.21.1

A description of each of these variables follows.

A.2.1 oraEM4AlertTargetName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the target to which this alert applies.

Typical Range
Not applicable

Significance
Very important

A.2.2 oraEM4AlertTargetType

Syntax
DisplayString

Max-Access
read-only

Status
Mandatory

Explanation
The type of the target to which this alert applies.

Typical Range
Not applicable

Significance
Very important

A.2.3 oraEM4AlertHostName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the host on which this alert originated.

Typical Range
Not applicable

Significance
Very important

A.2.4 oraEM4AlertMetricName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the metric or policy which generated this alert.

Typical Range
Not applicable

Significance
Very important

A.2.5 oraEM4AlertKeyName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the key-column, if present, for the metric which generated this alert.

Typical Range
Not applicable

Significance
Very important

A.2.6 oraEM4AlertKeyValue

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The value of the key-column, if present, for the metric which generated this alert.

Typical Range
Not applicable

Significance
Very important

A.2.7 oraEM4AlertTimeStamp

Syntax
DisplayString

Max-Access
read-only

Status
Mandatory

Explanation
The time at which this alert was generated.

Typical Range
Not applicable

Significance
Important

A.2.8 oraEM4AlertSeverity

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The severity of the alert (for example, Clear, Informational, Warning, Critical, Unreachable Start, Blackout End, Blackout Start, Metric Error Clear, Metric Error Start, Status Pending).

Typical Range
Critical, warning, clear

Significance
Very important

A.2.9 oraEM4AlertMessage

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The message associated with the alert.

Typical Range
Not applicable

Significance
Very important

A.2.10 oraEM4AlertRuleName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the notification rule that caused this notification.

Typical Range
Not applicable

Significance
Important

A.2.11 oraEM4AlertRuleOwner

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The owner of the notification rule that caused this notification.

Typical Range
Not applicable

Significance
Important

A.2.12 oraEM4AlertMetricValue

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The value of the metric which caused this alert to be generated.

Typical Range
Not applicable

Significance
Important

A.2.13 oraEM4AlertContext

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
A comma separated list of metric column names and values associated with the metric that caused this alert to be generated.

Typical Range
Not applicable

Significance
Important

A.2.14 oraEM4AlertCycleGuid

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
An Enterprise Manager-generated identifier that is unique for the lifecycle of an alert.

Typical Range
Not applicable

Significance
Important

A.2.15 oraEM4AlertRepeatCount

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation

The repeat notification counter for the alert.

Typical Range

Not applicable

Significance

Important

A.2.16 oraEM4AlertUDTargetProperties

Syntax

DisplayString

Max-Access

Read-only

Status

Mandatory

Explanation

User-defined target properties associated with the target.

Typical Range

Not applicable

Significance

Important

A.2.17 oraEM4AlertAck

Syntax

DisplayString

Max-Access

Read-only

Status

Mandatory

Explanation

Acknowledged status flag associated with the alert. 1 indicates acknowledged. 0 indicates unacknowledged.

Typical Range

Not applicable

Significance

Important

A.2.18 oraEM4AlertAckBy

Syntax

DisplayString

Max-Access

Read-only

Status

Mandatory

Explanation

Acknowledged By value associated with the alert.

Typical Range

Not applicable

Significance

Important

A.2.19 oraEM4AlertNotifType

Syntax

DisplayString

Max-Access

Read-only

Status

Mandatory

Explanation

Notification type.

Possible values:

- 1 - Normal
- 4 - Repeat
- 9 - Duration

Typical Range

Not applicable

Significance

Important

A.2.20 oraEM4AlertViolationGuid

Syntax

DisplayString

Max-Access

Read-only

Status

Mandatory

Explanation

An Enterprise Manager-generated identifier that identifies a particular alert.

Typical Range

Not applicable

Significance

Important

A.3 oraEM4JobAlertTable

The oraEM4JobAlertTable describes changes in the status of either a Job or a Corrective Action that is running as part of the Oracle Enterprise Manager Job system.

Table A–13 lists the variables of the oraEM4JobAlertTable and their corresponding Object IDs.

Table A–13 oraEM4JobAlertTable Variables and Corresponding Object IDs

Variable Name	Object ID
oraEM4JobAlertJobName	1.3.6.1.4.1.111.15.1.2.1.2.1
oraEM4JobAlertJobOwner	1.3.6.1.4.1.111.15.1.2.1.3.1
oraEM4JobAlertJobType	1.3.6.1.4.1.111.15.1.2.1.4.1
oraEM4JobAlertJobStatus	1.3.6.1.4.1.111.15.1.2.1.5.1
oraEM4JobAlertTargets	1.3.6.1.4.1.111.15.1.2.1.6.1
oraEM4JobAlertTimeStamp	1.3.6.1.4.1.111.15.1.2.1.7.1
oraEM4JobAlertRuleName	1.3.6.1.4.1.111.15.1.2.1.8.1
oraEM4JobAlertRuleOwner	1.3.6.1.4.1.111.15.1.2.1.9.1
oraEM4JobAlertMetricName	1.3.6.1.4.1.111.15.1.2.1.10.1
oraEM4JobAlertMetricValue	1.3.6.1.4.1.111.15.1.2.1.11.1
oraEM4JobAlertContext	1.3.6.1.4.1.111.15.1.2.1.12.1
oraEM4JobAlertKeyName	1.3.6.1.4.1.111.15.1.2.1.13.1

Table A–13 (Cont.) oraEM4JobAlertTable Variables and Corresponding Object IDs

Variable Name	Object ID
oraEM4JobAlertKeyValue	1.3.6.1.4.1.111.15.1.2.1.14.1
oraEM4JobAlertSeverity	1.3.6.1.4.1.111.15.1.2.1.15.1
oraEM4JobAlertJobId	1.3.6.1.4.1.111.15.1.2.1.16.1
oraEM4JobAlertJobExecId	1.3.6.1.4.1.111.15.1.2.1.17.1

A description of each of these variables follows.

A.3.1 oraEM4JobAlertJobName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the job to which this alert applies.

Typical Range
Not applicable

Significance
Very important

A.3.2 oraEM4JobAlertJobOwner

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The owner of the job to which this alert applies.

Typical Range
Not applicable

Significance
Very important

A.3.3 oraEM4JobAlertJobType

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The type of the job to which this alert applies.

Typical Range
Not applicable

Significance
Important

A.3.4 oraEM4JobAlertJobStatus

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The status of the job to which this alert applies.

Typical Range
Not applicable

Significance
Very important

A.3.5 oraEM4JobAlertTargets

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
A comma separated list of target to which this alert applies.

Typical Range
Not applicable

Significance
Very important

A.3.6 oraEM4JobAlertTimeStamp

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The time at which this job status changed causing this alert.

Typical Range
Not applicable

Significance
Important

A.3.7 oraEM4JobAlertRuleName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the notification rule that caused this notification.

Typical Range
Not applicable

Significance
Important

A.3.8 oraEM4JobAlertRuleOwner

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The owner of the notification rule that caused this notification.

Typical Range
Not applicable

Significance
Important

A.3.9 oraEM4JobAlertMetricName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the metric or policy which caused the Corrective Action to run that caused this alert.

Typical Range

Not applicable

Significance

Very important

A.3.10 oraEM4JobAlertMetricValue

Syntax

DisplayString

Max-Access

Read-only

Status

Mandatory

Explanation

The value of the metric which caused the Corrective Action to run that caused this alert.

Typical Range

Not applicable

Significance

Important

A.3.11 oraEM4JobAlertContext

Syntax

DisplayString

Max-Access

Read-only

Status

Mandatory

Explanation

A comma separated list of metric column names and values associated with the metric which caused the Corrective Action to run that caused this alert.

Typical Range

Not applicable

Significance

Important

A.3.12 oraEM4JobAlertKeyName

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The name of the key-column, if present, for the metric which caused the Corrective Action to run that generated this alert.

Typical Range
Not applicable

Significance
Very important

A.3.13 oraEM4JobAlertKeyValue

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The value of the key-column, if present, for the metric which caused the Corrective Action to run that generated this alert.

Typical Range
Not applicable

Significance
Very important

A.3.14 oraEM4JobAlertSeverity

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The severity of the metric which caused the Corrective Action to run that generated this alert (for example, Critical).

Typical Range
Critical, warning, clear

Significance
Very important

A.3.15 oraEM4JobAlertJobId

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation
The job ID of the Enterprise Manager job that triggered this notification.

