Oracle® Enterprise Manager

Oracle Database and Database-Related Metric Reference Manual

11*g* Release 1 (11.1.0.1)

E16285-01

May 2010

ORACLE®

Oracle Enterprise Manager Oracle Database and Database-Related Metric Reference Manual, 11*g* Release 1 (11.1.0.1)

E16285-01

Contents

3 Cluster Database

4 Database Instance

Preface

This manual is a compilation of the Oracle Database and database-related target metrics provided in Oracle Enterprise Manager.

Audience

This document is intended for Oracle Enterprise Manager users interested in Oracle Database and database-related target metrics.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, see the following manuals in the Oracle Enterprise Manager 11*g* Release 1 documentation set:

- *Oracle Enterprise Manager Grid Control Basic Installation Guide*
- *Oracle Enterprise Manager Grid Control Advanced Installation and Configuration Guide*
- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Quick Start Guide*
- *Oracle Enterprise Manager Administration*
- *Oracle Enterprise Manager Framework, Host, and Services Metric Reference Manual*

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.

How to Use This Manual

The *Oracle Enterprise Manager Oracle Database and Database-Related Metric Reference Manual* (hereafter referred to as the *Oracle Database and Database-Related Metric Reference Manual*) lists all the Oracle Database and database-related target metrics that Enterprise Manager monitors. This manual compiles in one place all the database and database-related target metric help available online, eliminating the need to have the Database Control Console up and running.

This preface describes:

Structure of the Oracle Database and Database-Related Metric Reference Manual

This manual contains a chapter for the Oracle Database target and database-related targets for which there are metrics.

The metrics in each chapter are in alphabetical order according to category.

Metric Information

The information for each metric comprises a description, summary of the metric's "vital statistics", data source (if available), and user action. The following list provides greater detail:

- Description

  Explanation following the metric name. This text defines the metric and, when available, provides additional information pertinent to the metric.

- Metric Summary

  Explains in table format the target version, collection frequency, upload frequency, operator, default warning threshold, default critical threshold, consecutive number of occurrences preceding notification, and alert text for the metric. Examples follow.

- Data Source

  How the metric is calculated. In some metrics, data source information is not available.

- User Action

  Suggestions of how to solve the problem causing the alert.

Examples of Metric Summary Tables

This section provides examples of Metric Summary tables you will see in the *Oracle Database and Database-Related Metric Reference Manual*.

When default thresholds are not defined for a metric, only the target version and collection frequency are available.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

The following table shows a metric where the server evaluation frequency is the same as the collection frequency.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 10 Minutes	After Every Sample	>	10000000	12500000	1	Bytes sent by the server are %value%

The following table shows a metric where the server evaluation frequency is different from the collection frequency.

Target Version	Server Evaluation Frequency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Definitions of Columns in Metric Summary Tables

As previously mentioned, the Metric Summary table is part of the overall metric information. The following table provides descriptions of columns in the Metric Summary table.

Column Header	Column Definition
Target Version	Version of the target, for example, 9.0.2.x and 10.1.0.x. The x at the end of a version (for example, 9.0.2.x) represents the subsequent patchsets associated with that release.
Evaluation and Collection Frequency	The rate at which the metric is collected and evaluated to determine whether it has crossed its threshold. The evaluation frequency is the same as the collection frequency.
Server Evaluation Frequency	The rate at which the metric is evaluated to determine whether it has crossed its threshold. For server-generated alerts, the evaluation frequency is determined by Oracle Database internals. For example, if the evaluation frequency is 10 minutes, then when the Average File Write Time degrades to the point an alert should trigger, it could be almost 10 minutes before Enterprise Manager receives indication of the alert. This column is present in the Metric Collection Summary table only for Oracle Database 10*g* metrics.
Collection Frequency	The rate at which the Management Agent collects data. The collection frequency for a metric comes from the Enterprise Manager default collection file for that target type.

Column Header	Column Definition
Upload Frequency	The rate at which the Management Agent moves data to the Management Repository. For example, upload every n^{th} collection. The upload frequency for a metric comes from the Enterprise Manager default collection file for that target type. This column is present in the Metric Collection Summary table only when the Upload Frequency is different from the Collection Frequency.
Comparison Operator	The comparison method Enterprise Manager uses to evaluate the metric value against the threshold values.
Default Warning Threshold	Value that indicates whether a warning alert should be initiated. If the evaluation of the warning threshold value returns a result of TRUE for the specified number of consecutive occurrences defined for the metric, an alert triggers at the warning severity level.
Default Critical Threshold	Value that indicates whether a critical alert should be initiated. If the evaluation of the critical threshold value returns a result of TRUE for the specified number of consecutive occurrences defined for the metric, an alert triggers at the critical severity level.
Consecutive Number of Occurrences Preceding Notification	Consecutive number of times a metric's value reaches either the warning threshold or critical threshold before a notification is sent.
Alert Text	Message indicating why the alert was generated. Words that display between percent signs (%) denote variables. For example, `Disk Utilization for %keyValue% is %value%%` could translate to `Disk Utilization for d0 is 80%`.

Abbreviations and Acronyms

To reduce the page count in this document, the following abbreviations and acronyms are used:

Abbreviation/Acronym	Name
Agent	Oracle Management Agent
Database	Oracle Database
Listener	Oracle Listener

Background Information on Metrics, Thresholds, and Alerts

A metric is a unit of measurement used to determine the health of a target. It is through the use of metrics and associated thresholds that Enterprise Manager sends out alerts notifying you of problems with the target.

Thresholds are boundary values against which monitored metric values are compared. For example, for each disk device associated with the Disk Utilization (%) metric, you can define a different warning and critical threshold. Some of the thresholds are predefined by Oracle, others are not.

Once a threshold is reached, an alert is generated. An alert is an indicator signifying that a particular condition has been encountered and is triggered when one of the following conditions is true:

- A threshold is reached.
- An alert has been cleared.
- The availability of a monitored service changes. For example, the availability of an application server changes from up to down.

- A specific condition occurs. For example, an alert is triggered whenever an error message is written to a database alert log file.

Alerts are detected through a polling-based mechanism by checking for the monitored condition from a separate process at regular, predefined intervals.

> **See Also:** See the *Oracle Enterprise Manager Concepts* manual and the Enterprise Manager online help for additional information about metrics, thresholds, and alerts

Editing

Out of the box, Enterprise Manager comes with thresholds for critical metrics. Warning and critical thresholds are used to generate an alert, letting you know of impending problems so that you can address them in a timely manner.

To better suit the monitoring needs of your organization, you can edit the thresholds provided by Enterprise Manager and define new thresholds. When defining thresholds, the key is to choose acceptable values to avoid unnecessary alerts, while still being notified of issues in a timely manner.

You can establish thresholds that will provide pertinent information in a timely manner by defining metric baselines that reflect how your system runs for a normal period of time.

The metrics listed on the Edit Thresholds page are either default metrics provided by Oracle or metrics whose thresholds you can change.

Specifying Multiple Thresholds

The Specifying Multiple Thresholds functionality allows you to define various subsets of data that can have different thresholds. By specifying multiple thresholds, you can refine the data used to trigger alerts, which are one of the key benefits of using Enterprise Manager.

The key in specifying multiple thresholds is to determine how the comparison relates to the metric threshold as a whole. What benefit will be realized by defining a more stringent or lax threshold for that particular device, mount point, and so on?

For example, using the Average Disk I/O Service Time metric, you can define warning and critical thresholds to be applied to all disks (sd0 and sd1), or you can define different warning and critical thresholds for a specific disk (sd0). This allows you to adjust the thresholds for sd0 to be more stringent or lax for that particular disk.

Accessing Metrics Using the Grid Control Console

To access metrics in the Grid Control Console, use the All Metrics page associated with a particular target by doing the following:

1. From the Grid Control Console, choose the target.
2. On the target's home page, click All Metrics in the Related Links section.
3. On the All Metrics page, choose the metric of interest and click Help. The help for that metric displays.

1

Automatic Storage Management

The Automatic Storage Management (ASM) metrics provide for each metric the following information:

- Description
- Metric Summary. The metric summary can include some or all of the following: target version, evaluation frequency, collection frequency, upload frequency, operator, default warning threshold, default critical threshold, consecutive number of occurrences preceding notification, and alert text.
- Multiple Thresholds (where applicable)
- Data Source
- User Action

1.1 Alert Log

This metric signifies that the ASM target being monitored has generated errors to the ALERT log file since the last sample time. The ALERT log file is a special trace file containing a chronological log of messages and errors.

Critical Alerts are generated for different type of failure, for example, when archiver hung, data block corrupted and Media failure are found in the alert log with the following error code (ORA-00257, 16038, 01157,01578,27048). The metric shows the user the line number and time when the error occurred.

Warning alerts are also generated when Session Terminated Error Stack (ORA- 00603) are present in the alert log. Many other critical alerts also occur when the Ora-15130 (Disk Group is being dismounted), Ora-15050 (Disk contains errors) and Ora-15051 (File contains errors) are present in alert log.

You can edit the metric threshold and change the value of error you want to collect under a different head. Also, you can modify the warning and critical alert values.

This metric is collected at a time interval of 15 minutes. You can change the threshold limit as per your requirements.

1.1.1 Alert Log Error Stack

This metric contains the information about different ORA- errors present in the alert log file. It ignores error patterns like ORA-0*(54 | 1142 | 1146) present in the alert log file and generate a warning alert when ORA-0*600x, ORA-07445, ORA-04 [0-9][0-9][0-9])[^0-9] errors are present.

Edit the metric threshold and change the value of the ORA- error to generate the warning and critical alert for a different set of ORA- errors.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	MATCH	ORA-0*(600?|7445|4[0-9][0-9][0-9])[^0-9]	Not Defined	1[1]	ORA-error stack (%errCodes%) logged in %alertLogName%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric column you can set different warning and critical threshold values for each for each "Timestamp/LineNumber" object.

If warning or critical threshold values are currently set for any "Timestamp/LineNumber" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Timestamp/LineNumber" object, use the Edit Thresholds page. .

Data Source

The data comes from Alert Log Files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent. The alert log file is scanned for the ORA- errors ignoring the patterns like ORA-0*(54|1142|1146).

User Action

Examine ALERT log for additional information.

1.1.2 Alert Log Error Stack Trace File Name

This metric provides information about the trace file name in which ORA- errors are present. It provides the detail of the trace file name and the line at which the error has occurred.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Evaluation and Collection Frequency
10.1.0.x; 10.2.0.x	Every 5 Minutes

Data Source

The data comes from the Alert Log files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

1.1.3 Alert Log Name

This metric provides the information about the alert log file in which ORA- errors are present. It displays the file name and the line at which the error has occurred.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Evaluation and Collection Frequency
10.1.0.x; 10.2.0.x	Every 5 Minutes

Data Source

The data comes from Alert Log Files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Examine ALERT log for additional information.

1.1.4 Archive Hung Error Stack

This metric contains the information about different ORA- errors, which indicate the presence of Archive Hung in the alert log files. The errors ORA-00257 and ORA-16038 in the alert log indicates an archive-hung problem. This also generates a critical alert when these problems are found in alert logs.

You can edit the metric threshold and change the value of the error you want to collect under a different head. Also, the warning and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	CONTAINS	Not Defined	ORA-	1[1]	The archiver hung at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric column you can set different warning and critical threshold values for each for each "Timestamp/LineNumber" object.

If warning or critical threshold values are currently set for any "Timestamp/LineNumber" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Timestamp/LineNumber" object, use the Edit Thresholds page.

Data Source

The data comes from Alert Log Files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent. Alert log file is scanned for the ORA-00257 and ORA-16038 error.

User Action

Examine ALERT log for additional information.

1.1.5 Data Block Corruption Error Stack

This metric contains the information about different ORA- errors, which indicate the presence of Data Block Corruption errors in the alert log files. The errors ORA- 01157, ORA-01578, and ORA-27048 in the alert log indicates Data Block Corruption problems. This also generates a critical alert when these problems are found in alert logs.

You can edit the metric threshold and change the value of the error you want to collect under a different head. Also, the warning and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	CONTAINS	Not Defined	ORA-	1[1]	The data block was corrupted at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric column you can set different warning and critical threshold values for each for each "Timestamp/LineNumber" object.

If warning or critical threshold values are currently set for any "Timestamp/LineNumber" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Timestamp/LineNumber" object, use the Edit Thresholds page.

Data Source

The data comes from Alert Log Files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent. Alert log file is scanned for the ORA- 01157, ORA-01578, and ORA-27048 error.

User Action

Examine ALERT log for additional information.

1.1.6 Media Failure Error Stack

This metric contains the information about different ORA- errors, which indicate the presence of Media Failure Errors in the alert log files. The errors ORA-15130,ORA-15049, ORA-15050 and ORA-15051 in the alert log indicates Media Failure Error problems. This generates a critical alert when these problems are found in alert logs.

You can edit the metric threshold and change the value of the error you want to collect under a different head. Also the warning and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	CONTAINS	Not Defined	ORA-	1[1]	Media failure was detected at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric column you can set different warning and critical threshold values for each for each "Timestamp/LineNumber" object.

If warning or critical threshold values are currently set for any "Timestamp/LineNumber" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Timestamp/LineNumber" object, use the Edit Thresholds page.

Data Source

The data comes from Alert Log Files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the

home of the Oracle Management Agent. Alert log file is scanned for the ORA-15130,ORA-15049, ORA-15050and ORA-15051 error.

User Action

Examine ALERT log for additional information.

1.1.7 Session Terminated Error Stack

This metric contains the information about different ORA- errors, which indicate the presence of Session Terminated problems in the alert log files. The ORA- 00603 error in the alert log indicates Session Terminated problems. This also generates a warning alert when these problems are found in alert logs.

You can edit the metric threshold and change the value of the error you want to collect under a different head. Also, the warning and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	CONTAINS	ORA-	Not Defined	1[1]	A session was terminated at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric column you can set different warning and critical threshold values for each for each "Timestamp/LineNumber" object.

If warning or critical threshold values are currently set for any "Timestamp/LineNumber" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Timestamp/LineNumber" object, use the Edit Thresholds page.

Data Source

The data comes from Alert Log Files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent. The alert log file is scanned for the ORA-00603 error.

User Action

Examine the ALERT log for additional information.

1.2 Alert Log Error Status

This metric displays the number of times an Alert has been generated for the Alert log metric. It provides information about the current status of different errors present in the alert log file.

This Metric is part of 10*g* Release 2 and generates a warning alert with any occurrence of ORA- Error [excluding ORA-0*(54 | 1142 | 1146)]. It also generates a Warning alert when it detects an Archiver Hung Error, Data Block Corruption Error, Media Failure Error and Session Terminated Error.

This metric is collected with the help Alert Log Metric, and the time interval for collection 5 Minutes. You can change the threshold limit count for the Warning alert and critical alert as required.

1.2.1 Archiver Hung Alert Log Error Status

This metric signifies the number of times the Archiver Hung error (ORA-00257 and ORA-16038) has been generated in the Alert log metric. It gives user an idea about the current status of Archiver Hung error present in the alert log file. This also generates a warning alert when this count is greater than zero.

User can edit the metric threshold and change the value of error he/she wants to collect under different head. Also the warning alert and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	>	0	Not Defined	1	Archiver hung errors have been found in the alert log.

Data Source

Calculated based on the Archive Hung Error Stack Metric rollup.

User Action

Examine ALERT log for additional information. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

1.2.2 Data Block Corruption Alert Log Error Status

This metric signifies the number of times the Data Block Corruption error (ORA-01157, ORA-01578, and ORA-27048) has been generated in the Alert log metric. It gives user an idea about the current status of Data Block Corruption error present in the alert log file. This also generates a warning alert when this count is greater than zero.

User can edit the metric threshold and change the value of error he/she wants to collect under different head. Also the warning alert and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	>	0	Not Defined	1	Data block corruption errors have been found in the alert log.

Data Source

Calculated based on the Data Block Corruption Error Stack Metric rollup.

User Action

Examine ALERT log for additional information. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

1.2.3 Generic Alert Log Error Status

This metric signifies the number of times the Generic Alert error (ORA-0*600x, ORA-07445, ORA-04 [0-9][0-9][0-9])[^0-9]) has been generated in the Alert log metric. It gives user an idea about the current status of Generic Alert (ORA-) error present in the alert log file. This also generates a warning alert when this count is greater than zero.

User can edit the metric threshold and change the value of error he/she wants to collect under different head. Also the warning alert and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	>	0	Not Defined	1	%value% distinct types of ORA-errors have been found in the alert log.

Data Source

Calculated based on the Generic Alert Error Stack Metric rollup.

User Action

Examine ALERT log for additional information.

1.2.4 Media Failure Alert Log Error Status

This metric signifies the number of times the Media Failure Alert error (ORA-15130,ORA-15049, ORA-15050and ORA-15051) has been generated in the Alert log metric. It gives user an idea about the current status of Media Failure Alert (ORA-) error present in the alert log file. This also generates a warning alert when this count is greater than zero.

User can edit the metric threshold and change the value of error he/she wants to collect under different head. Also the warning alert and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	>	0	Not Defined	1	Media failure errors have been found in the alert log.

Data Source

Calculated based on the Media Failure Alert Error Stack Metric rollup.

User Action

Examine ALERT log for additional information. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

1.2.5 Session Terminated Alert Log Error Status

This metric signifies the number of times the Session Terminated Alert error (ORA-00603) has been generated in the Alert log metric. It gives user an idea about the current status of Session Terminated Alert (ORA-) error present in the alert log file. This also generates a warning alert when this count is greater than zero.

User can edit the metric threshold and change the value of error he/she wants to collect under different head. Also the warning alert and critical alert values can be modified or set.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x	Every 5 Minutes	After Every Sample	>	0	Not Defined	1	Session terminations have been found in the alert log.

Data Source

Calculated based on the Session Terminated Alert Error Stack Metric rollup.

User Action

Examine ALERT log for additional information. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

1.3 ASM Cluster File System Metrics

The ASM Cluster File System metrics show the space used by all the ASM Cluster File Systems. These metrics are used to collect information about the ASM Cluster File System space usage and are used to show the trend of ASM Cluster File System space usage in the application. These metrics collect information for both mounted and dismounted ASM Cluster File Systems. This information is used to determine the following metrics for Space Usage: Allocated Space (GB), Size (GB), Free (GB), Used (GB), and Used (%). These metrics also collect information whether the ASM Cluster File System is corrupt. For dismounted ASM Cluster File Systems, 0 is returned for the Free (GB), Used (GB), and Used (%) metrics.

These metrics only collect information about the ASM Cluster File System that is not specific to a node in a cluster. They collect Space Usage information which is the same across all nodes in the cluster. Information like State and Availability of the ASM Cluster File System can be different across the nodes in a cluster and is collected by the ASM Cluster File System State metrics.

These metrics generate a warning alert if the ASM Cluster File System is 85% used and a critical alert if 97% used. These metrics also generate a critical alert if the ASM Cluster File System has sections that are corrupt.

These metrics are collected at a time interval of 15 minutes. You can change the threshold limit as required.

1.3.1 Corrupt

This metric shows if the mounted ASM Cluster File System has sections that are corrupt. A value of "TRUE" for this metric indicates that there are sections that are corrupt and hence the "Check and Repair" operation should be run on the ASM Cluster File System to fix it. For dismounted ASM Cluster File Systems, it returns a value of Null for this metric.

This metric generates a warning alert if the ASM Cluster File System is dismounted on a given host. The metric also generates a critical alert if the mounted ASM Cluster File System is not available on a host.

This metric is collected at a time interval of 15 minutes. You can change the threshold limit as required.

This metric is collected with the help of a SQL query which queries the V$ASM_ FILESYSTEM, V$ASM_VOLUME, V$ASM_OFSVOLUMES views.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 15 Minutes	After Every Sample	=	Not Defined	TRUE	1	The ASM Cluster File System using volume device %ofs_volume_ device% has sections that are corrupt. Run check and repair operation on the file system to fix the issue.

Multiple Thresholds

For this metric column you can set different warning and critical threshold values for each unique combination of "Volume Device" and "Disk Group" objects.

If warning or critical threshold values are currently set for any unique combination of "Volume Device" and "Disk Group" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Volume Device" and "Disk Group" objects, use the Edit Thresholds page.

Data Source

This metric is collected from the column CORRUPT in the V$ASM_FILESYSTEM view for mounted ASM Cluster File Systems. For Dismounted File Systems, a value of Null is returned for this metric.

User Action

Run Check and Repair on the ASM Cluster File System to fix the corrupted sections.

1.3.2 Disk Group Allocated Space (GB)

This metric shows the space allocated from the disk group for this ASM Cluster File System in GB.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is collected from the column SPACE in the V$ASM_FILE view

User Action

No user action is required.

1.3.3 Free (GB)

This metric shows the unused capacity of the ASM Cluster File System in gigabytes. It gives an indication of the free space available in the ASM Cluster File System. For dismounted ASM Cluster File Systems, a value of 0 is returned for this metric.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is collected from the column TOTAL_FREE in the V$ASM_FILESYSTEM view. For dismounted ASM Cluster File Systems, a value of 0 is returned.

User Action

Consider resizing the ASM Cluster File System if there is not enough Free Space available.

1.3.4 Size (GB)

This metric shows the Size in GB of the ASM Cluster File System.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is collected from the column TOTAL_SIZE in the V$ASM_FILESYSTEM view for mounted File Systems and from the column SIZE_MB in the view V$ASM_VOLUME for dismounted File Systems.

User Action

Consider resizing the ASM Cluster File System to add space.

1.3.5 Used (GB)

This metric shows the Space in GB that is used on the mounted ASM Cluster File System. For dismounted ASM Cluster File Systems, a value of 0 is returned for this metric.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is calculated from the columns TOTAL_SIZE and TOTAL_FREE in the V$ASM_FILESYSTEM view. It is calculated as:

```
TOTAL_SIZE - TOTAL_FREE
```

For dismounted ASM Cluster File Systems, a value of 0 is returned for this metric

User Action

Consider Resizing the ASM Cluster File System to add more space.

1.3.6 Used (%)

This metric shows the percentage of Space that is used on the ASM Cluster File System. For dismounted ASM Cluster File Systems, a value of 0 is returned for this metric.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 15 Minutes	After Every Sample	>	85	97	1	The ASM Cluster File System using volume device %ofs_volume_ device% is %ofs_ used_pct%%% full. Resize the file system to add more space.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Volume Device" and "Disk Group" objects.

If warning or critical threshold values are currently set for any unique combination of "Volume Device" and "Disk Group" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Volume Device" and "Disk Group" objects, use the Edit Thresholds page.

Data Source

This metric is calculated from the columns TOTAL_SIZE and TOTAL_FREE in the V$ASM_FILESYSTEM view. It is calculated as:

```
TOTAL_SIZE - TOTAL_FREE/TOTAL_SIZE * 100
```

For dismounted ASM Cluster File Systems, a value of 0 is returned for this metric

User Action

Consider resizing the ASM Cluster File System to add more space to fix the alert generated by this metric.

1.3.7 Volume Name

This metric shows the Volume Name of the Volume Device used to create the ASM Cluster File System.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is collected from the column VOLUME_NAME in the V$ASM_VOLUME view.

User Action

No user action is required.

1.4 ASM Cluster File System State Metrics

The ASM Cluster File System State metrics show the state of the ASM Cluster File System, whether it is MOUNTED or DISMOUNTED on a given host. In a cluster environment, the ASM Cluster File System could be mounted only on specific hosts. If the ASM Cluster File System is MOUNTED on a given host, the metrics also display if the system is AVAILABLE and the time since it is available. This is used to determine the following metrics: Mount Point, Mount State, Availability, and Available Time.

These metrics generate a warning alert if the ASM Cluster File System is dismounted on a given host. These metrics also generate a critical alert if the mounted ASM Cluster File System is not available on a host.

These metrics are collected with the help of a SQL query which queries the V$ASM_FILESYSTEM, V$ASM_VOLUME, V$ASM_OFSVOLUMES views.

1.4.1 ASM Cluster File System Availability

This metric shows if the MOUNTED ASM Cluster File System is AVAILABLE on a given host in a cluster. For DISMOUNTED ASM Cluster File System's this metric returns a value of NULL.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 5 Minutes	After Every Sample	=	Not Defined	Not Available	1	The ASM Cluster File System %ofs_ mount_point% is not available on host %ofs_host%

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Volume Device" and "Host" objects.

If warning or critical threshold values are currently set for any unique combination of "Volume Device" and "Host" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Volume Device" and "Host" objects, use the Edit Thresholds page.

Data Source

This metric is collected from the column STATE in the V$ASM_FILESYSTEM view.

User Action

No user action is required.

1.4.2 ASM Cluster File System Available Time

This metric shows the timestamp since which the MOUNTED ASM Cluster File System is AVAILABLE on a given host in a cluster. For DISMOUNTED ASM Cluster File System's this metric returns a value of NULL.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 5 Minutes

Data Source

This metric is collected from the column AVAILABLE_TIME in the V$ASM_ FILESYSTEM view.

User Action

No user action is required.

1.4.3 ACM Cluster File System Mount Point

This metric shows the mount point of the ASM Cluster File System on a given host in a cluster. The same ASM Cluster File System could be mounted on different mount points, on different hosts in a cluster. For DISMOUNTED ASM Cluster File Systems it will return NULL if the OFS has never been mounted on the host or it will return the last mount point if it was mounted and then dismounted on the host.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 5 Minutes

Data Source

For MOUNTED file systems this metric is collected from the column FS_NAME in the V$ASM_FILESYSTEM view. For DISMOUNTED file systems this metric is collected from the column MOUNTPATH in the V$ASM_VOLUME view.

User Action

No user action is required.

1.4.4 ASM Cluster File System Mount State

This metric shows the state of the ASM Cluster File Systems, whether it is MOUNTED or DISMOUNTED on a given host. In a cluster environment the ASM Cluster File System could be mounted only on specific hosts.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 5 Minutes	After Every Sample	=	Dismounted	Not Defined	1	The volume device %volume_device% is dismounted on host %ofs_host%

Multiple Threshold

For this metric you can set different warning and critical threshold values for each unique combination of "Volume Device" and "Host" objects.

If warning or critical threshold values are currently set for any unique combination of "Volume Device" and "Host" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Volume Device" and "Host" objects, use the Edit Thresholds page.

Data Source

An ASM Cluster File System is "MOUNTED" if the usage of the volume_device is "ACFS" and the volume_device exists in the V$ASM_ACFSVOLUMES view and the mount path exists in the V$ASM_FILESYSTEM view.

An ASM Cluster File System is "DISMOUNTED" if the usage of the volume_device is "ACFS" and the volume_device does not exist in the V$ASM_ACFSVOLUMES view and the mount path does not exist in the V$ASM_FILESYSTEM view.

User Action

Mount the ASM Cluster File System on the given host in the cluster

1.5 ASM Volumes Metrics

The ASM Volumes metrics show information about the Volumes created on a disk group. An ASM Volume file is a file created on the disk group to provide storage for an ASM Cluster File System or a third-party file system. This is used to determine the following metrics for ASM volumes: Volume Name, Status, Usage, Mount Point, Size (GB), Allocated Space (GB), and Redundancy.

These metrics are collected with the help of the V$ASM_VOLUME and GV$ASM_DISKGROUP views.

1.5.1 Disk Group Allocated Space (GB)

This metric gives the space in GB allocated on the disk group for the volume.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is retrieved from the column SPACE from the V$ASM_FILE view.

User Action

No user action is required.

1.5.2 Mount Point

An ASM Cluster File System is built on an ASM Volume which in turn uses ASM disk groups for storage. The ASM Cluster File System can then be mounted on any host in a cluster. This metric returns the current MOUNT POINT of the ASM Cluster File System if it is mounted or the most recent MOUNT POINT if it is currently DISMOUNTED. For ASM Volumes that are not used for ASM Cluster File Systems, this metric returns null.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is retrieved from the column MOUNTPATH from the V$ASM_VOLUME view.

User Action

No user action is required.

1.5.3 Redundancy

This metric returns the redundancy for the ASM Volume file. The ASM Volume file can use whatever redundancy (external, normal=2-way mirror, high=3-way mirror) is available to the ASM disk group where the ASM Volume file is created.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is retrieved from the REDUNDANCY column from the V$ASM_VOLUME view.

User Action

No user action is required.

1.5.4 Size (GB)

This metric returns the size of the ASM Volume in GB. The Volume Size is always created in multiples of the Volume Allocation Unit,

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is retrieved from the column SIZE_MB from the V$ASM_VOLUME view.

User Action

No user action is required.

1.5.5 Status

This metric shows the Status of the ASM Volume, if it is ENABLED or DISABLED.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is retrieved from the column STATE from the V$ASM_VOLUME view.

User Action

No user action is required.

1.5.6 Usage

This metric returns a string indicating what the ASM Volume is used for: ACFS, EXT3, null. A value of null means the usage of the Volume is Unknown.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric returns a string indicating what the ASM Volume is used for: ACFS, EXT3, null. A value of null means the usage of the Volume is Unknown.

User Action

No user action is required.

1.5.7 Volume Name

This metric returns the name of the ASM volume. This is the name entered when the user creates the ASM Volume on the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 15 Minutes

Data Source

This metric is retrieved from the column VOLUME_NAME from the view V$ASM_VOLUME view.

User Action

No user action is required.

1.6 Checker Failure

NOTE TO JACKIE: Sent e-mail to Mary Pawelko on 19-Feb-2010 requesting information. Mary pointed me to Sukumar.Vanka (IDC), the author of the metric. I sent Sukumar e-mail on 19-Feb-2010.

This metric...

1.6.1 Alert Log Name

This metric returns the name of the Alert Log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

This metric is retrieved from the....

User Action

No user action is required.

1.6.2 Checker Failure Detected

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[1]	Health checker runs found %numberOfFailures% new failures in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric column you can set different warning and critical threshold values for each for each "Time/LineNumber" object.

If warning or critical threshold values are currently set for any "Time/LineNumber" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/LineNumber" object, use the Edit Thresholds page.

Data Source

The data comes from

User Action

1.7 Cluster Disk Group Performance Metrics

The Cluster Disk Group Performance metrics show the Cluster Disk Group performance parameters for all the disk groups present in a cluster. These metrics are used to collect information, for example, total I/O and read/write requests, total I/O and read/write time, and total number of bytes read/written for the cluster disk group. These metrics also show the disk group response, throughput, operations per second, and size for read, write, and I/O.