Typical Range
Not applicable

Significance
Very important

A.3.16 oraEM4JobAlertJobExecId

Syntax
DisplayString

Max-Access
Read-only

Status
Mandatory

Explanation

The job execution ID of the Enterprise Manager job that triggered this notification.

Typical Range

Not applicable

Significance

Very important

B

Enterprise Manager MIB Definition

The following MIB definition is the latest version at the time of publication. For the most recent version of the Enterprise Manager 12*c* MIB definition, view your installation MIB definition file at:

OMS_HOME/network/doc/omstrap.v1

B.1 MIB Definition

```
ORACLE-ENTERPRISE-MANAGER-4-MIB DEFINITIONS ::= BEGIN

IMPORTS
TRAP-TYPE
FROM RFC-1215
DisplayString
FROM RFC1213-MIB
OBJECT-TYPE
FROM RFC-1212
enterprises
FROM RFC1155-SMI;

oracle OBJECT IDENTIFIER ::= { enterprises  111 }

oraEM4 OBJECT IDENTIFIER ::= { oracle  15 }

oraEM4Objects OBJECT IDENTIFIER ::= { oraEM4  1 }

oraEM4AlertTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF OraEM4AlertEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
     "Information on alerts generated by Oracle Enterprise Manager. This table is
not queryable; it exists only to document the variables included in the
oraEM4Alert trap.  Each trap contains a single instance of each variable in the
table."
    ::= { oraEM4Objects  1 }

oraEM4AlertEntry OBJECT-TYPE
    SYNTAX  OraEM4AlertEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
     "Information about a particular Oracle Enterprise Manager alert."
    INDEX   { oraEM4AlertIndex }
    ::= { oraEM4AlertTable  1 }
OraEM4AlertEntry ::=
    SEQUENCE {
        oraEM4AlertIndex
            INTEGER,

        oraEM4AlertTargetName
   DisplayString,

        oraEM4AlertTargetType
   DisplayString,

        oraEM4AlertHostName
   DisplayString,

        oraEM4AlertMetricName
   DisplayString,

        oraEM4AlertKeyName
   DisplayString,

        oraEM4AlertKeyValue
   DisplayString,

        oraEM4AlertTimeStamp
   DisplayString,

        oraEM4AlertSeverity
   DisplayString,

        oraEM4AlertMessage
   DisplayString,

        oraEM4AlertRuleName
   DisplayString,

        oraEM4AlertRuleOwner
   DisplayString,

oraEM4AlertMetricValue
           DisplayString,

        oraEM4AlertContext
           DisplayString,

oraEM4AlertCycleGuid
           DisplayString,

oraEM4AlertRepeatCount
           DisplayString,

oraEM4AlertUDTargetProperties
           DisplayString,

    oraEM4AlertAck
           DisplayString,

    oraEM4AlertAckBy
           DisplayString,
    oraEM4AlertNotifType
           DisplayString,
    oraEM4AlertViolationGuid
           DisplayString
 }

oraEM4AlertIndex OBJECT-TYPE
    SYNTAX  INTEGER (0..2147483647)
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Index of a particular alert, unique only at the moment an alert is
generated."
    ::= { oraEM4AlertEntry  1 }

oraEM4AlertTargetName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the target to which this alert applies."
    ::= { oraEM4AlertEntry  2 }

oraEM4AlertTargetType OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The type of the target to which this alert applies."
    ::= { oraEM4AlertEntry  3 }

oraEM4AlertHostName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the host on which this alert originated."
    ::= { oraEM4AlertEntry  4 }

oraEM4AlertMetricName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the metric or policy which generated this alert."
    ::= { oraEM4AlertEntry  5 }

oraEM4AlertKeyName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the key-column, if present, for the metric which generated this
alert."
    ::= { oraEM4AlertEntry  6 }

oraEM4AlertKeyValue OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The value of the key-column, if present, for the metric which generated this
alert."
    ::= { oraEM4AlertEntry  7 }

oraEM4AlertTimeStamp OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The time at which this alert was generated."
    ::= { oraEM4AlertEntry  8 }

oraEM4AlertSeverity OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The severity of the alert e.g. Critical."
    ::= { oraEM4AlertEntry  9 }

oraEM4AlertMessage OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The message associated with the alert."
    ::= { oraEM4AlertEntry  10 }

oraEM4AlertRuleName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the notification rule that caused this notification."
    ::= { oraEM4AlertEntry  11 }

oraEM4AlertRuleOwner OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The owner of the notification rule that caused this notification."
    ::= { oraEM4AlertEntry  12 }

oraEM4AlertMetricValue OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The value of the metric which caused this alert to be generated."
    ::= { oraEM4AlertEntry  13 }

oraEM4AlertContext OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "A comma separated list of metric column names and values associated with the
```

```
metric that caused this alert to be generated."
    ::= { oraEM4AlertEntry  14 }

oraEM4AlertCycleGuid OBJECT-TYPE
     SYNTAX  DisplayString
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
      "An EM generated identifier that is unique for the lifecyle of an alert."
     ::= { oraEM4AlertEntry  15 }

oraEM4AlertRepeatCount OBJECT-TYPE
     SYNTAX  DisplayString
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
      "The repeat notification counter for the alert."
     ::= { oraEM4AlertEntry  16 }

oraEM4AlertUDTargetProperties OBJECT-TYPE
     SYNTAX  DisplayString
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
      "User-defined target properties associated with the target."
     ::= { oraEM4AlertEntry  17 }

oraEM4AlertAck OBJECT-TYPE
     SYNTAX  DisplayString
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
      "Acknowledged status flag associated with the alert. 1 indicates
acknowledged, 0 indicates unacknowledged."
     ::= { oraEM4AlertEntry  18 }

oraEM4AlertAckBy OBJECT-TYPE
     SYNTAX  DisplayString
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
      "Acknowledged By value  associated with the alert."
     ::= { oraEM4AlertEntry  19 }

oraEM4AlertNotifType OBJECT-TYPE
     SYNTAX  DisplayString
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
      "Notification Type. 1 - Normal, 4 - Repeat, 9 - Duration"
     ::= { oraEM4AlertEntry  20 }

oraEM4AlertViolationGuid OBJECT-TYPE
     SYNTAX  DisplayString
     ACCESS  read-only
     STATUS  mandatory
     DESCRIPTION
      "An EM generated identifier that identifies a particular alert."
     ::= { oraEM4AlertEntry  21 }
```

```
oraEM4Traps OBJECT IDENTIFIER ::= { oraEM4  2 }

oraEM4Alert TRAP-TYPE
    ENTERPRISE  oraEM4Traps
    VARIABLES   { oraEM4AlertTargetName, oraEM4AlertTargetType,
                  oraEM4AlertHostName, oraEM4AlertMetricName,
                  oraEM4AlertKeyName, oraEM4AlertKeyValue, oraEM4AlertTimeStamp,
                  oraEM4AlertSeverity, oraEM4AlertMessage,
                  oraEM4AlertRuleName, oraEM4AlertRuleOwner,
                  oraEM4AlertMetricValue, oraEM4AlertContext,
 oraEM4AlertCycleGuid,
                  oraEM4AlertRepeatCount,
                  oraEM4AlertUDTargetProperties, oraEM4AlertAck, oraEM4AlertAckBy,
                  oraEM4AlertNotifType, oraEM4AlertViolationGuid }
    DESCRIPTION
     "The variables included in the oraEM4Alert trap."
    ::= 1

oraEM4JobAlertTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF OraEM4JobAlertEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
     "Information on alerts generated by Oracle Enterprise Manager. This table is
not queryable; it exists only to document the variables included in the
oraEM4JobAlert trap.  Each trap contains a single instance of each variable in the
table."
    ::= { oraEM4Objects  2 }

oraEM4JobAlertEntry OBJECT-TYPE
    SYNTAX  OraEM4JobAlertEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
     "Information about a particular Oracle Enterprise Manager alert."
    INDEX   { oraEM4JobAlertIndex }
    ::= { oraEM4JobAlertTable  1 }

OraEM4JobAlertEntry ::=
    SEQUENCE {
        oraEM4JobAlertIndex
            INTEGER,

        oraEM4JobAlertJobName
   DisplayString,

        oraEM4JobAlertJobOwner
   DisplayString,

        oraEM4JobAlertJobType
   DisplayString,

        oraEM4JobAlertJobStatus
   DisplayString,

        oraEM4JobAlertTargets
   DisplayString,

        oraEM4JobAlertTimeStamp
   DisplayString,
        oraEM4JobAlertRuleName
   DisplayString,
        oraEM4JobAlertRuleOwner
   DisplayString,

oraEM4JobAlertMetricName
           DisplayString,

oraEM4JobAlertMetricValue
           DisplayString,

        oraEM4JobAlertContext
           DisplayString,

        oraEM4JobAlertKeyName
   DisplayString,

        oraEM4JobAlertKeyValue
   DisplayString,

        oraEM4JobAlertSeverity
   DisplayString,

        oraEM4JobAlertJobId
   DisplayString,

        oraEM4JobAlertJobExecId
   DisplayString
    }

oraEM4JobAlertIndex OBJECT-TYPE
    SYNTAX  INTEGER (0..2147483647)
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Index of a particular alert, unique only at the moment an alert is
generated."
    ::= { oraEM4JobAlertEntry  1 }

oraEM4JobAlertJobName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the job to which this alert applies."
    ::= { oraEM4JobAlertEntry  2 }

oraEM4JobAlertJobOwner OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The owner of the job to which this alert applies."
    ::= { oraEM4JobAlertEntry  3 }

oraEM4JobAlertJobType OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The type of the job to which this alert applies."
    ::= { oraEM4JobAlertEntry  4 }

oraEM4JobAlertJobStatus OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The status of the job to which this alert applies."
    ::= { oraEM4JobAlertEntry  5 }

oraEM4JobAlertTargets OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "A comma separated list of target to which this alert applies."
    ::= { oraEM4JobAlertEntry  6 }

oraEM4JobAlertTimeStamp OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The time at which this job status changed causing this alert."
    ::= { oraEM4JobAlertEntry  7 }

oraEM4JobAlertRuleName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the notification rule that caused this notification."
    ::= { oraEM4JobAlertEntry  8 }

oraEM4JobAlertRuleOwner OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The owner of the notification rule that caused this notification."
    ::= { oraEM4JobAlertEntry  9 }

oraEM4JobAlertMetricName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the metric or policy which caused the Corrective Action to run