1.7.1 I/O Per Second

This metric shows the sum of disks I/O performance per second in terms of total I/O requests for all the disks within the disk group. The data is aggregated for all instances that are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/Os per second for each disk, the total number of I/O responses is divided by the total I/O time during the collection interval. This data is aggregated by the disk group name to get the average I/O operations per second of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.2 I/O Size (MB)

This metric shows the sum of disk I/O size for all disks within the disk group. The data is aggregated for all instances that are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/O size of each disk, the total number of bytes read and written is divided by the total number of I/Os during the collection interval. This data is aggregated by the disk group name to get the average I/O size of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.3 I/O Throughput

This metric shows the sum of I/O throughput for all disks within the disk group The data is aggregated for all instances that are part of the cluster. This gives an indication of the disk group I/O performance in terms of read and write.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/O throughput of each disk, the total number of bytes read and written is divided by the total I/O time during the collection interval. This data is aggregated by the disk group name to get the average I/O throughput of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.4 Read Response Time (MS)

This metric shows the read response time detail for a disk group in an Automatic Storage Management (ASM) instance. This gives an indication for the disk group response time in terms of read requests for the disks included in the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average read response time for each disk, the total read time is divided by the total number of read responses during the collection interval. This data is aggregated by the disk group name to get the average read response time of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.5 Read Size (MB)

This metric shows the sum of all disk read size for all disks within the disk group which are part of the cluster. The data is aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average read size of each disk, the total number of bytes read is divided by the total number of reads during the collection interval. This data is aggregated by the disk group name to get the average read size of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.6 Read Throughput

This metric shows the read throughput detail of a disk group mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes read from the disk group with proportion to the total read time for this disk group in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average read throughput of each disk, the total number of bytes read is divided by the total read time during the collection interval. This data is aggregated by the disk group name to get the average read throughput of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.7 Reads Per Second

This metric shows the detail of total read requests per second for the disk group. This metric shows the read performance of the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average reads per second for each disk, the total number of read responses is divided by the total read time during the collection interval. This data is aggregated by the disk group name to get the average read operations per second of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.8 Response Time (MS)

This metric shows the I/O response time detail of mounted disk groups. For this disk group, this metric indicates the response time in terms of total I/O requests for all the disks included in the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/O response time for each disk, the total I/O time is divided by the total number of I/O responses during the collection interval. This data is aggregated by the disk group name to get the average I/O response time of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.9 Write Response Time (MS)

This metric shows the write response time detail for a disk group in an Automatic Storage Management (ASM) instance. This gives an indication for the disk group response time in terms of total write requests for the disks included in a disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average write response time for each disk, the total write time is divided by the total number of write responses during the collection interval. This data is aggregated by the disk group name to get the average write response time of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.7.10 Write Size (MB)

This metric shows the sum of all disk write size for all disks within the disk group which are part of the cluster. The data is aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average write size of each disk, the total number of bytes written is divided by the total number of writes during the collection interval. This data is aggregated by the disk group name to get the average write size of a disk group. The data is then aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.7.11 Write Throughput

This metric shows the write throughput detail of a disk group mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes written from the disk group with proportion to the total write time for this disk group in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average write throughput of each disk, the total number of bytes written is divided by the total write time during the collection interval. This data is aggregated by the disk group name to get the average write throughput of a disk group. The data is then aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.7.12 Writes Per Second

This metric shows the detail of total write requests per second for a disk group in an Automatic Storage Management (ASM) instance. This metric shows the write performance of the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average writes per second for each disk, the total number of write responses is divided by the total write time during the collection interval. This data is aggregated by the disk group name to get the average write operations per second of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8 Cluster Disk Performance Metrics

The Cluster Disk Performance metrics show the cluster disk performance parameters for all the disks. These metrics are used to collect information, for example, total I/O and read/write requests, failed read/write and I/O for the disks, total I/O and read/write time, and total number of bytes read/written to the disks. These metrics also show the response of the disks for read, write, and I/O throughput.

1.8.1 I/O Per Second

This metric shows the sum of disks I/O performance per second in terms of total I/O requests for all the disks within the disk group. The data is aggregated for all instances that are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/Os per second for each disk, the total number of I/O responses is divided by the total I/O time during the collection interval. This data is aggregated by the disk group name to get the average I/O operations per second of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.2 I/O Size (MB)

This metric shows the sum of disk I/O size for all disks within the disk group. The data is aggregated for all instances that are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/O size of each disk, the total number of bytes read and written is divided by the total number of I/Os during the collection interval. This data is aggregated by the disk group name to get the average I/O size of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.3 I/O Throughput

This metric shows the sum of I/O throughput for all disks within the disk group The data is aggregated for all instances that are part of the cluster. This gives an indication of the disk group I/O performance in terms of read and write.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/O throughput of each disk, the total number of bytes read and written is divided by the total I/O time during the collection interval. This data is aggregated by the disk group name to get the average I/O throughput of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.4 Read Response Time (MS)

This metric shows the read response time detail for a disk group in an Automatic Storage Management (ASM) instance. This gives an indication for the disk group response time in terms of read requests for the disks included in the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average read response time for each disk, the total read time is divided by the total number of read responses during the collection interval. This data is aggregated by the disk group name to get the average read response time of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.5 Read Size (MB)

This metric shows the sum of all disk read size for all disks within the disk group which are part of the cluster. The data is aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average read size of each disk, the total number of bytes read is divided by the total number of reads during the collection interval. This data is aggregated by the disk group name to get the average read size of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.6 Read Throughput

This metric shows the read throughput detail of a disk group mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes read from the disk group with proportion to the total read time for this disk group in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average read throughput of each disk, the total number of bytes read is divided by the total read time during the collection interval. This data is aggregated by the disk group name to get the average read throughput of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.7 Reads Per Second

This metric shows the detail of total read requests per second for the disk group. This metric shows the read performance of the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average reads per second for each disk, the total number of read responses is divided by the total read time during the collection interval. This data is aggregated by the disk group name to get the average read operations per second of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.8 Response Time (MS)

This metric shows the I/O response time detail of mounted disk groups. For this disk group, this metric indicates the response time in terms of total I/O requests for all the disks included in the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/O response time for each disk, the total I/O time is divided by the total number of I/O responses during the collection interval. This data is aggregated by the disk group name to get the average I/O response time of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.9 Write Response Time (MS)

This metric shows the write response time detail for a disk group in an Automatic Storage Management (ASM) instance. This gives an indication for the disk group response time in terms of total write requests for the disks included in a disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average write response time for each disk, the total write time is divided by the total number of write responses during the collection interval. This data is aggregated by the disk group name to get the average write response time of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.8.10 Write Size (MB)

This metric shows the sum of all disk write size for all disks within the disk group which are part of the cluster. The data is aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average write size of each disk, the total number of bytes written is divided by the total number of writes during the collection interval. This data is aggregated by the disk group name to get the average write size of a disk group. The data is then aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.8.11 Write Throughput

This metric shows the write throughput detail of a disk group mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes written from the disk group with proportion to the total write time for this disk group in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average write throughput of each disk, the total number of bytes written is divided by the total write time during the collection interval. This data is aggregated by the disk group name to get the average write throughput of a disk group. The data is then aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.8.12 Writes Per Second

This metric shows the detail of total write requests per second for a disk group in an Automatic Storage Management (ASM) instance. This metric shows the write performance of the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average writes per second for each disk, the total number of write responses is divided by the total write time during the collection interval. This data is aggregated by the disk group name to get the average write operations per second of a disk group. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.9 Cluster Volume Performance Metrics

The Cluster Volume Performance metrics show the cluster volume performance parameters for all the volumes. These metrics are used to collect information, for example, total I/O and read/write requests, failed read/write and I/O for the disks, total I/O and read/write time, and total number of bytes read/written to the volumes. These metrics also show the response of the volumes for read, write, and I/O throughput.

1.9.1 I/O Per Second

This metric shows the Volumes I/O performance per second in terms of total I/O requests for all the Volumes, which are part of the cluster.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average I/Os per second for each volume, the total number of I/O responses is divided by the total I/O time during the collection interval. The data is aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.9.2 I/O Size (MB)

This metric shows the volume I/O size of volumes present in a cluster. The data is aggregated for all instances that are part of the cluster.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average I/O size of each volume, the total number of bytes read and written is divided by the total number of I/Os during the collection interval. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.9.3 I/O Throughput

This metric shows the I/O throughput detail of a volume in a cluster. The data is aggregated for all instances that are part of the cluster. This gives an indication of the volume I/O performance in terms of reads and writes.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average throughput of each volume, the total number of bytes read and written is divided by the total I/O time during the collection interval. The data is aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.9.4 Read Response Time (MS)

This metric shows the read response time detail of volumes present in a cluster. This gives an indication of a volume response time in terms of total read requests for volumes in a cluster.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average I/O response time for each volume, the total I/O time is divided by the total number of I/O responses during the collection interval. The data is then aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.9.5 Read Size (MB)

This metric shows the read size in megabytes of volumes present in a cluster. The data is aggregated for all volumes that are part of the cluster.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average read size of each volume, the total number of bytes read is divided by the total number of reads during the collection interval. The data is aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.9.6 Read Throughput

This metric shows the read throughput detail of volumes present in a cluster. This gives an indication of the total number of bytes read from the volume with proportion to the total read time for read requests for this volume.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average read throughput of each volume, the total number of bytes read is divided by the total read time during the collection interval. The data is then aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.9.7 Read Write Errors

This metric shows the detail of the total number of failed reads and writes of volumes present in a cluster. This gives an indication of the total number of failed attempts of reads and writes for the volume.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average read response time for each volume, the total read time is divided by the total number of read responses during the collection interval. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.9.8 Reads Per Second

This metric shows the reads per second detail of volumes present in a cluster.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average reads per second for each volume, the total number of read responses is divided by the total read time during the collection interval. The data is then aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.9.9 Response Time (MS)

This metric displays the I/O response time details of volumes present in a cluster. This provides an indication of the volume response time in terms of total I/O requests for this volume.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric, which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average I/O response time for each volume, the total I/O time is divided by the total number of I/O responses during the collection interval. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.9.10 Write Response Time (MS)

This metric shows the write response time detail of volumes present in a cluster. This gives an indication for the volume response time in terms of total write requests for the volume in a cluster.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average write response time for each volume, the total write time is divided by the total number of write responses during the collection interval. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.9.11 Write Size (MB)

This metric shows the sum of all volume writes for all volumes which are part of the cluster. The data is aggregated for all instances.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average write size of each volume, the total number of bytes written is divided by the total number of writes during the collection interval. The data is then aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.9.12 Write Throughput

This metric shows the write throughput detail of volumes present in a cluster. This gives an indication for the total number of bytes written to a volume with proportion to the total write time for write requests for the volume in a cluster.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average write throughput of each volume, the total number of bytes written is divided by the total write time during the collection interval. The data is then aggregated for all instances that are part of the cluster.

User Action

No user action is required.

1.9.13 Writes Per Second

This metric shows the detail of total write requests per second for volumes in the cluster.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every Hour

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average writes per second for each volume, the total number of write responses is divided by the total write time during the collection interval. The data is aggregated for all instances that are part of the cluster

User Action

No user action is required.

1.10 Database Disk Group Usage Metric

The Database Disk Group Usage metric show the detail of the disk group space used by a database. With the help of this metric, you can know the space used in a disk group by different database instances.

1.10.1 Total Bytes

This metric shows the total bytes of the disk group space used by a database. With the help of this metric one can know the space used in a disk group by different database instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

We get the space used by a file using the V$OSM_FILE view and then it is joined with the V$ASM_ALIAS and V$ASM_DISKGROUP views for 10*g* Release 1 and the VASM_ALIAS, VASM_DISKGROUP_STAT views for 10*g* Release 2 to get the disk group space used by a database instance

User Action

No user action is required.

1.11 Disk Group Imbalance Status Metrics

The Disk Group Imbalance Status metrics check if any disk groups are out of balance. Under normal operations, ASM automatically rebalances disk groups. These metrics detect conditions where manual rebalances may be required or the power level of a rebalance in progress may need to be raised to give it the necessary resources to complete faster.

1.11.1 Actual Imbalance (%)

Actual Imbalance (%) measures the difference in space allocated to the fullest and emptiest disks in the disk group. Comparison is in percent full since ASM tries to keep all disks equally full as a percent of their size. The imbalance is relative to the space allocated not the space available. An imbalance of a couple percent is reasonable.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11 2.0.x	Every 15 Minutes

Data Source

Actual Imbalance (%) is calculated as:

```
100 * (max((total_mb - free_mb) / total_mb) - min((total_mb - free_mb)
/ total_mb)) / max((total_mb - free_mb) / total_mb)
where total_mb and free_mb are columns in V$ASM_DISK_STAT
```

User Action

An imbalance of more than a couple percent may signal the need to initiate a manual rebalance of the disk group.

1.11.2 Actual Minimum Percent Free

Actual Minimum Percent Free lists the amount of free disk space on the fullest disk as a percentage of the disk size. If the imbalance is zero, then this represents the total free space. Since all allocations are done evenly across all disks, the minimum free space limits how much space can be used.

If one disk has only one percent free, then only one percent of the space in the disk group is really available for allocation, even if the rest of the disks are only half full

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11 2.0.x	Every 15 Minutes

Data Source

Actual Minimum Percent Free is calculated as 100 * (min(free_mb / total_mb)), where free_mb and total_mb are columns in V$ASM_DISK_STAT.

User Action

If the actual minimum percent free is a low number, a configuration change may be required in order to provide an even distribution of file extents and space usage across all disks in a disk group.

1.11.3 Disk Count

Disk count is the number of disks in the disk group which gives a sense of how widely files can be spread.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11 2.0.x	Every 15 Minutes

Data Source

Disk Count is calculated using count(*) on all disks (V$ASM_DISK_STAT) in a disk group (V$ASM_DISKGROUP_STAT).

User Action

No user action is required.

1.11.4 Disk Group Imbalance (%) without Rebalance

Disk Group Imbalance (%) without Rebalance is used to determine if a disk group requires rebalance. Temporary imbalances (caused by a rebalance in progress) are ignored.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	>	10	Not Defined	1	Disk Group %diskGroup% requires rebalance because the space usage imbalance between disks is high.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group" object.

If warning or critical threshold values are currently set for any "Disk Group" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group" object, use the Edit Thresholds page.

Data Source

Disk Group Imbalance (%) without Rebalance is the same value as Actual Imbalance (%) if a rebalance operation is not in progress, 0 otherwise.

User Action

A warning alert will be generated if Disk Group Imbalance (%) without Rebalance is greater than or equal to 10%. In this case, a rebalance is necessary because the space usage imbalance between disks is high. The user should manually initiate a rebalance operation.

1.11.5 Disk Maximum Used (%) with Rebalance

Disk Maximum Used (%) with Rebalance is used to determine if a rebalance in progress needs a power boost to complete in a timely manner and prevent other errors from occurring due to space constraints.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	>	Not Defined	95	1	Increase the rebalance power for Disk Group %diskGroup% because at least one disk is critically low on space.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group" object.

If warning or critical threshold values are currently set for any "Disk Group" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group" object, use the Edit Thresholds page.

Data Source

If a rebalance is in progress and the power value is greater than 0, then Disk Maximum Used (%) with Rebalance is calculated as (100 - Actual Minimum Percent Free), 0 otherwise.

User Action

A critical alert will be generated if Disk Maximum Used (%) with Rebalance is greater than or equal to 95%. In this case the rebalance power for the disk group must be increased because at least one disk is critically low on space. Increase the rebalance power (maximum power level is 11).

1.11.6 Disk Minimum Free (%) without Rebalance

Disk Minimum Free (%) without Rebalance is used to determine if a disk group requires rebalance. Temporary imbalances (caused by a rebalance in progress) are ignored.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	<	20	10	1	Disk Group %diskGroup% requires rebalance because at least one disk is low on space.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group" object.

If warning or critical threshold values are currently set for any "Disk Group" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group" object, use the Edit Thresholds page.

Data Source

Disk Minimum Free (%) without Rebalance is the same value as Actual Minimum Percent Free if a rebalance operation is not in progress, 100 otherwise.

User Action

A warning alert will be generated if Disk Minimum Free (%) without Rebalance is less than or equal to 20%. In this case a rebalance is necessary because at least one disk is low on space. The user should manually initiate a rebalance operation.

1.11.7 Disk Size Variance (%)

Disk Size Variance (%) lists the percentage difference in size between the largest and smallest disks in the disk group. This will be zero if best practices have been followed and all disks are the same size.

Small differences in size are acceptable. Large differences can result in some disks getting much more I/O than others. With normal or high redundancy disk groups, a large size variance can make it impossible to reduce the percent imbalance to a small value.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11 2.0.x	Every 15 Minutes

Data Source

```
Disk Size Variance (%) is calculated as 100 *
(max(total_mb) - min(total_mb)) / max(total_mb),
where total_mb is a column in V$ASM_DISK_STAT
```

User Action

A large size variance may require a configuration change to provide an even distribution of file extents and space usage across all disks in a disk group.

1.11.8 Rebalance In Progress

Rebalance In Progress returns "Yes" if a rebalance operation is in progress, "No" otherwise.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11 2.0.x	Every 15 Minutes

Data Source

Rebalance In Progress is retrieved from the operation column of V$ASM_ OPERATION.

User Action

No user action is required.

1.12 Disk Group Usage Metrics

The Disk Group Usage metrics show the space used by all the disk groups having the state as 'MOUNTED'. These metrics are used to collect information about the disk usage and is used to show the trend of disk group space usage in the application. This information is used to determine the following metrics: Free MB, Total MB, Total Safely Usable MB, Type, Safely Usable File MB, Used %, and Used % of Safely Usable of a disk group for 10*g* Release 2 and Free MB, Total MB, Type, and Used % for 10*g* Release 1.

These metrics generate a warning alert if the disk group is 75% used and a critical warning if 90% used. The thresholds for the Disk Group Usage alert should *not* be fixed at 75% and 90%, since the value depends on the redundancy. In version 10*g* Release 2, these metrics use the USABLE_FILE_MB column of the V$ASM_ DISKGROUP_STAT view to indicate usable mirrored free space. This column displays the amount of free space that can be safely utilized taking mirroring into account, and yet is able to restore redundancy after disk failure.

Enterprise Manager issues alerts for the following:

- Critical alert when USABLE_FILE_MB <= 0
- Warning alert when USABLE_FILE_MB < 0.1 * REQUIRED_MIRROR_FREE_MB

This metric is collected at a time interval of 15 minutes. You can change the threshold limit as required.

This metric is collected with the help of a SQL query which queries the V$ASM_ DISKGROUP view for 10*g* Release 1 and the V$ASM_DISKGROUP_STAT view for 10*g* Release 2.

1.12.1 Disk Group Free (MB)

This metric shows the unused capacity of the disk group in megabytes. It gives an indication of the free space available in a disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Total free size for Disk Group %dg_ name% has fallen to %value% (MB).

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group Name" object.

If warning or critical threshold values are currently set for any "Disk Group Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group Name" object, use the Edit Thresholds page.

Data Source

This metric is collected from the column FREE_MB in the view V$ASM_DISKGROUP for 10g Release 1 and the V$ASM_DISKGROUP_STAT view for 10g Release 2.

User Action

Consider adding more disks to the disk group or deleting existing files in the disk group.

1.12.2 Disk Group Usable (Free MB)

The usable free space of a disk group depends on the redundancy, so in 10g Release 2 it uses the USABLE_FILE_MB column of the V$ASM_DISKGROUP_STAT view to indicate usable mirrored free space. This column indicates the amount of free space that can be "safely" utilized taking mirroring into account, and yet is able to restore redundancy after disk failure. This column is used to determine the usable free megabytes of a disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Usable free size for Disk Group %dg_ name% has fallen to %value% (MB).

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group Name" object.

If warning or critical threshold values are currently set for any "Disk Group Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group Name" object, use the Edit Thresholds page.

Data Source

This metric is collected from the column USABLE_FILE_MB in the V$ASM_ DISKGROUP_STAT view for 10g Release 2.

User Action

Consider adding more disks to the disk group or removing existing files from the disk group.

1.12.3 Disk Group Usable (MB)

This metric shows the capacity of the disk group based on the type of the disk group. This column indicates the amount of free space that can be "safely" utilized taking mirroring into account, and yet is able to restore redundancy after disk failure.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

This metric is collected using the V$ASM_DISKGROUP_STAT view.

```
Total Safely Usable MB = (total_mb - required_mirror_free_mb)/redundancy_factor
```

Where *total_mb* and *required_mirror_free_mb* come from the view column, and *redundancy factor* is 1 for External Redundancy Disk Group, 2 for Normal Redundancy Disk Group, and 3 for High Redundancy Disk Group.

User Action

Consider adding more disks to the disk group or removing existing files from the disk group

1.12.4 Disk Group Used %

This metric shows the percentage of space used by a disk group. It generates a warning alert if the disk group is 75% used and a critical warning if 90 % used. The threshold limit can be changed to generate alerts at different values.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	>	75	90	1	Disk Group %dg_name% is %value%% used.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group Name" object.

If warning or critical threshold values are currently set for any "Disk Group Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group Name" object, use the Edit Thresholds page.

Data Source

This metric is collected from the V$ASM_DISKGROUP view for 10g Release 1 and the V$ASM_DISKGROUP_STAT view for 10g Release 2.

```
Used % = (total_mb-free_mb)/total_mb)*100
```

User Action

New disks can be added in a disk group to avoid the alerts. Go to the Disk Group general page and click Add to add a new disk to a disk group. Also, you can remove existing files from the disk group.

1.12.5 Redundancy

This metric shows the Redundancy Type of the disk group. It can be one of the three values: External, Normal, and High. This property determines the restore redundancy after disk failure.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

This metric is collected from the column TYPE in the V$ASM_DISKGROUP view for 10g Release 1 and the V$ASM_DISKGROUP_STAT view for 10g Release 2.

User Action

No user action is required.

1.12.6 Size (MB)

This metric shows the total capacity of the disk group in megabytes. It gives an indication of the size or the space used by the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

This metric is collected from the column TOTAL_MB in the V$ASM_DISKGROUP view for 10*g* Release 1 and the V$ASM_DISKGROUP_STAT view for 10*g* Release 2.

User Action

Consider adding more disks to the disk group.

1.12.7 Used % of Safely Usable

This metric shows the percentage of safely usable space used by a disk group. Usable free space of a disk group depends on the redundancy. In 10*g* Release 2, it uses the USABLE_FILE_MB column of the V$ASM_DISKGROUP_STAT view to indicate usable mirrored free space. This column displays the amount of free space that can be safely utilized taking mirroring into account and restores redundancy after disk failure. This column is used to determine the "Used % of Safely Usable" for a disk group.

This metric generates a warning alert if the disk group is using 90% of the safely usable space and critical warning for 100%. The threshold limit can be changed to generate an alert at different values.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	>	75	90	1	Disk group %dg_name% has used %value%% of safely usable free space (space that can be allocated while still having enough space to recover from failure group failures).

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group Name" object.

If warning or critical threshold values are currently set for any "Disk Group Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group Name" object, use the Edit Thresholds page.

Data Source

This metric is collected from the V$ASM_DISKGROUP_STAT view for 10g Release 2.

```
Used % of Safely Usable = 100 - (usable_file_mb/usable_total_mb)*100

Where usable_total_mb = total_mb - required_mirror_free_mb)/redundancy_factor
```

total_mb and *required_mirror_free_mb* are derived from the view column and *redundancy factor* is 1 for External Redundancy Disk Group, 2 for Normal Redundancy Disk Group, and 3 for High Redundancy Disk Group.

User Action

New disks can be added in a disk group to avoid the alerts. Go to the Disk Group general page and click Add to add a new disk to a disk group. Also, you can remove existing files from the disk group.

1.13 Disk Path Metrics

The Disk Path metrics show the disk name and disk path of all the disks. This information is collected at a time interval of 12 Hours.

These metrics are collected with the help of the V$ASM_DISK view for 10*g* Release 1 and the V$ASM_DISK_STAT view for 10*g* Release 2.

1.13.1 Disk Name

This metric is the name of the disk.

This metric is available in Database Control and Grid Control; in target versions 10.2.0.x, 11.1.0.x, and 11 2.0.x.

Data Source

Name column value in the V$ASM_DISK_STAT and V$ASM_DISK views

User Action

No user action is required.

1.13.2 Disk Path

This metric is the physical path of the disk

This metric is available in Database Control and Grid Control; in target versions 10.2.0.x, 11.1.0.x, and 11 2.0.x.

Data Source

Path column value. For databases prior to 10*g* Release 2, this metric uses the GV$ASM_DISK view. For databases 10*g* Release 2 and higher, this metric uses the GV$ASM_DISK_STAT view.

User Action

No user action is required.

1.13.3 Group Name

This metric provides the name of the group.

This metric is available in Database Control and Grid Contro; in target versions 10.2.0.x, 11.1.0.x, and 11 2.0.x.

Data Source

Path column value. For databases prior to 10*g* Release 2, this metric uses the GV$ASM_DISK view. For databases 10*g* Release 2 and higher, this metric uses the GV$ASM_DISK_STAT view.

User Action

No user action is required.

1.14 Disk Status Metric

The Disk Status metric provides disk mode status (offline and online). A critical warning alert is generated if any of the disks are offline.

This metric is collected at a time interval of 15 minutes. You can change the time limit and threshold limit as required.

1.14.1 Disk Mode Status

This metric displays disk mode status (offline and online). A critical warning alert is generated if any of the disks go offline.

You can change the threshold limit.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 15 Minutes	After Every Sample	=	Not Defined	OFFLINE	1	Disk %dg_ name%.%disk_ name% is offline.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Disk Group Name" and "Disk Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Disk Group Name" and "Disk Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Disk Group Name" and "Disk Name" objects, use the Edit Thresholds page.

Data Source

This metric is collected with the help view column mode status from GV$ASM_DISK for 10*g*Release 1 and GV$ASM_DISK_STAT for 10*g* Release 2.

User Action

Try to bring the disk online. Currently Enterprise Manager does not support this feature

1.15 Failure Group Imbalance Status Metrics

The Failure Group Imbalance Status metrics check how even failure group disks are laid out for ASM disk groups. ASM strives for an even distribution of file extents and space usage across all disks in a disk group. It accomplishes this through rebalancing. If the disks are different sizes or the failure groups are different sizes then effective rebalancing cannot be achieved. In this situation, configuration changes are required.

These metrics only apply to disk groups with normal or high redundancy. These metrics will not return data for disk groups with external redundancy, since failure groups are not used in this configuration.

1.15.1 Disk Count Imbalance Variance

Failure groups are used to store mirror copies of data, two copies for normal redundancy, three copies for high redundancy. Disk Count Imbalance Variance gives the difference in the failure group disk count for the disk in the disk group with the highest failure group disk count and the disk with the lowest.

It may not be possible for every disk to have the same failure group disk count even when all the failure groups are the same size. However an imbalance of more than one indicates that the failure groups are different sizes.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	>=	2	Not Defined	1	Disk Group %diskGroup% has failure groups with different numbers of disks which may lead to suboptimal space usage. Changing the configuration may alleviate this problem.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group" object.

If warning or critical threshold values are currently set for any "Disk Group" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group" object, use the Edit Thresholds page.

Data Source

Disk Count Imbalance Variance is calculated using the V$ASM_DISKGROUP_STAT and V$ASM_DISK_STAT views, along with some internal ASM fixed tables.

User Action

A warning alert will be generated when the Disk Count Imbalance Variance is greater than 1 (by default). Disk groups that have failure groups with different numbers of disks may lead to suboptimal space usage. To alleviate this problem, try changing the configuration.

1.15.2 Disk Size Imbalance (%)

Disk Size Imbalance (%) checks if some disks have more space in their failure group disks than others. The space is calculated as a ratio between the size of a disk and the sum of the sizes of its active failure group disks. This ratio is compared for all the disks. The difference in the highest and lowest failure group disk space is reported as a percentage. An imbalance of 10% is acceptable.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	>	10	Not Defined	1	Disk Group %diskGroup% has failure groups with disks of different sizes which may lead to suboptimal space usage. Changing the configuration may alleviate this problem.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Disk Group" object.

If warning or critical threshold values are currently set for any "Disk Group" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Disk Group" object, use the Edit Thresholds page.

Data Source

Disk Size Imbalance is calculated using the V$ASM_DISKGROUP_STAT and V$ASM_DISK_STAT views, along with some internal ASM fixed tables.

User Action

A warning alert will be generated when the Disk Size Imbalance (%) is greater than 10% (by default). Disk groups that have failure groups with disks of different sizes may lead to suboptimal space usage. To alleviate this problem, try changing the configuration.

1.15.3 Failure Group Count

Failure Group Count reports the number of failure groups per disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

Failure Group Count is retrieved from a calculation involving the V$ASM_DISKGROUP_STAT and V$ASM_DISK_STAT views, and some internal ASM fixed tables.

User Action

No user action is required.

1.16 Failure Group Status Metrics

The Failure Group Status metrics check to see if all the member disks of any failure group are offline. This is an undesirable condition which risks data loss, since mirror copies of data cannot be stored.

These metrics only apply to disk groups with normal or high redundancy.

1.16.1 Available Disks

Available Disks reports the number of disks in the failure group that are online.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric’s value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

Available Disks is calculated by subtracting the number of offline disks in the failure group from the number of total disks.

User Action

No user action is required.

1.16.2 Disk Count for Alerts

Disk Count for Alerts will have the same value as Available Disks if there is more than one disk in the failure group. If there is exactly one disk in the failure group, Disk Count for Alerts will be 1, regardless if that one disk is offline. The reason for this is to avoid duplicate alerts being generated for the same root cause. The disk_status metric will generate a critical alert when a disk goes offline.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	=	Not Defined	0	1	Failure Group %diskGroup%.%failureGroup% is offline.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Disk Group" and "Failure Group" objects.

If warning or critical threshold values are currently set for any unique combination of "Disk Group" and "Failure Group" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Disk Group" and "Failure Group" objects, use the Edit Thresholds page.

Data Source

Disk Count for Alerts is set to 1 if there is only one disk in the disk group, otherwise it is set to the value of Available Disks.

User Action

A critical alert will be generated if all disks comprising a failure group are taken offline. In this situation, data is not being mirrored, despite the disk group having been configured with normal or high redundancy. Action must be taken to bring some of the disks in the failure group back online, or to add more disks to the disk group and assign them to that failure group.

1.16.3 Total Disks

Total Disks reports the number of disks in the failure group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

Total Disks is retrieved from the V$ASM_DISKGROUP_STAT and V$ASM_DISK_STAT views.

User Action

No user action is required.