that caused this alert."
    ::= { oraEM4JobAlertEntry  10 }

oraEM4JobAlertMetricValue OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The value of the metric which caused the Corrective Action to run that
caused this alert."
```

```
    ::= { oraEM4JobAlertEntry  11 }

oraEM4JobAlertContext OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "A comma separated list of metric column names and values associated with the
metric which caused the Corrective Action to run that caused this alert."
    ::= { oraEM4JobAlertEntry  12 }

oraEM4JobAlertKeyName OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the key-column, if present, for the metric which caused the
Corrective Action to run that generated this alert."
    ::= { oraEM4JobAlertEntry  13 }

oraEM4JobAlertKeyValue OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The value of the key-column, if present, for the metric which caused the
Corrective Action to run that generated this alert."
    ::= { oraEM4JobAlertEntry  14 }

oraEM4JobAlertSeverity OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The severity of the metric which caused the Corrective Action to run that
generated this alert e.g. Critical."
    ::= { oraEM4JobAlertEntry  15 }

oraEM4JobAlertJobId OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The Job Id of the EM Job that triggered this notification."
    ::= { oraEM4JobAlertEntry  16 }

oraEM4JobAlertJobExecId OBJECT-TYPE
    SYNTAX  DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The Job Execution Id of the EM Job that triggered this notification."
    ::= { oraEM4JobAlertEntry  17 }

oraEM4JobAlert TRAP-TYPE
    ENTERPRISE  oraEM4Traps
    VARIABLES   { oraEM4JobAlertJobName, oraEM4JobAlertJobOwner,
                  oraEM4JobAlertJobType, oraEM4JobAlertJobStatus,
                  oraEM4JobAlertTargets, oraEM4JobAlertTimeStamp,
                  oraEM4JobAlertRuleName, oraEM4JobAlertRuleOwner,
                  oraEM4JobAlertMetricName, oraEM4JobAlertMetricValue,
                  oraEM4JobAlertContext, oraEM4JobAlertKeyName,
                  oraEM4JobAlertKeyValue, oraEM4JobAlertSeverity,
                  oraEM4JobAlertJobId, oraEM4JobAlertJobExecId }
    DESCRIPTION
     "The variables included in the oraEM4JobAlert trap."
    ::= 2

oraEMNGObjects OBJECT IDENTIFIER ::= { oraEM4  3 }

oraEMNGEventTable OBJECT-TYPE
    SYNTAX  SEQUENCE OF OraEMNGEventEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
     "Information on events published to Oracle Enterprise Manager. This table is
not queryable; it exists only to document the variables included in the
oraEMNGEventTrap trap.  Each trap can contain a single instance of each variable
in the table."
    ::= { oraEMNGObjects  1 }

oraEMNGEventEntry OBJECT-TYPE
    SYNTAX  OraEMNGEventEntry
    ACCESS  not-accessible
    STATUS  mandatory
    DESCRIPTION
     "Information about a particular Oracle Enterprise Manager event."
    INDEX   { oraEMNGEventIndex }
    ::= { oraEMNGEventTable  1 }

OraEMNGEventEntry ::=
    SEQUENCE {
        oraEMNGEventIndex
            INTEGER,

        oraEMNGEventNotifType
            DisplayString,

        oraEMNGEventMessage
            DisplayString,

        oraEMNGEventMessageURL
            DisplayString,

        oraEMNGEventSeverity
            DisplayString,

        oraEMNGEventSeverityCode
            DisplayString,

        oraEMNGEventRepeatCount
            DisplayString,

        oraEMNGEventActionMsg
            DisplayString,

        oraEMNGEventOccurrenceTime
            DisplayString,

        oraEMNGEventReportedTime
            DisplayString,

        oraEMNGEventCategories
            DisplayString,

        oraEMNGEventCategoryCodes
            DisplayString,

        oraEMNGEventType
            DisplayString,

        oraEMNGEventName
            DisplayString,

        oraEMNGAssocIncidentId
            DisplayString,

        oraEMNGAssocIncidentOwner
            DisplayString,

        oraEMNGAssocIncidentAcked
            DisplayString,

        oraEMNGAssocIncidentStatus
            DisplayString,

        oraEMNGAssocIncidentPriority
            DisplayString,

        oraEMNGAssocIncidentEscLevel
            DisplayString,

        oraEMNGEventTargetName
            DisplayString,

        oraEMNGEventTargetNameURL
            DisplayString,

        oraEMNGEventTargetType
            DisplayString,

        oraEMNGEventHostName
            DisplayString,

        oraEMNGEventTargetOwner
            DisplayString,

        oraEMNGEventTgtLifeCycleStatus
            DisplayString,

        oraEMNGEventTargetVersion
            DisplayString,

        oraEMNGEventUserDefinedTgtProp
            DisplayString,

        oraEMNGEventSourceObjName
            DisplayString,

        oraEMNGEventSourceObjNameURL
```

```
    DisplayString,

oraEMNGEventSourceObjType
    DisplayString,

oraEMNGEventSourceObjSubType
    DisplayString,

oraEMNGEventSourceObjOwner
    DisplayString,

oraEMNGEventCAJobName
    DisplayString,

oraEMNGEventCAJobStatus
    DisplayString,

oraEMNGEventCAJobOwner
    DisplayString,

oraEMNGEventCAJobStepOutput
    DisplayString,

oraEMNGEventCAJobType
    DisplayString,

oraEMNGEventRuleSetName
    DisplayString,

oraEMNGEventRuleName
    DisplayString,

oraEMNGEventRuleOwner
    DisplayString,

oraEMNGEventSequenceId
    DisplayString,

oraEMNGEventRCADetails
    DisplayString,

oraEMNGEventContextAttrs
    DisplayString,

oraEMNGEventUserComments
    DisplayString,

oraEMNGEventUpdates
    DisplayString,

oraEMNGEventTypeAttr1
    DisplayString,

oraEMNGEventTypeAttr2
    DisplayString,

oraEMNGEventTypeAttr3
    DisplayString,

oraEMNGEventTypeAttr4
```

```
    DisplayString,

oraEMNGEventTypeAttr5
    DisplayString,

oraEMNGEventTypeAttr6
    DisplayString,

oraEMNGEventTypeAttr7
    DisplayString,

oraEMNGEventTypeAttr8
    DisplayString,

oraEMNGEventTypeAttr9
    DisplayString,

oraEMNGEventTypeAttr10
    DisplayString,

oraEMNGEventTypeAttr11
    DisplayString,

oraEMNGEventTypeAttr12
    DisplayString,

oraEMNGEventTypeAttr13
    DisplayString,

oraEMNGEventTypeAttr14
    DisplayString,

oraEMNGEventTypeAttr15
    DisplayString,

oraEMNGEventTypeAttr16
    DisplayString,

oraEMNGEventTypeAttr17
    DisplayString,

oraEMNGEventTypeAttr18
    DisplayString,

oraEMNGEventTypeAttr19
    DisplayString,

oraEMNGEventTypeAttr20
    DisplayString,

oraEMNGEventTypeAttr21
    DisplayString,

oraEMNGEventTypeAttr22
    DisplayString,

oraEMNGEventTypeAttr23
    DisplayString,

oraEMNGEventTypeAttr24
```

```
            DisplayString,

        oraEMNGEventTypeAttr25
            DisplayString
  }

oraEMNGEventIndex OBJECT-TYPE
    SYNTAX INTEGER (0..2147483647)
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Index of a particular event, unique only at the moment an event is
generated."
    ::= { oraEMNGEventEntry  1 }

oraEMNGEventNotifType  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "Notification Type. NOTIF_NORMAL, NOTIF_RETRY, NOTIF_DURATION, NOTIF_REPEAT,
NOTIF_CA, NOTIF_RCA"
    ::= { oraEMNGEventEntry  2 }

oraEMNGEventMessage  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The message associated with this event."
    ::= { oraEMNGEventEntry  3 }

oraEMNGEventMessageURL  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "EM Console URL for the event message. Populated for events with severity
other than INFORMATIONAL. Empty if trap size exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  4 }

oraEMNGEventSeverity  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The severity of the event e.g. Critical."
    ::= { oraEMNGEventEntry  5 }

oraEMNGEventSeverityCode  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Internal code of the severity: FATAL, WARNING, CRITICAL, MINOR_WARNING,
INFORMATIONAL, CLEAR."
    ::= { oraEMNGEventEntry  6 }

oraEMNGEventRepeatCount  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The repeat notification counter for the event."
    ::= { oraEMNGEventEntry  7 }

oraEMNGEventActionMsg  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The action message for this event."
    ::= { oraEMNGEventEntry  8 }

oraEMNGEventOccurrenceTime  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The time when this event occurred (optional), this is only populated for
events that have occurrence time."
    ::= { oraEMNGEventEntry  9 }

oraEMNGEventReportedTime  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The time when this event was reported."
    ::= { oraEMNGEventEntry  10 }

oraEMNGEventCategories  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The list of categories to which this event belongs to. Empty if trap size
exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  11 }

oraEMNGEventCategoryCodes  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The list of internal category codes to which this event belongs to. Empty if
trap size exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  12 }

oraEMNGEventType  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "The name of the event type to which this event belongs to."
    ::= { oraEMNGEventEntry  13 }

oraEMNGEventName  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
      "The name of this event."
    ::= { oraEMNGEventEntry  14 }

oraEMNGAssocIncidentId  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "ID of the associated incident with the event (optional)."
    ::= { oraEMNGEventEntry  15 }

oraEMNGAssocIncidentOwner  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Owner of the associated incident with the event (optional)."
    ::= { oraEMNGEventEntry  16 }

oraEMNGAssocIncidentAcked  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Acknowledged status of the associated incident with the event. 1 indicates
acknowledged, 0 indicates unacknowledged."
    ::= { oraEMNGEventEntry  17 }

oraEMNGAssocIncidentStatus  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The status of the associated incident with the event."
    ::= { oraEMNGEventEntry  18 }

oraEMNGAssocIncidentPriority  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The proirity of the associated incident with the event."
    ::= { oraEMNGEventEntry  19 }

oraEMNGAssocIncidentEscLevel  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The Escalation Level of the associated incident with the event."
    ::= { oraEMNGEventEntry  20 }

oraEMNGEventTargetName  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the target to which this event applies. Populated for events
```

```
that are about a target only."
    ::= { oraEMNGEventEntry  21 }