1.17 Incident Metrics

The Incident metrics represent incidents, for example, generic internal error, access violation, and so on as recorded in the ASM alert log file. The alert log file has a chronological log of messages and errors.

Each metric signifies that the ASM being monitored has detected a critical error condition about the ASM and has generated an incident to the alert log file since the last sample time. The Support Workbench in Enterprise Manager contains more information about each generated incident.

1.17.1 Access Violation

This metric signifies that the ASM has generated an incident due to some memory access violation. This type of incident is typically related to Oracle Exception messages such as ORA-3113 and ORA-7445. The ASM can also generate this type of incident when it detects a SIGSEGV or SIGBUS signals.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	An access violation detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.2 Alert Log Error Trace File

This metric is the name of the trace file (if any) associated with the logged incident.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

1.17.3 Alert Log Name

This metric is the name of the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The data comes from the alert log files. It is collected using the Perl script: $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

1.17.4 ASM Block Corruption

ASM Block corruption can happen due to many reasons over lifetime (for example head misalignment, dust spec, and so on). If the disk groups are mirrored, ASM automatically repairs the corrupted blocks from the mirror.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	An ASM data block was corrupted at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

Incident metric

User Action

User can execute check and remap commands which have been implemented in Enterprise Manager.

1. Check

   This checks the consistency of disk group metadata and logs the result in alert log and may repair depending upon repair/norepair option provided. In case of corruptions, the result would look like: "cache read a corrupted block group=NORM3 fn=1 blk=0 from disk 0" and so on.

2. Remap

   This repairs a range of physical blocks that maps to a valid ASM file.

In addition, you can use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.17.5 Cluster Error

This metric signifies that the ASM has generated an incident due to a member evicted from the group by a member of the cluster database. This type of incident is typically related to Oracle Exception message ORA-29740.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A cluster error detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.6 Deadlock

This metric signifies that the ASM has generated an incident due to a deadlock detected while trying to lock a library object. This type of incident is typically related to Oracle Exception message ORA-4020.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A deadlock error detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.7 File Access Error

This metric signifies that the ASM has generated an incident due to failure to read a file at the time. This type of incident is typically related to Oracle Exception message ORA-376.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A file access error detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.8 Generic Incident

This metric signifies that the ASM has generated an incident due to some error.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Incident (%errCodes%) detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.9 Generic Internal Error

This metric signifies that the ASM has generated an incident due to an internal ASM error. This type of incident is typically related to Oracle Exception message ORA-600 or ORA-0060*.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Internal error (%errCodes%) detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.10 Impact

This metric is the impact of an incident. For a Generic Internal Error incident, the impact describes how the incident may affect the ASM.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

1.17.11 Incident ID

This metric is a number identifying an incident. The Support Workbench in Enterprise Manager uses this ID to specify an incident.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

1.17.12 Internal SQL Error

This metric signifies that the ASM has generated an incident due to an internal SQL error. This type of incident is typically related to Oracle Exception message ORA-604.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	An internal SQL error detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.
[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.13 Out of Memory

This metric signifies that the ASM has generated an incident due to failure to allocate memory. This type of incident is typically related to Oracle Exception message ORA-4030 or ORA-4031.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Out of memory detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.
[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.14 Redo Log Corruption

This metric signifies that the ASM has generated an incident due to an error with the redo log. This type of incident is typically related to Oracle Exception message ORA-353, ORA-355, or ORA-356.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A data block was corrupted at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.17.15 Session Terminated

This metric contains the information about different ORA- errors, which indicate the presence of Session Terminated problems in the alert log files. The ORA- 00603 error in

the alert log indicates Session Terminated problems. This also generates a warning alert when these problems are found in alert logs.

You can edit the metric threshold and change the value of the error you want to collect under a different head. Also, the warning and critical alert values can be modified or set.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A session termination detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent. The alert log file is scanned for the ORA-00603 error.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.

1.18 Incident Status Metrics

The Incident Status metrics represent whether the last scan of the alert log identified each type of incident and, if so, how many.

1.18.1 Access Violation Status

This metric reflects the number of Access Violation incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Access violation errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.2 ASM Block Corruption Error Status

This metric reflects the number of ASM Block Corruption incidents witnessed the last time Enterprise Manager scanned the alert log

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	ASM data block corruption errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.3 Cluster Error Status

This metric reflects the number of Cluster Error incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Cluster errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.4 Deadlock Error Status

This metric reflects the number of Deadlock incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Deadlock errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.5 File Access Error Status

This metric reflects the number of File Access Error incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	File access errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.6 Generic Incident Status

This metric reflects the number of Generic Incident incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	%value% distinct types of incidents have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.7 Generic Internal Error Status

This metric reflects the number of Generic Internal Error incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Generic internal errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.8 Internal SQL Error Status

This metric reflects the number of Internal SQL Error incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Internal SQL errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.9 Out of Memory Status

This metric reflects the number of Out of Memory incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Out of memory errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.10 Redo Log Corruption Error Status

This metric reflects the number of Redo Log Corruption incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Redo log corruption errors have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.18.11 Session Terminated Status

This metric reflects the number of Session Terminated incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Session terminations have been found in the alert log.

Data Source

Incident metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incidents.

1.19 Instance Disk Group Performance Metrics

The Instance Disk Group Performance metrics indicate the performance of the disk groups present in an Automatic Storage Management (ASM) instance. These metrics show the disk group performance parameters for all the disk groups mounted on an ASM Instance.

These metrics are used to collect information, for example, total I/O and read/write requests, total I/O and read/write time, and the total number of bytes read/written to the disk group. These metrics also show the response of the disk group for read, write, and I/O throughput.

1.19.1 I/O per Second

This metric shows the sum of disks I/O performance per second in terms of total I/O requests for all the disks within the disk group. The data is displayed for all instances that are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average I/Os per second for each disk, the total number of I/O responses is divided by the total I/O time during the collection interval. This data is aggregated by the disk group name to get the average I/O operations per second of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.2 I/O Size (MB)

This metric shows the sum of all disk I/O for all disks within the disk group. The data is not aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average I/O size of each disk, the total number of bytes read and written is divided by the total number of I/Os during the collection interval. This data is aggregated by the disk group name to get the average I/O size of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.3 I/O Throughput

This metric shows the sum of I/O throughput for all disks within the disk group. The data is aggregated for all instances that are part of the cluster. This gives an indication of the disk group I/O performance in terms of read and write.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average throughput of each disk, the total number of bytes read and written is divided by the total I/O time during the collection interval. This data is aggregated by the disk group name to get the average I/O throughput of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.4 Read Response Time (MS)

This metric shows the read response time detail for a disk group in an Automatic Storage Management (ASM) instance. This gives an indication for the disk group response time in terms of read requests for the disks included in the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average read response time for each disk, the total read time is divided by the total number of read responses during the collection interval. This data is aggregated by the disk group name to get the average read response time of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.5 Read Size (MB)

This metric shows the sum of all disk reads for all disks within the disk group which are part of the cluster. The data is not aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average read size of each disk, the total number of bytes read are divided by the total number of reads during the collection interval. This data is aggregated by the disk group name to get the average read size of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.6 Read Throughput

This metric shows the read throughput detail of a disk group mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total

number of bytes read from the disk group with proportion to the total read time for this disk group in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average read throughput of each disk, the total number of bytes read is divided by the total read time during the collection interval. This data is aggregated by the disk group name to get the average read throughput of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.7 Reads per Second

This metric shows the detail of total read requests per second for a disk group in an Automatic Storage Management (ASM) instance. This metric shows the read performance of all the disks included in the disk group of an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average reads per second for each disk, the total number of read responses is divided by the total read time during the collection interval. This data is aggregated by the disk group name to get the average reads per second of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.8 Response Time (MS)

This metric shows the I/O response time detail of mounted disk groups. For this disk group, this metric indicates the response time in terms of total I/O requests for all the disks included in the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average I/O response time for each disk, the total I/O time is divided by the total number of I/O responses during the collection interval. This data is aggregated by the disk group name to get the average I/O response time of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.9 Write Response Time (MS)

This metric shows the write response time detail for a disk group in an Automatic Storage Management (ASM) instance. This gives an indication for the disk group response time in terms of total write requests for the disks included in a disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average write response time for each disk, the total write time is divided by the total number of write responses during the collection interval. This data is aggregated by the disk group name to get the average write response time of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.10 Write Size (MB)

This metric shows the sum of all disk writes for all disks within the disk group which are part of the cluster. The data is not aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average write size of each disk, the total number of bytes written is divided by the total number of writes during the collection interval. This data is aggregated by the disk group name to get the average write size of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.11 Write Throughput

This metric shows the write throughput detail of a disk group mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes written from the disk group with proportion to the total write time for this disk group in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average write throughput of each disk, the total number of bytes written is divided by the total write time during the collection interval. This data is aggregated by the disk group name to get the average write throughput of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.19.12 Writes per Second

This metric shows the detail of total write requests per second for a disk group in an Automatic Storage Management (ASM) Instance. This metric shows the write performance of the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average writes per second for each disk, the total number of write responses is divided by the total write time during the collection interval. This data is aggregated by the disk group name to get the average writes per second of a disk group. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20 Instance Disk Performance Metrics

The Instance Disk Performance metrics indicate the performance of the disks present in an Automatic Storage Management (ASM) instance. These metrics show the disk performance parameters for all the disks mounted on an ASM Instance.

These metrics are used to collect information, for example, total I/O and read/write requests, total I/O and read/write time, and the total number of bytes read/written to the disk. These metrics also show the response of the disk for read, write, and I/O throughput.

1.20.1 I/O Size (MB)

This metric shows the sum of all disk I/O for all disks. The data is not aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average I/O size of each disk, the total number of bytes read and written is divided by the total number of I/Os during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.2 I/O Throughput

This metric shows the sum of I/O throughput for all disks. The data is displayed for all instances that are part of the cluster. This gives an indication of the disk group I/O performance in terms of read and write.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average throughput of each disk, the total number of bytes read and written is divided by the total I/O time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.3 IOPS

This metric shows the sum of disks I/O performance per second in terms of total I/O requests for all the disks. The data is displayed for all instances that are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average I/Os per second for each disk, the total number of I/O responses is divided by the total I/O time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.4 Read Response Time (MS)

This metric shows the disk read response time detail of the disks. This gives an indication for the disk response time in terms of total read requests for this disk.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average read response time for each disk, the total read time is divided by the total number of read responses during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.5 Read Size (MB)

This metric shows the sum of all disk reads for all disks which are part of the cluster. The data is *not* aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average read size of each disk, the total number of bytes read are divided by the total number of reads during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.6 Read Throughput

This metric shows the read throughput detail of a disk mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes read from the disk with proportion to the total read time for this disk in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average read throughput of each disk, the total number of bytes read is divided by the total read time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.7 Read Write Errors

This metric shows the detail of the total number of failed read/writes for the disk. This provides information about the total number of failed attempts of reads and writes for the disk.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	After Every Sample	>	Not Defined	0	1	Disk %dg_ name%.%disk_ name% has %value% Read/Write errors.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Instance ID", "Disk Group Name", and "Disk Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Instance ID", "Disk Group Name", and "Disk Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Instance ID", "Disk Group Name", and "Disk Name" objects, use the Edit Thresholds page.

Data Source

It is calculated using the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for

10*g* Release 2. From these views, the total number of failed read/writes for the disk is added to calculate the read write errors detail.

User Action

Investigate the issues behind read/write errors.

1.20.8 Reads Per Second

This metric shows the detail of total read requests per second for a disk in an Automatic Storage Management (ASM) instance. This metric shows the read performance of all the disks included in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average reads per second for each disk, the total number of read responses is divided by the total read time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.9 Response Time (MS)

This metric shows the I/O response time detail of mounted disks. For this disk, this metric indicates the response time in terms of total I/O requests for all the disks.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average I/O response time for each disk, the total I/O time is divided by the total number of I/O responses during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.10 Write Response Time (MS)

This metric shows the write response time detail of the disks. This gives an indication for the disk response time in terms of total write requests for this disk.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average write response time for each disk, the total write time is divided by the total number of write responses during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.11 Write Size (MB)

This metric shows the sum of all disk writes for all disks which are part of the cluster. The data is not aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average write size of each disk, the total number of bytes written is divided by the total number of writes during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.12 Write Throughput

This metric shows the write throughput detail of a disk mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes written from the disk with proportion to the total write time for this disk in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average write throughput of each disk, the total number of bytes written is divided by the total write time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.20.13 Writes Per Second

This metric shows the detail of total write requests per second for a disk in an Automatic Storage Management (ASM) Instance. This metric shows the write performance of the disk.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10g Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10g Release 2.

To calculate the average writes per second for each disk, the total number of write responses is divided by the total write time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21 Instance Volume Performance Metrics

The Instance Volume Performance metrics indicate the performance of the volumes present in an Automatic Storage Management (ASM) instance. These metrics show the volume performance parameters for all the volumes created on all disk groups mounted on an ASM Instance.

These metrics are used to collect information, for example, total I/O and read/write requests, total I/O and read/write time, and the total number of bytes read/written to the volume. These metrics also show the response of the volume for read, write, and I/O throughput and the Read Write Errors.

1.21.1 I/O Per Second

This metric shows the sum of ASM volume I/O performance per second in terms of total I/O requests for all the ASM Volumes. The data is displayed for all instances that are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average I/Os per second for each volume, the total number of I/O responses is divided by the total I/O time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.2 I/O Size (MB)

This metric shows the sum of all volume I/O for all volumes. The data is not aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average I/O size of each volume, the total number of bytes read and written is divided by the total number of I/Os during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.3 I/O Throughput

This metric shows the sum of I/O throughput for all volumes. The data is displayed for all instances that are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average throughput of each volume, the total number of bytes read and written is divided by the total I/O time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.4 Read Response Time (MS)

This metric shows the volume read response time detail of the volumes. This gives an indication of the volume response time in terms of total read requests for this volume.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average read response time for each volume, the total read time is divided by the total number of read responses during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.5 Read Size (MB)

This metric shows the sum of all volume reads for all volumes which are part of the cluster. The data is not aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average read size of each volume, the total number of bytes read are divided by the total number of reads during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.6 Read Throughput

This metric shows the read throughput detail of a volume created in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes read from the volume in proportion to the total read time for this volume in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average read throughput of each volume, the total number of bytes read is divided by the total read time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.7 Read Write Errors

This metric shows the detail of the total number of failed read/writes for the volume. This provides information about the total number of failed attempts of reads and writes for the volume.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views. From these views, the total number of failed read/writes for the volume is added to calculate the read write errors detail.

User Action

Investigate the issues behind read/write errors.

1.21.8 Reads Per Second

This metric shows the detail of total read requests per second for a volume in a disk group in an Automatic Storage Management (ASM) instance. This metric shows the read performance of all the volumes included in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average reads per second for each volume, the total number of read responses is divided by the total read time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.9 Response Time (MS)

This metric shows the I/O response time detail of volumes. For this volume, this metric indicates the response time in terms of total I/O requests for all the volumes.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average I/O response time for each volume, the total I/O time is divided by the total number of I/O responses during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.10 Write Response Time (MS)

This metric shows the write response time detail of the volumes. This gives an indication for the volume response time in terms of total write requests for this volume.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average write response time for each volume, the total write time is divided by the total number of write responses during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.11 Write Size (MB)

This metric shows the sum of all volume writes for all volumes which are part of the cluster. The data is not aggregated for all instances.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average write size of each volume, the total number of bytes written is divided by the total number of writes during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.12 Write Throughput

This metric shows the write throughput detail of a volume created on a disk group in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes written from the volume with proportion to the total write time for this volume in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average write throughput of each volume, the total number of bytes written is divided by the total write time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.21.13 Writes Per Second

This metric shows the detail of total write requests per second for a Volume in an Automatic Storage Management (ASM) Instance. This metric shows the write performance of the volume.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every Hour

Data Source

It is calculated using the Instance Volume Performance metric which in turn collects data from the GV$ASM_DISKGROUP_STAT and GV$ASM_VOLUME_STAT views.