oraEMNGEventTargetNameURL  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "EM Console URL of the target to which this event applies. Populated for
events that are about a target only. Empty if trap size exceeds configured snmp
packet size."
    ::= { oraEMNGEventEntry  22 }

oraEMNGEventTargetType  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The type of the target to which this event applies. Populated for events
that are about a target only."
    ::= { oraEMNGEventEntry  23 }

oraEMNGEventHostName  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the host on which this event originated. Populated for events
that are about a target only."
    ::= { oraEMNGEventEntry  24 }

oraEMNGEventTargetOwner  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The primary administrator of the target on which this event originated.
Empty if trap size exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  25 }

oraEMNGEventTgtLifeCycleStatus  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The life cycle status of the target on which this event originated."
    ::= { oraEMNGEventEntry  26 }

oraEMNGEventTargetVersion  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The version of the target on which this event originated."
    ::= { oraEMNGEventEntry  27 }

oraEMNGEventUserDefinedTgtProp  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The user defined target properties [name,value pair list] of the associated
target with this event. Empty if trap size exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  28 }

oraEMNGEventSourceObjName  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the source object to which this event belongs to. Populated for
events that are about a non-target object only, such as Job."
    ::= { oraEMNGEventEntry  29 }

oraEMNGEventSourceObjNameURL  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "EM Console URL for the source object to which this event belongs to. Empty
if trap size exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  30 }

oraEMNGEventSourceObjType  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The type of the source object to which this event belongs to."
    ::= { oraEMNGEventEntry  31 }

oraEMNGEventSourceObjSubType  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The sub type of the source object to which this event belongs to (Optional
property). Empty if trap size exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  32 }

oraEMNGEventSourceObjOwner  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The primary adminstrator of the source object to which this event belongs
to. (Optional property). Empty if trap size exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  33 }

oraEMNGEventCAJobName  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The Name of the Corrective Action Job associated with this event."
    ::= { oraEMNGEventEntry  34 }

oraEMNGEventCAJobStatus  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The Status of the Corrective Action Job associated with this event."
    ::= { oraEMNGEventEntry  35 }

oraEMNGEventCAJobOwner  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The Owner of the Corrective Action Job associated with this event."
    ::= { oraEMNGEventEntry  36 }

oraEMNGEventCAJobStepOutput  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The job step output from the Corrective Action Job associated with this
event."
    ::= { oraEMNGEventEntry  37 }

oraEMNGEventCAJobType  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The job type from the Corrective Action Job associated with this event."
    ::= { oraEMNGEventEntry  38 }

oraEMNGEventRuleSetName  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the ruleset that caused this notification. Empty if trap size
exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  39 }

oraEMNGEventRuleName  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The name of the rule within the ruleset that caused this notification."
    ::= { oraEMNGEventEntry  40 }

oraEMNGEventRuleOwner  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The owner of the ruleset that caused this notification."
    ::= { oraEMNGEventEntry  41 }

oraEMNGEventSequenceId  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
```

```
     "An EM generated identifier that uniquely identifies current issue until it
is cleared."
    ::= { oraEMNGEventEntry  42 }

oraEMNGEventRCADetails  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Root Cause Analysis details associated with this event if it exists."
    ::= { oraEMNGEventEntry  43 }

oraEMNGEventContextAttrs  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The context attributes associated with this event. Empty if trap size
exceeds configured snmp packet size."
    ::= { oraEMNGEventEntry  44 }

oraEMNGEventUserComments  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The user comments associated with this event. Empty if trap size exceeds
configured snmp packet size."
    ::= { oraEMNGEventEntry  45 }

oraEMNGEventUpdates  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "The updates associated with this event. Empty if trap size exceeds
configured snmp packet size."
    ::= { oraEMNGEventEntry  46 }

oraEMNGEventTypeAttr1  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#1."
    ::= { oraEMNGEventEntry  61 }

oraEMNGEventTypeAttr2  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#2."
    ::= { oraEMNGEventEntry  62 }

oraEMNGEventTypeAttr3  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
```

```
     "Name and value pair as name=value for event type specific attribute#3."
    ::= { oraEMNGEventEntry  63 }

oraEMNGEventTypeAttr4  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#4."
    ::= { oraEMNGEventEntry  64 }

oraEMNGEventTypeAttr5  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#5."
    ::= { oraEMNGEventEntry  65 }

oraEMNGEventTypeAttr6  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#6."
    ::= { oraEMNGEventEntry  66 }

oraEMNGEventTypeAttr7  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#7."
    ::= { oraEMNGEventEntry  67 }

oraEMNGEventTypeAttr8  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#8."
    ::= { oraEMNGEventEntry  68 }

oraEMNGEventTypeAttr9  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#9."
    ::= { oraEMNGEventEntry  69 }

oraEMNGEventTypeAttr10  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#10."
    ::= { oraEMNGEventEntry  70 }

oraEMNGEventTypeAttr11  OBJECT-TYPE
```

```
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#11."
    ::= { oraEMNGEventEntry  71 }

oraEMNGEventTypeAttr12  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#12."
    ::= { oraEMNGEventEntry  72 }

oraEMNGEventTypeAttr13  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#13."
    ::= { oraEMNGEventEntry  73 }

oraEMNGEventTypeAttr14  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#14."
    ::= { oraEMNGEventEntry  74 }

oraEMNGEventTypeAttr15  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#15."
    ::= { oraEMNGEventEntry  75 }

oraEMNGEventTypeAttr16  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#16."
    ::= { oraEMNGEventEntry  76 }

oraEMNGEventTypeAttr17  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#17."
    ::= { oraEMNGEventEntry  77 }

oraEMNGEventTypeAttr18  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
```

```
     "Name and value pair as name=value for event type specific attribute#18."
    ::= { oraEMNGEventEntry  78 }

oraEMNGEventTypeAttr19  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#19."
    ::= { oraEMNGEventEntry  79 }

oraEMNGEventTypeAttr20  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#20."
    ::= { oraEMNGEventEntry  80 }

oraEMNGEventTypeAttr21  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#21."
    ::= { oraEMNGEventEntry  81 }

oraEMNGEventTypeAttr22  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#22."
    ::= { oraEMNGEventEntry  82 }

oraEMNGEventTypeAttr23  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#23."
    ::= { oraEMNGEventEntry  83 }

oraEMNGEventTypeAttr24  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#24."
    ::= { oraEMNGEventEntry  84 }

oraEMNGEventTypeAttr25  OBJECT-TYPE
    SYNTAX DisplayString
    ACCESS  read-only
    STATUS  mandatory
    DESCRIPTION
     "Name and value pair as name=value for event type specific attribute#25."
    ::= { oraEMNGEventEntry  85 }

oraEMNGEvent TRAP-TYPE
```

```
    ENTERPRISE  oraEM4Traps
    VARIABLES   {
          oraEMNGEventNotifType,
          oraEMNGEventMessage, oraEMNGEventMessageURL,
          oraEMNGEventSeverity, oraEMNGEventSeverityCode,
          oraEMNGEventRepeatCount, oraEMNGEventActionMsg,
          oraEMNGEventOccurrenceTime, oraEMNGEventReportedTime,
          oraEMNGEventCategories, oraEMNGEventCategoryCodes,
          oraEMNGEventType, oraEMNGEventName,
          oraEMNGAssocIncidentId, oraEMNGAssocIncidentOwner,
          oraEMNGAssocIncidentAcked, oraEMNGAssocIncidentStatus,
          oraEMNGAssocIncidentPriority, oraEMNGAssocIncidentEscLevel,
          oraEMNGEventTargetName, oraEMNGEventTargetNameURL,
          oraEMNGEventTargetType, oraEMNGEventHostName,
          oraEMNGEventTargetOwner, oraEMNGEventTgtLifeCycleStatus,
          oraEMNGEventTargetVersion, oraEMNGEventUserDefinedTgtProp,
          oraEMNGEventSourceObjName, oraEMNGEventSourceObjNameURL,
          oraEMNGEventSourceObjType, oraEMNGEventSourceObjSubType,
          oraEMNGEventSourceObjOwner, oraEMNGEventCAJobName,
          oraEMNGEventCAJobStatus, oraEMNGEventCAJobOwner,
          oraEMNGEventCAJobStepOutput, oraEMNGEventCAJobType,
          oraEMNGEventRuleSetName, oraEMNGEventRuleName,
          oraEMNGEventRuleOwner, oraEMNGEventSequenceId,
          oraEMNGEventRCADetails, oraEMNGEventContextAttrs,
          oraEMNGEventUserComments, oraEMNGEventUpdates,
          oraEMNGEventTypeAttr1, oraEMNGEventTypeAttr2,
          oraEMNGEventTypeAttr3, oraEMNGEventTypeAttr4,
          oraEMNGEventTypeAttr5, oraEMNGEventTypeAttr6,
          oraEMNGEventTypeAttr7, oraEMNGEventTypeAttr8,
          oraEMNGEventTypeAttr9, oraEMNGEventTypeAttr10,
          oraEMNGEventTypeAttr11, oraEMNGEventTypeAttr12,
          oraEMNGEventTypeAttr13, oraEMNGEventTypeAttr14,
          oraEMNGEventTypeAttr15, oraEMNGEventTypeAttr16,
          oraEMNGEventTypeAttr17, oraEMNGEventTypeAttr18,
          oraEMNGEventTypeAttr19, oraEMNGEventTypeAttr20,
          oraEMNGEventTypeAttr21, oraEMNGEventTypeAttr22,
          oraEMNGEventTypeAttr23, oraEMNGEventTypeAttr24,
          oraEMNGEventTypeAttr25
}
    DESCRIPTION
     "The variables included in the oraEMNGAlert trap."
    ::= 3
END
```

C

SNMP Trap Mappings

The following tables list SNMP trap mappings between Enterprise Manager 12c and previous releases.

C.1 Pre-12c Enterprise Manager Metric Alerts

Prior to Enterprise Manager 12c, metric alerts were sent using the oraEM4Alert trap type. In 12c, the event type corresponding to these alerts is metric alert. The value for oraEMNGEventType in an Enterprise Manager 12c SNMP trap would be set to 'Metric Alert'.

Table C–1 Metric Alert Mappings

Pre-12C OID Number	Pre-12C OID Name	12C OID Number	12C OID Name
1.3.6.1.4.1.111.15.1.1.1.2.1	oraEM4AlertTargetName	1.3.6.1.4.1.111.15.3.1.1.21.1	oraEMNGEventTargetName
1.3.6.1.4.1.111.15.1.1.1.3.1	oraEM4AlertTargetType	1.3.6.1.4.1.111.15.3.1.1.23.1	oraEMNGEventTargetType
1.3.6.1.4.1.111.15.1.1.1.4.1	oraEM4AlertHostName	1.3.6.1.4.1.111.15.3.1.1.24.1	oraEMNGEventHostName
1.3.6.1.4.1.111.15.1.1.1.5.1	oraEM4AlertMetricName	1.3.6.1.4.1.111.15.3.1.1.65.1	oraEMNGEventTypeAttr5
1.3.6.1.4.1.111.15.1.1.1.6.1	oraEM4AlertKeyName	1.3.6.1.4.1.111.15.3.1.1.66.1	oraEMNGEventTypeAttr6
1.3.6.1.4.1.111.15.1.1.1.7.1	oraEM4AlertKeyValue	* See the note below for details	* See the note below for details
1.3.6.1.4.1.111.15.1.1.1.8.1	oraEM4AlertTimeStamp	1.3.6.1.4.1.111.15.3.1.1.10.1	oraEMNGEventReportedTime
1.3.6.1.4.1.111.15.1.1.1.9.1	oraEM4AlertSeverity	1.3.6.1.4.1.111.15.3.1.1.5.1	oraEMNGEventSeverity
1.3.6.1.4.1.111.15.1.1.1.10.1	oraEM4AlertMessage	1.3.6.1.4.1.111.15.3.1.1.3.1	oraEMNGEventMessage
1.3.6.1.4.1.111.15.1.1.1.11.1	oraEM4AlertRuleName	1.3.6.1.4.1.111.15.3.1.1.39.1	oraEMNGEventRuleSetName
1.3.6.1.4.1.111.15.1.1.1.12.1	oraEM4AlertRuleOwner	1.3.6.1.4.1.111.15.3.1.1.41.1	oraEMNGEventRuleOwner
1.3.6.1.4.1.111.15.1.1.1.13.1	oraEM4AlertMetricValue	1.3.6.1.4.1.111.15.3.1.1.68.1	oraEMNGEventTypeAttr8
1.3.6.1.4.1.111.15.1.1.1.14.1	oraEM4AlertContext	1.3.6.1.4.1.111.15.3.1.1.44.1	oraEMNGEventContextAttrs
1.3.6.1.4.1.111.15.1.1.1.15.1	oraEM4AlertCycleGuid	1.3.6.1.4.1.111.15.3.1.1.70.1	oraEMNGEventTypeAttr3
1.3.6.1.4.1.111.15.1.1.1.16.1	oraEM4AlertRepeatCount	1.3.6.1.4.1.111.15.3.1.1.7.1	oraEMNGEventRepeatCount
1.3.6.1.4.1.111.15.1.1.1.17.1	oraEM4AlertUDTargetProperties	1.3.6.1.4.1.111.15.3.1.1.28.1	oraEMNGEventUserDefinedTgtProp
1.3.6.1.4.1.111.15.1.1.1.18.1	oraEM4AlertAck	1.3.6.1.4.1.111.15.3.1.1.17.1	oraEMNGAssocIncidentAcked