To calculate the average writes per second for each volume, the total number of write responses is divided by the total write time during the collection interval. The data is displayed for all instances that are part of the cluster.

User Action

No user action is required.

1.22 Offline Disk Count Metric

The Offline Disk Count metric provides the count of the disk with mode status offline.

User can change the time limit and threshold limit.

1.22.1 Offline Disk Count

This metric provides the count of the disk with mode status offline. A critical alert is generated if the offline disk count changes or any of the disks go offline.

You can change the time limit and threshold limit as required.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 15 Minutes	After Every Sample	>	Not Defined	0	1	%offline_count% disks are offline.

Data Source

This metric is collected with the help of Disk Status metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

User Action

Try to bring the disk online. Currently Enterprise Manager does not support this administration feature so it needs to be done manually.

1.23 Operational Error Metrics

The Operational Error metrics represent errors that may affect the operation of the ASM, for example, data block corruption, media failure, and so on as recorded in the ASM alert log file. The alert log file has a chronological log of messages and errors.

Each metric signifies that the ASM being monitored has detected a critical error condition that may affect the normal operation of the ASM and has generated an error message to the alert log file since the last sample time. The Support Workbench in Enterprise Manager may contain more information about the error.

1.23.1 Alert Log Error Trace File

This metric is the name of the trace file (if any) associated with the logged error.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

1.23.2 Alert Log Name

This metric is the name of the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

1.23.3 Data Block Corruption

This metric signifies that the ASM being monitored has generated a corrupted block error (ORA-01157 or ORA-27048) to the alert file since the last sample time. The alert file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages are written to the alert file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A data block was corrupted at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

1.23.4 Generic Operational Error

This metric signifies that the ASM being monitored has generated some error that may affect the normal operation of the ASM to the alert file since the last sample time. The alert file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages are written to the alert file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Operational error (%errCodes%) detected in %alertLogName % at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

1.23.5 Media Failure

This metric signifies that the ASM being monitored has generated a media failure error (ORA-01242 or ORA-01243) to the alert file since the last sample time. The alert file is a

special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages are written to the alert file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Media failure detected in %alertLogName % at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

Data Source

The data comes from the alert log files. It is collected using the Perl script $ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

1.24 Operational Error Status Metrics

The Operational Error Status metrics place all the types of alert log errors into the following categories: Data Block Corruption, Media Failure, and Generic Operational Error. These metrics represent whether the last scan of the alert log identified any of the aforementioned categories of error and, if so, how many.

1.24.1 Data Block Corruption Error Status

This metric reflects the number of Data Block Corruption alert log errors witnessed the last time Enterprise Manager scanned the Alert Log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Data block corruption errors have been found in the alert log.

Data Source

Alert Log metric

User Action

Examine the Alert Log.

1.24.2 Generic Operational Error Status

This metric reflects the number of Generic Operation Error errors witnessed the last time Enterprise Manager scanned the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	%value% distinct types of operational errors have been found in the alert log.

Data Source

Operational Error metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

1.24.3 Media Failure Status

This metric reflects the number of Media Failure errors witnessed the last time Enterprise Manager scanned the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Media failure errors have been found in the alert log.

Data Source

Operational Error metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

1.25 Response Metric

The Response metric shows the status of the Automatic Storage Management (ASM) instance. It shows whether the instance is up or down. The check is performed every five minutes and returns the status of the connection as successful or it displays the ORA error for connection failure. This generates a critical alert if the ASM instance is down.

1.25.1 Status

This metric shows the status of the Automatic Storage Management (ASM) instance. It displays whether the instance is up or down. This check is performed every five minutes and returns the status of the connection as successful or it displays the ORA error for connection failure. This generates a critical alert if the ASM instance is down.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	=	Not Defined	0	1	Failed to connect to ASM instance %oraerr%.

Data Source

You can establish a connection to the ASM instance with instance properties, and if the connection succeeds then the status is shown as Up, otherwise is displays as Down. It may also display as Down if there is an error in the metric collection.

User Action

Perform one of the following:

- Check that the configuration property saved for the ASM instance is correct.
- If it displays as Down, the ASM instance is down. Try to reestablish the connection using the startup/shutdown feature using the Enterprise Manager application. Alternately, you can restart the application manually.

1.26 Single Instance Disk Group Performance Metrics

The Single Instance Disk Group Performance metrics indicate the performance of the single instance disk group present in an Automatic Storage Management (ASM) instance. These metrics are used to collect information, for example, total I/O and read/write requests, total I/O and read/write time, and the total number of bytes read/written to the disk group. These metrics also show the response of the disk group for read, write, and I/O throughput.

1.26.1 I/O Per Second

This metric shows the sum of disks I/O performance per second in terms of total I/O requests for all the disks within the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average I/Os per second for each disk, the total number of I/O responses is divided by the total I/O time during the collection interval. This data is aggregated by the disk group name to get the average I/O per second of a disk group.

User Action

No user action is required.

1.26.2 I/O Size (MB)

This metric shows the sum of all disk I/O for all disks within the disk group for one and only one instance. This is the instance that the user connects to using the UI navigation path.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average I/O size of each disk, the total number of bytes read and written is divided by the total number of I/Os during the collection interval. This data is aggregated by the disk group name to get the average I/O size of a disk group.

User Action

No user action is required.

1.26.3 I/O Throughput

This metric shows the sum of I/O throughput for all disks within the disk group. This gives an indication of the disk group I/O performance in terms of reads and writes for the instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average throughput of each disk, the total number of bytes read and written is divided by the total I/O time during the collection interval. This data is aggregated by the disk group name to get the average I/O throughput of a disk group.

User Action

No user action is required.

1.26.4 Read Response Time (MS)

This metric shows the read response time detail for the disk group mounted on the Automatic Storage Management (ASM) instance. This gives an indication for the disk group response time in terms of total read requests for this disk.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average read response time for each disk, the total read time is divided by the total number of read responses during the collection interval. This data is aggregated by the disk group name to get the average read response time of a disk group.

User Action

No user action is required.

1.26.5 Read Size (MB)

This metric shows the sum of all disk reads for all disks within the disk group which are part of the cluster.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average read size of each disk, the total number of bytes read are divided by the total number of reads during the collection interval. This data is aggregated by the disk group name to get the average read size of a disk group.

User Action

No user action is required.

1.26.6 Read Throughput

This metric shows the read throughput detail of a disk group mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes read from the disk group with proportion to the total read time for this disk group in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average read throughput of each disk, the total number of bytes read is divided by the total read time during the collection interval. This data is aggregated by the disk group name to get the average read throughput of a disk group.

User Action

No user action is required.

1.26.7 Reads Per Second

This metric shows the detail of total read requests per second for the single instance disk group in an Automatic Storage Management (ASM) instance. This metric shows the read performance of all the disks included in the disk group of an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average reads per second for each disk, the total number of read responses is divided by the total read time during the collection interval. This data is aggregated by the disk group name to get the average reads per second of a disk group.

User Action

No user action is required.

1.26.8 Response Time (MS)

This metric shows the I/O response time detail of a mounted single instance disk group. For this disk group, this metric indicates the response time in terms of total I/O requests for all the disks included in the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average I/O response time for each disk, the total I/O time is divided by the total number of I/O responses during the collection interval. This data is aggregated by the disk group name to get the average I/O response time of a disk group.

User Action

No user action is required.

1.26.9 Write Response Time (MS)

This metric shows the write response time detail for a disk group in an Automatic Storage Management (ASM) instance. This gives an indication for the disk group response time in terms of total write requests for the disks included in the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average write response time for each disk, the total write time is divided by the total number of write responses during the collection interval. This data is aggregated by the disk group name to get the average write response time of a disk group.

User Action

No user action is required.

1.26.10 Write Size (MB)

This metric shows the sum of all disk writes for all disks within the disk group which are part of the cluster. This is the instance that the user connects to using the UI navigation path.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average write size of each disk, the total number of bytes written is divided by the total number of writes during the collection interval. This data is aggregated by the disk group name to get the average write size of a disk group.

User Action

No user action is required.

1.26.11 Write Throughput

This metric shows the write throughput detail of a disk group mounted in an Automatic Storage Management (ASM) instance. This gives an indication for the total number of bytes written from the disk group with proportion to the total write time for this disk group in an instance.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average write throughput of each disk, the total number of bytes written is divided by the total write time during the collection interval. This data is aggregated by the disk group name to get the average write throughput of a disk group.

User Action

No user action is required.

1.26.12 Writes Per Second

This metric shows the details of total write requests per second for the disk group mounted on the Automatic Storage Management (ASM) instance. This metric shows the write performance of the disk group.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

It is calculated using the Instance Disk Performance metric which in turn collects data from the GV$ASM_DISKGROUP and GV$ASM_DISK views for 10*g* Release 1 and the GV$ASM_DISKGROUP_STAT and GV$ASM_DISK_STAT views for 10*g* Release 2.

To calculate the average writes per second for each disk, the total number of write responses is divided by the total write time during the collection interval. This data is aggregated by the disk group name to get the average writes per second of a disk group.

User Action

No user action is required.

2

Cluster

The Oracle RAC database metrics provide the following information for each metric:

- Description
- Metric summary. The metric summary can include some or all of the following: target version, evaluation frequency, collection frequency, upload frequency, operator, default warning threshold, default critical threshold, consecutive number of occurrences preceding notification, and alert text.
- Multiple Thresholds (where applicable)
- Data source
- User action

2.1 Clusterware

The metrics in this category provide an overview of the clusterware status for this cluster, how many nodes in this cluster have problems, and the CLUVFY utility output for all the nodes of this cluster. Generally, the clusterware is up if the clusterware on at least one host is up.

2.1.1 Cluster Verification Output

This metric shows the CLUVFY output of clusterware for all nodes of this cluster.

Data Source

The load list is:

cluvfy comp crs -n node1, node2 ...

where node1, node2 is the node list for the cluster.

User Action

Search for the CLUVFY utility in the 10g Release 2 Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide.

2.1.2 Clusterware Status

This metric shows the overall clusterware status for this cluster. The clusterware is up if the clusterware on at least one host is up.

Metric Summary

The following table shows how often the metric's value is collected.

Table 2–1 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.0	Every 5 Minutes	After Every Sample	=	2	0	1	Clusterware has problems on all hosts of this cluster. %CRS_output%

Note: Although the warning threshold by default is 0, you can change this value to represent how many nodes should have problems before an alert is triggered.

Data Source

The load list is:

cluvfy comp crs -n node1, node2 ...

User Action

Search for the CLUVFY utility in the 10g Release 2 Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide.

2.1.3 Node(s) with Clusterware Problem

This metric shows how many nodes have clusterware problems.

Data Source

The load list is:

cluvfy comp crs -n node1, node2 ...

where node1, node2 is the node list for the cluster.

Metric Summary

The following table shows how often the metric's value is collected.

Table 2–2 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	>	0	Not Defined	1	There are %CRS_ failed_node_count% host(s) with Clusterware problems. %CRS_ output%

Note: Although the warning threshold by default is 0, you can change this value to represent how many nodes have problems before an alert is triggered.

User Action

Search for the CLUVFY utility in the 10g Release 2 Oracle Clusterware and Oracle Real Application Clusters Administration and Deployment Guide.

2.2 Clusterware Alert Log

Cluster Alert Log metrics

2.2.1 Alert Log Name

This column shows the name and full path of the CRS alert log.

This metric appears in Enterprise Manager Grid Control 10.2.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
CRS Version 10.2	Every 5 Minutes

2.2.2 Clusterware Service Alert Log Error

This metric collects certain error messages in the CRS alert log at the cluster level.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 2–3 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	CONTAINS	Not Defined	CRS-	1*	%crsErrStack% See %alertLogName for details.

* After an alert is triggered for this metric, you must manually clear it.

Multiple Thresholds

For this metric, you can set different warning and critical threshold values for each "Time/Line Number" object. If warning or critical threshold values are currently set for any "Time/Line Number" object, you can view these thresholds on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

2.2.3 Node Configuration Alert Log Error

This column collects CRS-1607, 1802, 1803, 1804 and 1805 messages from the CRS alert log at the cluster level, and issues alerts based on the error code.

Metric Summary

This metric appears in version 10.2 of Enterprise Manager Grid Control.

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 2–4 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	MATCH	CRS-180(2|3|4|5)	CRS-1607	1*	%nodeErrStack% See %alertLogName for details.

* After an alert is triggered for this metric, you must manually clear it.

Multiple Thresholds

For this metric, you can set different warning and critical threshold values for each "Time/Line Number" object. If warning or critical threshold values are currently set for any "Time/Line Number" object, these thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

2.2.4 OCR Alert Log Error

This column collects CRS-1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008, 1010 and 1011 messages from CRS alert log at the cluster level and issue alerts based on the error code.

Metric Summary

This metric appears in version 10.2 of Enterprise Manager Grid Control.

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 2–5 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	MATCH	CRS-100(1|2|3|4|5|7)	CRS-(1006|1008|1010|1011)	1*	%ocrErrStack% See %alertLogName for details.

* After an alert is triggered for this metric, you must manually clear it.

Multiple Thresholds

For this metric, you can set different warning and critical threshold values for each "Time/Line Number" object. If warning or critical threshold values are currently set

for any "Time/Line Number" object, these thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

2.2.5 Voting Disk Alert Log Error

This column collects CRS-1607, 1802, 1803, 1804 and 1805 messages from the CRS alert log at the cluster level, and issues alerts based on the error code.

Metric Summary

This metric appears in version 10.2 of Enterprise Manager Grid Control.

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 2–6 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	MATCH	Not Defined	CRS-160(4|5|6)	1*	%votingErrStack% See %alertLogName for details.

* After an alert is triggered for this metric, you must manually clear it.

Multiple Thresholds

For this metric, you can set different warning and critical threshold values for each "Time/Line Number" object. If warning or critical threshold values are currently set for any "Time/Line Number" object, these thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

2.3 Response

This metric category contains the metrics that represent the status of the cluster; that is, whether it is up or down. As long as one of the member hosts is up, the cluster is up.

2.3.1 Status

This metric indicates the overall status of the hosts in the cluster. When all the hosts in the cluster are down, the cluster is considered unreachable.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. This metric is evaluated every minute on the OMS side to check if all the members are down.

Table 2–7 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every Minute	After Every Sample	=	Not Defined	0	1	Target is down -- all members are down.

Data Source

The calculation is based on the status of each member host. As long as one host is up, the cluster is up.

User Action

Check if the network is down or all the hosts for the cluster are shut down.

3

Cluster Database

The Oracle RAC database metrics provide the following information for each metric:

- Description
- Metric summary. The metric summary can include some or all of the following: target version, evaluation frequency, collection frequency, upload frequency, operator, default warning threshold, default critical threshold, consecutive number of occurrences preceding notification, and alert text.
- Multiple Thresholds (where applicable)
- Data source
- User action

3.1 Data Guard

The Data Guard metrics check the status, data not received, and data not applied for the databases in the Data Guard configuration.