Table C–1 (Cont.) Metric Alert Mappings

Pre-12C OID Number	Pre-12C OID Name	12C OID Number	12C OID Name
1.3.6.1.4.1.111.15.1.1.1.19.1	oraEM4AlertAckBy	1.3.6.1.4.1.111.15.3.1.1.16.1	oraEMNGAssocIncidentOwner
1.3.6.1.4.1.111.15.1.1.1.20.1	oraEM4AlertNotifType	1.3.6.1.4.1.111.15.3.1.1.2.1	oraEMNGEventNotifType
1.3.6.1.4.1.111.15.1.1.1.21.1	oraEM4AlertViolationGuid	1.3.6.1.4.1.111.15.3.1.1.42.1	oraEMNGEventSequenceId

C.2 Pre-12C Target Availability Alerts

Prior to Enterprise Manager 12*c*, target availability alerts were sent using oraEM4Alert SNMP trap type. In 12c, the event type corresponding to these alerts is target_availability. Value for oraEMNGEventType in the 12C trap would be set to 'Target Availability'.

Table C–2 Target Availability Alert Mappings

Pre-12C OID Number	Pre-12C OID Name	12C OID Number	12C OID Name
1.3.6.1.4.1.111.15.1.1.1.2.1	oraEM4AlertTargetName	1.3.6.1.4.1.111.15.3.1.1.21.1	oraEMNGEventTargetName
1.3.6.1.4.1.111.15.1.1.1.3.1	oraEM4AlertTargetType	1.3.6.1.4.1.111.15.3.1.1.23.1	oraEMNGEventTargetType
1.3.6.1.4.1.111.15.1.1.1.4.1	oraEM4AlertHostName	1.3.6.1.4.1.111.15.3.1.1.24.1	oraEMNGEventHostName
1.3.6.1.4.1.111.15.1.1.1.5.1	oraEM4AlertMetricName	N/A	N/A
1.3.6.1.4.1.111.15.1.1.1.6.1	oraEM4AlertKeyName	// deprecated in 12C, was always null in 11GC	// deprecated in 12C, was always null in 11GC
1.3.6.1.4.1.111.15.1.1.1.7.1	oraEM4AlertKeyValue	N/A	N/A
1.3.6.1.4.1.111.15.1.1.1.8.1	oraEM4AlertTimeStamp	1.3.6.1.4.1.111.15.3.1.1.10.1	oraEMNGEventReportedTime
1.3.6.1.4.1.111.15.1.1.1.9.1	oraEM4AlertSeverity	1.3.6.1.4.1.111.15.3.1.1.61.1	oraEMNGEventTypeAttr1 //target_status
1.3.6.1.4.1.111.15.1.1.1.10.1	oraEM4AlertMessage	1.3.6.1.4.1.111.15.3.1.1.3.1	oraEMNGEventMessage
1.3.6.1.4.1.111.15.1.1.1.11.1	oraEM4AlertRuleName	1.3.6.1.4.1.111.15.3.1.1.39.1	oraEMNGEventRuleSetName
1.3.6.1.4.1.111.15.1.1.1.12.1	oraEM4AlertRuleOwner	1.3.6.1.4.1.111.15.3.1.1.41.1	oraEMNGEventRuleOwner
1.3.6.1.4.1.111.15.1.1.1.13.1	oraEM4AlertMetricValue	N/A	N/A
1.3.6.1.4.1.111.15.1.1.1.14.1	oraEM4AlertContext	1.3.6.1.4.1.111.15.3.1.1.44.1	oraEMNGEventContextAttrs
1.3.6.1.4.1.111.15.1.1.1.15.1	oraEM4AlertCycleGuid	1.3.6.1.4.1.111.15.3.1.1.66.1	oraEMNGEventTypeAttr6
1.3.6.1.4.1.111.15.1.1.1.16.1	oraEM4AlertRepeatCount	1.3.6.1.4.1.111.15.3.1.1.7.1	oraEMNGEventRepeatCount
1.3.6.1.4.1.111.15.1.1.1.17.1	oraEM4AlertUDTargetProperties	1.3.6.1.4.1.111.15.3.1.1.28.1	oraEMNGEventUserDefinedTgtProp
1.3.6.1.4.1.111.15.1.1.1.18.1	oraEM4AlertAck	1.3.6.1.4.1.111.15.3.1.1.17.1	oraEMNGAssocIncidentAcked
1.3.6.1.4.1.111.15.1.1.1.19.1	oraEM4AlertAckBy	1.3.6.1.4.1.111.15.3.1.1.16.1	oraEMNGAssocIncidentOwner
1.3.6.1.4.1.111.15.1.1.1.20.1	oraEM4AlertNotifType	1.3.6.1.4.1.111.15.3.1.1.2.1	oraEMNGEventNotifType
1.3.6.1.4.1.111.15.1.1.1.21.1	oraEM4AlertViolationGuid	1.3.6.1.4.1.111.15.3.1.1.42.1	oraEMNGEventSequenceId

C.3 Pre-12C Corrective Action Results for Metric Alerts

Prior to Enterprise Manager 12*c*, corrective action results for metric alerts were sent using the oraEM4JobAlert trap type. For Enterprise Manager 12*c*, the event type corresponding to these alerts is metric alert. The value for oraEMNGEventType in the 12*c* trap would be set to 'Metric Alert'.

Table C–3 Corrective Action Results for Metric Alert Mappings

Pre-12C OID Number	Pre-12C OID Name	12C OID Number	12C OID Name
1.3.6.1.4.1.111.15.1.2.1.2.1	oraEM4JobAlertJobName	1.3.6.1.4.1.111.15.3.1.1.34.1	oraEMNGEventCAJobName
1.3.6.1.4.1.111.15.1.2.1.3.1	oraEM4JobAlertJobOwner	1.3.6.1.4.1.111.15.3.1.1.36.1	oraEMNGEventCAJobOwner
1.3.6.1.4.1.111.15.1.2.1.4.1	oraEM4JobAlertJobType	1.3.6.1.4.1.111.15.3.1.1.38.1	oraEMNGEventCAJobType
1.3.6.1.4.1.111.15.1.2.1.5.1	oraEM4JobAlertJobStatus	1.3.6.1.4.1.111.15.3.1.1.35.1	oraEMNGEventCAJobStatus
1.3.6.1.4.1.111.15.1.2.1.6.1	oraEM4JobAlertTargets	1.3.6.1.4.1.111.15.3.1.1.23.1	oraEMNGEventTargetType
		1.3.6.1.4.1.111.15.3.1.1.21.1	oraEMNGEventTargetName
1.3.6.1.4.1.111.15.1.2.1.7.1	oraEM4JobAlertTimeStamp	1.3.6.1.4.1.111.15.3.1.1.10.1	oraEMNGEventReportedTime
1.3.6.1.4.1.111.15.1.2.1.8.1	oraEM4JobAlertRuleName	1.3.6.1.4.1.111.15.3.1.1.39.1	oraEMNGEventRuleSetName
1.3.6.1.4.1.111.15.1.2.1.9.1	oraEM4JobAlertRuleOwner	1.3.6.1.4.1.111.15.3.1.1.41.1	oraEMNGEventRuleOwner
1.3.6.1.4.1.111.15.1.2.1.10.1	oraEM4JobAlertMetricName	1.3.6.1.4.1.111.15.3.1.1.65.1	oraEMNGEventTypeAttr5
1.3.6.1.4.1.111.15.1.2.1.11.1	oraEM4JobAlertMetricValue	1.3.6.1.4.1.111.15.3.1.1.68.1	oraEMNGEventTypeAttr8
1.3.6.1.4.1.111.15.1.2.1.12.1	oraEM4JobAlertContext	1.3.6.1.4.1.111.15.3.1.1.44.1	oraEMNGEventContextAttrs
1.3.6.1.4.1.111.15.1.2.1.13.1	oraEM4JobAlertKeyName	1.3.6.1.4.1.111.15.3.1.1.66.1	oraEMNGEventTypeAttr6
1.3.6.1.4.1.111.15.1.2.1.14.1	oraEM4JobAlertKeyValue	1.3.6.1.4.1.111.15.3.1.1.69.1	oraEMNGEventTypeAttr9
1.3.6.1.4.1.111.15.1.2.1.15.1	oraEM4JobAlertSeverity	1.3.6.1.4.1.111.15.3.1.1.5.1	oraEMNGEventSeverity
1.3.6.1.4.1.111.15.1.2.1.16.1	oraEM4JobAlertJobId	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.17.1	oraEM4JobAlertJobExecId	N/A	N/A