3.1.1 Data Guard Status

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Use the Data Guard Status metric to check the status of each database in the Data Guard configuration.

By default, a critical and warning threshold value was set for this metric column. Alerts will be generated when threshold values are reached. You can edit the value for a threshold as required.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–1 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x	Every 5 Minutes	After Every Sample	CONTAINS	Warning	Error	1	The Data Guard status of %dg_name% is %value%.

User Action

1. Check the Edit Properties General page for the primary and standby databases for detailed information.
2. Examine the database alert logs and the Data Guard broker logs for additional information.

3.1.2 Data Not Applied (logs)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

The broker computes the highest applied SCN and uses its value to find the last continuous log that was successfully archived to the standby database. Redo data in all subsequent log files are counted as logs not applied. If the primary database goes down at this point, the redo data from these log files can be applied on the standby database. If there is a gap in the log files received on the standby database, any log files received after the gap cannot be applied.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database and log apply services is currently applying log 1, log apply services can continue to apply up to log 3. Log apply services cannot apply any more log files because log 4 is missing. Even though log files 6, 7, and 9 are received, they cannot be applied and they will not be counted as data not applied.

If all the archived log files on the standby database are continuous, and standby redo logs are used, the standby redo logs are also counted as data not applied, unless real-time apply is turned on and log apply services is already working on the standby redo log files.

If the standby redo logs are multithreaded, the broker computes the highest applied SCN for every thread and totals the numbers. If there are multiple incarnations and the standby database is in a different incarnation from the primary database, each incarnation is computed separately and the results are then totaled.

3.1.3 Data Not Applied (MB)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

The broker computes the highest applied SCN and uses its value to find the last continuous log that was archived to the standby database. The size of redo data in all subsequent log files are counted as data not applied. If the primary database goes down at this point, redo from these log files can be applied on the standby database. If there is a gap in the log files received on the standby database, any log files received after the gap cannot be applied.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database and log apply services is currently applying log 1, log apply services can continue to apply up

to log 3. Log apply services cannot apply any more log files because log 4 is missing. Even though log files 6, 7, and 9 are received, they cannot be applied and they will not be counted as data not applied. In this case, the total size of log files 1, 2, and 3 is the size of Data Not Applied.

If all the archived log files on the standby database are continuous, and standby redo log files are used, the standby redo log files are also counted as data not applied, unless real-time apply is turned on and log apply services is already working on the standby redo log files. The size of an archived log file is its file size. However, the size of a standby redo log is the size of the actual redo in the log and not the file size.

If the standby redo log files are multithreaded, the broker computes the highest applied SCN for every thread and totals the numbers. If there are multiple incarnations and the standby database is in a different incarnation from the primary database, each incarnation is computed separately and the results are then totaled.

3.1.4 Data Not Received (logs)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

The broker computes the highest applied SCN and uses its value to find the last continuous log file that was successfully archived to the standby database. Redo data in all subsequent log files, including the current online redo log file, are counted as log files for potential data loss and will be unrecoverable if the primary database goes down at this point.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database, and if log 10 is the current online log file, and if log apply services are currently applying log 1, the last continuous log after the highest applied SCN is log 3. All log files after log 3, that is log files 4 through 10, are counted as data not received. If the primary database goes down at this point, all redo data in log files 4 through 10 are lost on the standby database.

If the primary database is multithreaded (in a RAC database), the broker computes the highest applied SCN for every thread and totals the numbers. If the primary database has multiple incarnations (for example, due to a flashback operation) and the standby database is in a different incarnation from the primary database, the computation is done on each incarnation and the results are then totaled.

3.1.5 Data Not Received (MB)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

The broker computes the highest applied SCN and uses its value to find the last continuous log file that was successfully archived to the standby database. The size of redo data in all subsequent log files, including the current online redo log file, are counted as data for potential data loss and will be unrecoverable if the primary database goes down at this point. The size of an archived log file is its file size, and the size of the online redo log file is the size of the actual redo in the online log file, not the file size of the online redo log file.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database, and if log 10 is the current online log file, and if log apply services is currently applying log 1, the last continuous log after the highest applied SCN is log 3. All log files after log 3, that is log files 4 through 10, are counted as data not received and the total size of redo data in these log files is the size of Data Not Received.

If the primary database is multithreaded (in a RAC database), the broker computes the highest applied SCN for every thread and totals the numbers. If the primary database has multiple incarnations (for example, due to a flashback operation) and the standby database is in a different incarnation from the primary database, the computation is done on each incarnation and the results are then totaled.

3.2 Data Guard Fast-Start Failover

The metrics in this category are database-level metrics. For cluster databases, these metrics are monitored at the cluster database target level and not by member instances. The metrics are:

Table 3–2 Data Guard Fast-Start Failover Metrics

Metric
Current Fast-Start Failover Target
Fast-Start Failover Occurred
Fast-Start Failover Time
New Fast-Start Failover SCN
Previous Fast-Start Failover SCN

3.3 Data Guard Performance

Data Guard Performance metrics

3.3.1 Apply Lag (seconds)

Displays (in seconds) how far the standby is behind the primary.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Data Source

v$dataguard_stats('apply lag')

3.3.2 Estimated Failover Time (seconds)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric shows the approximate number of seconds required to failover to this standby database. This accounts for the startup time, if necessary, plus the remaining time required to apply all the available redo on the standby. If a bounce is not required, it is only the remaining apply time.

Data Source

v$dataguard_stats ('estimated startup time','apply finish time','standby has been open')

3.3.3 Redo Apply Rate (KB/second)

Displays the Redo Apply Rate in KB/second on this standby.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

3.3.4 Redo Generation Rate (KB/second)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

3.3.5 Transport Lag (seconds)

The approximate number of seconds of redo not yet available on this standby database. This may be because the redo has not yet been shipped or there may be a gap.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Data Source

v$dataguard_stats('transport lag')

3.4 Data Guard Status

The Data Guard metrics check the status, data not received, and data not applied for the databases in the Data Guard configuration.

3.4.1 Data Guard Status

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Use the Data Guard Status metric to check the status of each database in the Data Guard configuration.

By default, a critical and warning threshold value was set for this metric column. Alerts will be generated when threshold values are reached. You can edit the value for a threshold as required.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–3 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x	Every 5 Minutes	After Every Sample	CONTAINS	Warning	Error	1	The Data Guard status of %dg_name% is %value%.

User Action

1. Check the Edit Properties General page for the primary and standby databases for detailed information.

2. Examine the database alert logs and the Data Guard broker logs for additional information.

3.5 Database Cardinality

This metric category contains the metrics that monitor the number of active instances of a cluster database.

3.5.1 Open Instance Count

This metric monitors how many instances are in an open state.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

3.5.2 Total Instance Count

This metric monitors how many instances this cluster database has. This metric is collected at 5-minute intervals and applies for all versions of cluster databases.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

3.6 Database Job Status

This metric category contains the metrics that represent the health of database jobs registered through the DBMS_JOB interface.

3.6.1 Broken Job Count

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

The Oracle Server job queue is a database table that stores information about local jobs such as the PL/SQL call to execute for a job such as when to run a job. Database replication is also managed by using the Oracle job queue mechanism using jobs to push deferred transactions to remote master sites, to purge applied transactions from the deferred transaction queue, or to refresh snapshot refresh groups.

A job can be broken in two ways:

Oracle has failed to successfully execute the job after sixteen attempts. The job has been explicitly marked as broken by using the procedure DBMS_ JOB.BROKEN.

This metric checks for broken DBMS jobs. A critical alert is generated if the number of broken jobs exceeds the value specified by the threshold argument.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–4 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	Not Uploaded	>	0	Not Defined	1	%value% job(s) are broken.

Data Source

```
SELECT COUNT(*)
  FROM dba_jobs
  WHERE broken < > 'N'
```

User Action

Check the ALERT log and trace files for error information. Correct the problem that is preventing the job from running. Force immediate re-execution of the job by calling DBMS_JOB.RUN.

3.6.2 Failed Job Count

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

The Oracle Server job queue is a database table that stores information about local jobs such as the PL/SQL call to execute for a job such as when to run a job. Database replication is also managed by using the Oracle job queue mechanism using jobs to push deferred transactions to remote master sites, to purge applied transactions from the deferred transaction queue or to refresh snapshot refresh groups.

If a job returns an error while Oracle is attempting to execute it, the job fails. Oracle repeatedly tries to execute the job doubling the interval of each attempt. If the job fails sixteen times, Oracle automatically marks the job as broken and no longer tries to execute it.

This metric checks for failed DBMS jobs. An alert is generated if the number of failed job exceeds the value specified by the threshold argument.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–5 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	Not Uploaded	>	0	Not Defined	1	%value% job(s) have failed.

Data Source

```
SELECT COUNT(*)
  FROM dba_jobs
  WHERE NVL(failures, 0) < >  0"
```

User Action

Check the ALERT log and trace files for error information. Correct the problem that is preventing the job from running.

3.7 Database Wait Bottlenecks

This metric category contains the metrics that approximate the percentage of time spent waiting by user sessions across instances for the cluster database. This approximation takes system-wide totals and discounts the effects of sessions belonging to background processes.

3.7.1 Active Sessions Using CPU

This metric represents the active sessions using CPU.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute

3.7.2 Active Sessions Waiting: I/O

This database-level metric represents the active sessions waiting for I/O. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute

3.7.3 Active Sessions Waiting: Other

This database-level metric represents all the waits that are neither idle nor user I/O. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute

3.7.4 Average Database CPU (%)

This metric represents the average database CPU across instances as a percentage.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

3.7.5 Host CPU Utilization (%)

This metric represents the percentage of CPU being used across hosts.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes

3.7.6 Load Average

This metric is the sum of the current CPU load for all cluster database hosts.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

3.7.7 Maximum CPU

This metric represents the total CPU count across all the cluster database hosts.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes

3.7.8 Wait Time (%)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric represents the percentage of time spent waiting, database-wide, for resources or objects during this sample period.

This test checks the percentage time spent waiting, database-wide, for resources or objects during this sample period. If the % Wait Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–6 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	Not Defined	Not Defined	3	%value%% of database service time is spent waiting.

Table 3–7 Metric Summary Table

Target Version	Server Evaluation Frequency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every Minute	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	3	Generated By Database Server

Data Source

DeltaTotalWait / (DeltaTotalWait + DeltaCpuTime) where:

- DeltaTotalWait: Difference of 'sum of time waited for all wait events in v$system_event' between sample end and start.
- DeltaCpuTime: Difference of 'select value from v$sysstat where name='CPU used by this session' between sample end and start.

User Action

Investigate further into which specific wait events are responsible for the bulk of the wait time. Individual wait events may identify unique problems within the database. Diagnosis will be tailored where appropriate through drilldowns specific to individual wait events.

3.8 Deferred Transactions

This metric category contains the metrics associated with this distributed database's deferred transactions.

3.8.1 Deferred Transaction Count

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Oracle uses deferred transactions to propagate data-level changes asynchronously among master sites in an advanced replication system as well as from an updatable snapshot to its master table.

This metric checks for the number of deferred transactions. An alert is generated if the number of deferred transactions exceeds the value specified by the threshold argument.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–8 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	Not Uploaded	>	100	Not Defined	3	Number of deferred transactions is %value%.

Data Source

```
SELECT count(*)
  FROM sys.deftran
```

User Action

When the advanced replication facility pushes a deferred transaction to a remote site, it uses a distributed transaction to ensure that the transaction has been properly committed at the remote site before the transaction is removed for the queue at the local site. If transactions are not being pushed to a given remote site, verify that the destination for the transaction was correctly specified. If you specify a destination database when calling DBMS_DEFER_SYS.SCHEDULE_EXECUTION using the DBLINK parameter, or DBMS_DEFER_SYS.EXECUTE using the DESTINATION parameter, make sure the full database link is provided.

Wrong view destinations can lead to erroneous deferred transaction behavior. Verify that the DEFCALLEST and DEFTRANDEST views are the definitions from the CATREPC.SQL and not those from CATDEFER.SQL.

3.8.2 Deferred Transaction Error Count

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Oracle uses deferred transactions to propagate data-level changes asynchronously among master sites in an advanced replication system as well as from an updatable snapshot to its master table. If a transaction is not successfully propagated to the remote site, Oracle rolls back the transaction, logs the transaction in the SYS.DEFERROR view in the remote destination database.

This metric checks for the number of transactions in SYS.DEFERROR view and raises an alert if it exceeds the value specified by the threshold argument.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–9 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	Not Uploaded	>	0	Not Defined	3	Number of deferred transactions with errors is %value%.

Data Source

```
SELECT count(*)
  FROM sys.deferror
```

User Action

An error in applying a deferred transaction may result from a database problem, such as a lack of available space in the table to be updated, or may be the result of an unresolved insert, update, or delete conflict. The SYS.DEFERROR view provides the ID of the transaction that could not be applied. Use this ID to locate the queued calls associated with the transaction. These calls are stored in the SYS.DEFCALL view. You can use the procedures in the DBMS_DEFER_QUERY package to determine the arguments to the procedures listed in the SYS.DEFCALL view.

3.9 Failed Logins

The metric in this metric category checks for the number of failed logins on the target database. This check is performed every ten minutes and returns the number of failed logins for that ten-minute interval. This metric will only work for databases where the audit_trail initialization parameter is set to DB or XML and the session is being audited.

3.9.1 Failed Login Count

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric checks for the number of failed logins on the target database. This check is performed every ten minutes and returns the number of failed logins for that ten-minute interval. This metric will only work for databases where the audit_trail initialization parameter is set to DB or XML and the session is being audited.

If the failed login count crosses the values specified in the threshold arguments, then a warning or critical alert is generated. Since it is important to know every time a significant number of failed logins occurs on a system, this metric will generate a new alert for any ten-minute interval where the thresholds are crossed. You can manually clear these alerts; they will not automatically clear after the next collection.

Data Source

The database stores login information in different views based on the audit_trail setting. The database views used are:

- DB or DB_EXTENDED: DBA_AUDIT_SESSION
- XML (10*g* Release 2 only): DBA_COMMON_AUDIT_TRAIL

3.10 Flash Recovery

This metric category contains the metrics representing flash recovery.

3.10.1 Flash Recovery Area

This metric returns the Flash Recovery Area Location.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary 10gR1 or higher Collection every 5 minutes Not evaluated (not alertable)

Data Source

```
SELECT value
  FROM v$parameter
  WHERE name='db_recovery_file_dest';
```

3.10.2 Flashback On

This metric returns whether or not flashback logging is enabled - YES or NO.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric returns whether or not flashback logging is enabled - YES or NO.

Metric Summary 10gR1 or higher Collection every 5 minutes Not evaluated (not alertable)

Data Source

```
SELECT flashback_on
  FROM v$database;
```

3.10.3 Log Mode

This metric returns the log mode of the database - ARCHIVELOG or NOARCHIVELOG.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary 10gR1 or higher Collection every 5 minutes Not evaluated (not alertable)

Data Source

```
SELECT log_mode
  FROM v$database;
```

3.10.4 Oldest Flashback Time

This metric represents the oldest point-in-time to which you can flashback your database.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary 10gR1 or higher Collection every 5 minutes Not evaluated (not alertable)

Data Source

```
SELECT to_char(oldest_flashback_time, 'YYYY-MM-DD HH24:MI:SS')
  FROM v$flashback_database_log;
```

3.10.5 Usable Flash Recovery Area (%)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric represents the percentage of space usable in the flash recovery area. The space usable is composed of the space that is free in addition to the space that is reclaimable.