C.4 Corrective Action Results for Target Availability

Prior to Enterprise Manager 12c, corrective action results for target availability alerts were sent using the oraEM4JobAlert trap type. In 12c, the event type corresponding to these alerts is target_availability alert. The value for oraEMNGEventType in the 12*c* trap would be set to 'Metric Alert'.

Table C–4 Target Availability Mappings

Pre-12C OID Number	Pre-12C OID Name	12C OID Number	12C OID Name
1.3.6.1.4.1.111.15.1.2.1.2.1	oraEM4JobAlertJobName	1.3.6.1.4.1.111.15.3.1.1.34.1	oraEMNGEventCAJobName
1.3.6.1.4.1.111.15.1.2.1.3.1	oraEM4JobAlertJobOwner	1.3.6.1.4.1.111.15.3.1.1.36.1	oraEMNGEventCAJobOwner
1.3.6.1.4.1.111.15.1.2.1.4.1	oraEM4JobAlertJobType	1.3.6.1.4.1.111.15.3.1.1.38.1	oraEMNGEventCAJobType
1.3.6.1.4.1.111.15.1.2.1.5.1	oraEM4JobAlertJobStatus	1.3.6.1.4.1.111.15.3.1.1.35.1	oraEMNGEventCAJobStatus
1.3.6.1.4.1.111.15.1.2.1.6.1	oraEM4JobAlertTargets	1.3.6.1.4.1.111.15.3.1.1.23.1	oraEMNGEventTargetType and
		1.3.6.1.4.1.111.15.3.1.1.21.1	oraEMNGEventTargetName
1.3.6.1.4.1.111.15.1.2.1.7.1	oraEM4JobAlertTimeStamp	1.3.6.1.4.1.111.15.3.1.1.10.1	oraEMNGEventReportedTime

Table C–4 (Cont.) Target Availability Mappings

Pre-12C OID Number	Pre-12C OID Name	12C OID Number	12C OID Name
1.3.6.1.4.1.111.15.1.2.1.8.1	oraEM4JobAlertRuleName	1.3.6.1.4.1.111.15.3.1.1.39.1	oraEMNGEventRuleSetName
1.3.6.1.4.1.111.15.1.2.1.9.1	oraEM4JobAlertRuleOwner	1.3.6.1.4.1.111.15.3.1.1.41.1	oraEMNGEventRuleOwner
1.3.6.1.4.1.111.15.1.2.1.10.1	oraEM4JobAlertMetricName	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.11.1	oraEM4JobAlertMetricValue	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.12.1	oraEM4JobAlertContext	1.3.6.1.4.1.111.15.3.1.1.44.1	oraEMNGEventContextAttrs
1.3.6.1.4.1.111.15.1.2.1.13.1	oraEM4JobAlertKeyName	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.14.1	oraEM4JobAlertKeyValue	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.15.1	oraEM4JobAlertSeverity	1.3.6.1.4.1.111.15.3.1.1.61.1	oraEMNGEventTypeAttr5 // target_status
1.3.6.1.4.1.111.15.1.2.1.16.1	oraEM4JobAlertJobId	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.17.1	oraEM4JobAlertJobExecId	N/A	N/A

C.5 Job Status Change

Prior to Enterprise Manager 12c , job status change was sent using oraEM4JobAlert trap type. For 12c, the event type corresponding to these alerts is the job_status_change alert. The value for the oraEMNGEventType in the 12c trap would be set to 'Job Status Change'.

Table C–5 Job Status Change Mappings

Pre-12c OID Number	Pre-12c OID Name	12c OID Number	12c OID Name
1.3.6.1.4.1.111.15.1.2.1.2.1	oraEM4JobAlertJobName	1.3.6.1.4.1.111.15.3.1.1.29.1	oraEMNGEventSourceObjName
1.3.6.1.4.1.111.15.1.2.1.3.1	oraEM4JobAlertJobOwner	1.3.6.1.4.1.111.15.3.1.1.33.1	oraEMNGEventSourceObjOwner
1.3.6.1.4.1.111.15.1.2.1.4.1	oraEM4JobAlertJobType	1.3.6.1.4.1.111.15.3.1.1.32.1	oraEMNGEventSourceObjSubType
1.3.6.1.4.1.111.15.1.2.1.5.1	oraEM4JobAlertJobStatus	1.3.6.1.4.1.111.15.3.1.1.62.1	oraEMNGEventTypeAttr2
1.3.6.1.4.1.111.15.1.2.1.6.1	oraEM4JobAlertTargets	1.3.6.1.4.1.111.15.3.1.1.23.1	oraEMNGEventTargetType and
		1.3.6.1.4.1.111.15.3.1.1.21.1	oraEMNGEventTargetName
1.3.6.1.4.1.111.15.1.2.1.7.1	oraEM4JobAlertTimeStamp	1.3.6.1.4.1.111.15.3.1.1.10.1	oraEMNGEventReportedTime
1.3.6.1.4.1.111.15.1.2.1.8.1	oraEM4JobAlertRuleName	1.3.6.1.4.1.111.15.3.1.1.39.1	oraEMNGEventRuleSetName
1.3.6.1.4.1.111.15.1.2.1.9.1	oraEM4JobAlertRuleOwner	1.3.6.1.4.1.111.15.3.1.1.41.1	oraEMNGEventRuleOwner
1.3.6.1.4.1.111.15.1.2.1.10.1	oraEM4JobAlertMetricName	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.11.1	oraEM4JobAlertMetricValue	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.12.1	oraEM4JobAlertContext	1.3.6.1.4.1.111.15.3.1.1.44.1	oraEMNGEventContextAttrs
1.3.6.1.4.1.111.15.1.2.1.13.1	oraEM4JobAlertKeyName	N/A	N/A

Table C–5 (Cont.) Job Status Change Mappings

Pre-12c OID Number	Pre-12c OID Name	12c OID Number	12c OID Name
1.3.6.1.4.1.111.15.1.2.1.14.1	oraEM4JobAlertKeyValue	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.15.1	oraEM4JobAlertSeverity	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.16.1	oraEM4JobAlertJobId	N/A	N/A
1.3.6.1.4.1.111.15.1.2.1.17.1	oraEM4JobAlertJobExecId	1.3.6.1.4.1.111.15.3.1.1.61.1	oraEMNGEventTypeAttr1

* **Note**: When mapping 1.3.6.1.4.1.111.15.1.1.1.7.1 oraEM4AlertKeyValue to 12g metric_alert event to 1.3.6.1.4.1.111.15.1.1.1.7.1 oraEM4AlertKeyValue, you need to look at 1.3.6.1.4.1.111.15.3.1.1.84.1 oraEMNGEventTypeAttr24.

```
if oraEMNGEventTypeAttr24 is null
       then
         oraEM4AlertKeyValue is null

       if oraEMNGEventTypeAttr24 value =  "Number of keys=1"
         oraEM4AlertKeyValue --> oraEMNGEventTypeAttr8

       if oraEMNGEventTypeAttr24 value =  "Number of keys=x" where x is greater
than 1
         => check the values for the following pairs of attributes.
            <oraEMNGEventTypeAttr10, oraEMNGEventTypeAttr11>
            <oraEMNGEventTypeAttr12, oraEMNGEventTypeAttr13>
            <oraEMNGEventTypeAttr14, oraEMNGEventTypeAttr15>
            <oraEMNGEventTypeAttr16, oraEMNGEventTypeAttr17>
            <oraEMNGEventTypeAttr18, oraEMNGEventTypeAttr19>
            <oraEMNGEventTypeAttr20, oraEMNGEventTypeAttr21>
            <oraEMNGEventTypeAttr22, oraEMNGEventTypeAttr23>
            ...
            ...
```

As many pairs as the number of parts present in the key would be populated, the rest of will be set to null.

For each non-null pair of attributes, the first attribute provides the name for that part of the key and second attribute provides the value for that part of the key.

Important: OID 1.3.6.1.4.1.111.15.3.1.1.13.1 specifies the event type. Examples:

For a metric_alert event type

oraEMNGEventType=Metric Alert

For a target_availability event type,

oraEMNGEventType=Target Availability

For a job_status_change event type

oraEMNGEventType=Job Status Change

D

Overview of Target Availability States

The following sections summarize available states and how to set real-time target status updates.

D.1 Target Availability State Changes

Enterprise Manager displays a comprehensive array of target availability statuses in the form of informational icons. Various Cloud Control console pages display these icons to indicate the current status of targets in the repository.

The following table contains all available target availability status icons and their meaning.

Icon	Availability State	Description
N/A	N/A	Target availability state does not apply.
⬇	Down	Target is down. The target may be unreachable due to the fact that the Agent is down. If the Agent was brought down as part of planned maintenance, consider creating a blackout on the Agent.
⬆	Up	Target is up.
⊗	Availability Evaluation Error	An error occurred while attempting to determine target availability status. A target availability evaluation error can be caused by metric collection errors, the Agent being unreachable, or network problems.
⚙⬇	Agent Down	The Agent monitoring the target is down. If an Agent was brought down in error it should be restarted. If Agent was brought down as part of planned maintenance, consider creating a blackout on the Agent.
⬆⊗	Agent Down, Target Up	The Agent monitoring the target is down, however, the target is currently up but not monitored. To troubleshoot, go to the Agent homepage and run the *Symptom Analysis* tool located next to the Status field.
⚙⊗	Agent Unreachable	The Agent is not reachable. Specifically, the Oracle Management Service (OMS) cannot communicate with the Agent. An Agent is generally unreachable when it is down, when it is blocked by the OMS, or when the Management Agent host is down. A Management Agent may also be unreachable due to network problems or certain other issues.

Icon	Availability State	Description
	Agent Unreachable (Under Migration)	The Agent is unreachable because it is in the process of being migration.
	Agent Unreachable (Cannot Write to File System)	The Agent cannot write to the file system. Check the Agent file system for accessibility. To troubleshoot problems, navigate to the Agent home page from the Enterprise Manager console and run the *Symptom Analysis* tool (located next to the *Status* field).
	Agent Unreachable (Collections Disabled)	Agent metric collection has been disabled. Check that the Agent can upload to the OMS. To troubleshoot problems, navigate to the Agent home page from the Enterprise Manager console and run the *Symptom Analysis* tool (located next to the Status field).
	Agent Unreachable (Disk Full)	The Agent file system is full. Check the Agent file system for available space. To troubleshoot problems, navigate to the Agent home page from the Enterprise Manager console and run the *Symptom Analysis* tool (located next to the Status field).
	Agent Unreachable (Post Blackout)	The Agent is unreachable because the first alert condition has not yet occurred since the blackout period ended.
	Agent Blocked (Blocked Manually)	The Agent has been blocked manually. Unblock the Agent.
	Agent Blocked (Plug-in Mismatch)	The Agent has been blocked due to a plug-in mismatch. If the Agent has been restored from a backup, perform an Agent Resync.
N	Agent Blocked (Bounce Counter Mismatch)	The Agent has been blocked due to Bounce Counter mismatch. If the Agent has been restored from a backup, perform an Agent Resync.
	Agent Unreachable (Agent Misconfigured)	The Agent is configured for communication with a different OMS. Check the Agent configuration to ensure the Agent is communicating with the correct OMS.
	Agent Unreachable (Communication Broken)	The Agent is unreachable due to a communication break between the Agent and the OMS.
	Blackout	The target is currently blacked out.
	Status Pending	The target status is currently unknown.
	Status Pending (Target Addition in Progress)	The target status is currently unknown. Target addition is in progress.
	Status Pending (Post Blackout)	The target status is currently unknown. Blackout has recently ended on this target and *Availability Status* is pending.

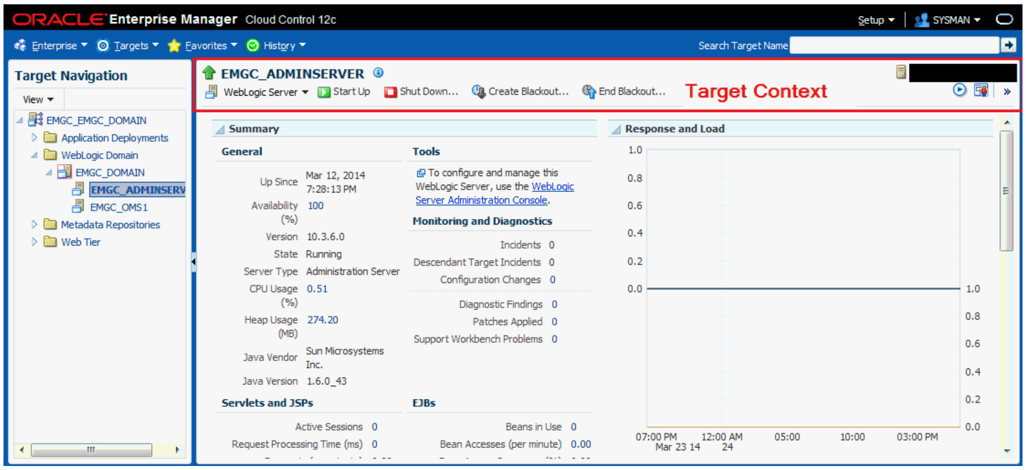
Icon	Availability State	Description
	Status Pending (Post Metric Error)	A metric error has recently ended on the target and Availability Status is pending. To troubleshoot, refer to My Oracle Support article Enterprise Manager 12c: How to run the "Targets Status Diagnostics Report" to Troubleshoot Target Status Availability Issues (up, down, metric collection error, pending, unreachable) for all Targets (Doc ID 1546575.1).

D.2 Target Status: Real-time Updates

Enterprise Manager can provide real-time status updates for specific target context UI pages without having to refresh the browser page or wait for the status change to be detected by the Response metric, where the collection interval delay may take anywhere from a few tenths of a second to a few minutes.

A *target context* page displays information about a particular target. It has a context header at the top showing information such as target name, target type, target status, or target menu. The following figure shows a WebLogic Server page displaying target status information.

Figure D–1 Target Context Area



Up Since: Mar 12, 2014 7:28:13 PM
Availability (%): 100
Version: 10.3.6.0
State: Running
Server Type: Administration Server
CPU Usage (%): 0.51
Heap Usage (MB): 274.20
Java Vendor: Sun Microsystems Inc.
Java Version: 1.6.0_43

To configure and manage this WebLogic Server, use the WebLogic Server Administration Console.

Incidents: 0
Descendant Target Incidents: 0
Configuration Changes: 0
Diagnostic Findings: 0
Patches Applied: 0
Support Workbench Problems: 0

Active Sessions: 0
Request Processing Time (ms): 0
Beans in Use: 0
Bean Accesses (per minute): 0.00

Real-time status updates are available for the following target types:

- Agent
- Host
- Database Instance (Single Instance Database Only)
- Application Deployment
- WebLogic Server

As mentioned earlier, this feature allows target context pages to be updated automatically when that target's status changes (from *up* to *down*, for example). By default, real-time update is off. You must toggle real-time update on or off using the *oracle.sysman.core.uifwk.realTimeUIEnabled* OMS property.

To enable real-time updates, run the following emctl command:

```
emctl set property -name oracle.sysman.core.uifwk.realTimeUIEnabled -value true
```

Index