Metric Summary 10gR2 or higher Collection every 5 minutes Not evaluated (not alertable)

Data Source

```
SELECT (100 - sum(percent_space_used)) + sum(percent_space_reclaimable)
  FROM v$flash_recovery_area_usage;
```

3.11 Invalid Objects

This metric category contains the metrics associated with invalid objects.

3.11.1 Total Invalid Object Count

This metric represents the total invalid object count.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–10 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	Not Uploaded	>	Not Defined	Not Defined	1	%value% object(s) are invalid in the database.

3.12 Invalid Objects by Schema

This metric category contains the metrics that represent the number of invalid objects in each schema.

3.12.1 Owner's Invalid Object Count

This metric represents the invalid object count by owner.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–11 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	Not Uploaded	>	2	Not Defined	1	%value% object(s) are invalid in the %owner% schema.

Data Source

For each metric index:

```
SELECT count(1)
```

User Action

View the status of the database objects in the schema identified by the Invalid Object Owner metric. Recompile objects as necessary.

3.13 Recovery

This metric category contains the metrics representing database recovery.

3.13.1 Corrupt Data Block Count

This metric represents the count of corrupt data blocks.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary 9iR2 or higher Evaluated and Collected every 15 minutes Operator > Warning Threshold - 0 Critical Threshold - Not Defined Number of corrupt data blocks is %value%.

Data Source

```
SELECT count(unique(file#))
  FROM v$database_block_corruption;
```

User Action

Perform a database recovery.

3.13.2 Missing Media File Count

This metric represents the count of missing media files.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary 8i or higher Evaluated and Collected every 15 minutes Operator > Warning Threshold - 0 Critical Threshold - Not Defined Number of missing media files is %value%.

Data Source

```
SELECT count(file#)
  FROM v$datafile_header
  WHERE recover ='YES' OR error is not null;
```

User Action

You should perform a database recovery.

3.14 Recovery Area

This metric category contains the recovery area metrics.

3.14.1 Recovery Area Free Space (%)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric is evaluated by the server periodically every 15 minutes or during a file creation, whichever occurs first. It is also printed in the alert log. The Critical Threshold is set for < 3% and the Warning Threshold is set for < 15%. It is not user-customizable. The user is alerted the first time the alert occurs, and the alert is not cleared until the available space rises above 15%.

User Action

To free up space from the Flash Recovery Area, follow these steps:

1. Consider changing your RMAN retention policy. If you are using dataguard, then consider changing your RMAN archivelog deletion policy.
2. Back up files to a tertiary device, such as tape using the RMAN command BACKUP RECOVERY AREA.
3. Add disk space and increase the db_recovery_file_dest_size parameter to reflect the new space.
4. Delete unnecessary files using the RMAN DELETE command. If an OS command was used to delete files, then use RMAN CROSSCHECK and DELETE EXPIRED commands.

3.15 Response

This metric category contains the metrics that represent the overall responsiveness of the cluster database with respect to a client.

3.15.1 Status

This metric checks whether a new connection can be established to any cluster database instance. If the database is down, the maximum number of users is exceeded, or the listener is down, the database instance is down. If a new connection cannot be made to any cluster database instance, the cluster database is down. As long as one cluster database instance is up, the cluster database is up.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. This metric is evaluated every minute on the OMS side to check if all the members are down.

Table 3–12 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every Minute	After Every Sample	=	Not Defined	0	1	Target is down -- all members are down.

Data Source

The calculation is based on the status of each cluster database instance. As long as one database instance is up, the cluster database is up.

User Action

Check the status of each cluster database instance to determine if it is up. Also, check the listener to make sure it is running on all the nodes. If the listener is running, check to see if the number of users is at the session limit. Make sure at least one of the cluster database instances is up. For details, refer to the database instance Status metric.

3.16 Segment Advisor Recommendations

Oracle uses the Automatic Segment Advisor job to detect segment issues regularly within maintenance windows. It determines whether the segments have unused space that can be released. The Number of recommendations is the number of segments that have Reclaimable Space. The recommendations come from all runs of the automatic segment advisor job and any user-scheduled segment advisor jobs.

3.16.1 Number of recommendations

Oracle uses the Automatic Segment Advisor job to detect segment issues regularly within maintenance windows. It determines whether the segments have unused space that can be released. The Number of recommendations is the number of segments that have Reclaimable Space. The recommendations come from all runs of the automatic segment advisor job and any user-scheduled segment advisor jobs.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

3.17 Session Suspended

This metric category contains the metrics that represent the number of resumable sessions that are suspended due to a correctable error.

3.17.1 Session Suspended by Data Object Limitation

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric represents the session suspended by a data object limitation.

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

3.17.2 Session Suspended by Quota Limitation

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric represents the session suspended by a quota limitation.

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

3.17.3 Session Suspended by Rollback Segment Limitation

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric represents the session suspended by a rollback segment limitation.

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

3.17.4 Session Suspended by Tablespace Limitation

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric represents the session suspended by a tablespace limitation.

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

3.18 Snapshot Too Old

This metric category contains the snapshot too old metrics.

3.18.1 Snapshot Too Old due to Rollback Segment Limit

This database-level metric represents snapshots too old because of the rollback segment limit. This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

3.18.2 Snapshot Too Old due to Tablespace Limit

This database-level metric represents snapshots too old because of the tablespace limit. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

3.19 Streams Processes Count

This metric shows the total number of Streams capture processes, propagations, and apply processes at the local database. This metric also shows the number of capture processes, propagations, and apply processes that have encountered errors.

3.19.1 Apply Processes Having Errors

This metric shows the number of apply processes that have encountered errors at the local database.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 10 Minutes

Data Source

The information in this metric is in the `DBA_APPLY` data dictionary view.

User Action

If an apply process has encountered errors, then correct the conditions that caused the errors.

3.19.2 Capture Processes Having Errors

This metric shows the number of capture processes that have encountered errors at the local database.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 10 Minutes

Data Source

The information in this metric is in the `DBA_CAPTURE` data dictionary view.

User Action

If a capture process has encountered errors, then correct the conditions that caused the errors.

3.19.3 Number of Apply Processes

This metric shows the number of apply processes at the local database.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 10 Minutes

Data Source

The information in this metric is in the `DBA_APPLY` data dictionary view.

User Action

Use this metric to determine the total number of apply processes at the local database.

3.19.4 Number of Capture Processes

This metric shows the number of capture processes at the local database.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 10 Minutes

Data Source

The information in this metric is in the `DBA_CAPTURE` data dictionary view.

User Action

Use this metric to determine the total number of capture processes at the local database.

3.19.5 Number of Propagation Jobs

This metric shows the number of propagations at the local database.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 10 Minutes

Data Source

The information in this metric is in the `DBA_PROPAGATION` data dictionary view.

User Action

Use this metric to determine the total number of propagations at the local database.

3.19.6 Propagation Errors

This metric shows the number of propagations that have encountered errors at the local database.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 10 Minutes

Data Source

The information in this metric is in the `DBA_PROPAGATION` data dictionary view.

User Action

If a propagation has encountered errors, then correct the conditions that caused the errors.

3.20 Suspended Session

This metric category contains the metrics that represent the number of resumable sessions that are suspended due to a correctable error.

3.20.1 Suspended Session Count

This metric represents the number of resumable sessions currently suspended in the database.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–13 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x	Every 5 Minutes	Not Uploaded	>	0	Not Defined	1	%value% session(s) are suspended.

Data Source

```
SELECT count(*)
  FROM v$resumable
  WHERE status = 'SUSPENDED' and enabled = 'YES'
```

User Action

Query the v$resumable view to see what the correctable errors are that are causing the suspension. The method to correct each error depends on the nature of the error.

3.21 Tablespace Allocation

The metrics in this metric category check the amount of space used and the amount of space allocated to each tablespace. The used space can then be compared to the allocated space to determine how much space is unused in the tablespace. This metric is intended for reporting, rather than alerts. Historical views of unused allocated free space can help DBAs to correctly size their tablespaces, eliminating wasted space.

3.21.1 Tablespace Allocated Space (MB)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

The allocated space of a tablespace is the sum of the current size of its data files. A portion of this allocated space is used to store data while some may be free space. If segments are added to a tablespace, or if existing segments grow, they will use the allocated free space. The allocated free space is only available to segments within the tablespace. If, over time, the segments within a tablespace are not using this free space, the allocated free space is not being used.

This metric calculates the space allocated for each tablespace. It is not intended to generate alerts. Rather it should be used in conjunction with the Allocated Space Used (MB) metric to produce a historical view of the amount of space being used and unused by each tablespace.

Data Source

Tablespace Allocated Space (MB) is calculated by looping though the tablespaces data files and totalling the size of the data files.

3.21.2 Tablespace Used Space (MB)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

The allocated space of a tablespace is the sum of the current size of its data files. Some of this allocated space is used to store data, and some of it may be free space. If segments are added to a tablespace, or if existing segments grow, they will use the allocated free space. The allocated free space is only available to segments within the tablespace. If, over time, the segments within a tablespace are not using this free space, then the allocated free space is being wasted.

This metric calculates the space used for each tablespace. It is not intended to generate alerts. Rather it should be used in conjunction with the Tablespace Allocated Space (MB) metric to produce a historical view of the amount of space being used and unused by each tablespace.

Data Source

Tablespace Used Space (MB) is Tablespace Allocated Space (MB) Tablespace Allocated Free Space (MB) where:

Tablespace Allocated Space (MB) is calculated by looping through the tablespaces data files and totaling the size of the data files.

Tablespace Allocated Free Space (MB) is calculated by looping through the tablespaces data files and totaling the size of the free space in each data file.

3.22 Tablespaces Full

The metrics in this metric category check for the amount of space used by each tablespace. The used space is then compared to the available free space to determine tablespace fullness. The available free space accounts for the maximum data file size as well as available disk space. This means that a tablespace will not be flagged as full if data files can extend and there is enough disk space available for them to extend.

3.22.1 Tablespace Free Space (MB)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

As segments within a tablespace grow, the available free space decreases. If there is no longer any available free space, meaning data files reached their maximum size or there is no more disk space, then the creation of new segments or the extension of existing segments will fail.

This metric checks for the total available free space in each tablespace. This metric is intended for larger tablespaces, where the Available Space Used (%) metric is less meaningful. If the available free space falls below the size specified in the threshold arguments, then a warning or critical alert is generated.

If the version of the monitored database target is Oracle Database 10*g* Release 1 or later and the tablespace uses Local Extent Management, then the Oracle Database Server evaluates this metric internally every 10 minutes. Alternatively, if the version of the monitored Database target is Oracle 9*i* or earlier, or the tablespace uses Dictionary Extent Management, then the Oracle Management Agent tests the value of this metric every 30 minutes.

Data Source

MaximumSize Total Used Space where:

- TotalUsedSpace: Total used space in MB of tablespace
- MaximumSize: Maximum size (in MB) of the tablespace. The maximum size is determined by looping through the tablespaces data files, as well as additional free space on the disk that would be available for the tablespace should a data file autoextend.

User Action

Perform one of the following:

- Increase the size of the tablespace by: Enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace, thereby increasing the free space in this tablespace.
- Run the Segment Advisor on the tablespace.

3.22.2 Tablespace Space Used (%)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

As segments within a tablespace grow, the available free space decreases. If there is no longer any available free space, meaning data files have reached their maximum size or there is no more disk space, then the creation of new segments or the extension of existing segments will fail.

This metric checks the Available Space Used (%) for each tablespace. If the percentage of used space is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

If the version of the monitored database target is Oracle Database 10*g* Release 1 or later and the tablespace uses Local Extent Management, then the Oracle Database Server evaluates this metric internally every 10 minutes. Alternatively, if the version of the monitored Database target is Oracle 9*i* or earlier, or the tablespace uses Dictionary Extent Management, then the Oracle Management Agent tests the value of this metric every 30 minutes.

Metric Summary

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–14 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 30 Minutes	After Every Sample	>	85	97	1	Tablespace [%name%] is [%value% percent] full
10.2.0.x	Every 30 Minutes	After Every Sample	>	85	97	1	Not Defined

Table 3–15 Metric Summary Table

Target Version	Server Evaluation Frequency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every 10 Minutes	Every 30 Minutes	After Every Sample	>	85	97	1	Generated By Database Server

Data Source

(TotalUsedSpace / MaximumSize) * 100 where:

- TotalUsedSpace: total used space in MB of tablespace
- MaximumSize: Maximum size (in MB) of the tablespace. The maximum size is determined by looping through the tablespaces data files, as well as additional free space on the disk that would be available for the tablespace should a data file autoextend.

For additional information about the data source, refer to the fullTbsp.pl Perl script located in the sysman/admin/scripts directory.

User Action

Perform one of the following:

- Increase the size of the tablespace by: Enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace, thus increasing the free space in this tablespace.
- Run the Segment Advisor on the tablespace.

3.23 Tablespaces Full (dictionary managed)

The metrics in this metric category check for the amount of space used by each tablespace. The used space is then compared to the available free space to determine tablespace fullness. The available free space accounts for the maximum data file size as well as available disk space. This means that a tablespace will not be flagged as full if data files can extend, and there is enough disk space available for them to extend.

3.23.1 Tablespace Free Space (MB) (dictionary managed)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

As segments within a tablespace grow, the available free space decreases. If there is no longer any available free space, meaning data files have reached their maximum size or there is no more disk space, then the creation of new segments or the extension of existing segments will fail.

This metric checks for the total available free space in each tablespace. This metric is intended for larger tablespaces, where the Available Space Used (%) metric is less meaningful. If the available free space falls below the size specified in the threshold arguments, then a warning or critical alert is generated.

If the version of the monitored database target is Oracle Database 10*g* Release 1 or later and the tablespace uses Local Extent Management, then the Oracle Database Server evaluates this metric internally every 10 minutes. Alternatively, if the version of the monitored Database target is Oracle 9*i* or earlier, or the tablespace uses Dictionary Extent Management, then the Oracle Management Agent tests the value of this metric every 30 minutes.

Data Source

MaximumSize Total Used Space where:

- TotalUsedSpace: Total used space in MB of tablespace
- MaximumSize: Maximum size (in MB) of the tablespace. The maximum size is determined by looping through the tablespaces data files, as well as additional free space on the disk that would be available for the tablespace should a data file autoextend.

3.23.2 Tablespace Space Used (%) (dictionary managed)

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

As segments within a tablespace grow, the available free space decreases. If there is no longer any available free space, meaning data files have reached their maximum size or there is no more disk space, then the creation of new segments or the extension of existing segments will fail.

This metric checks the Available Space Used (%) for each tablespace. If the percentage of used space is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

If the version of the monitored database target is Oracle Database 10*g* Release 1 or later and the tablespace uses Local Extent Management, then the Oracle Database Server evaluates this metric internally every 10 minutes. Alternatively, if the version of the monitored Database target is Oracle 9*i* or earlier, or the tablespace uses Dictionary Extent Management, then the Oracle Management Agent tests the value of this metric every 30 minutes.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–16 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every 30 Minutes	After Every Sample	>	85	97	1	Tablespace [%name%] is [%value% percent] full

Data Source

(TotalUsedSpace / MaximumSize) * 100 where:

- TotalUsedSpace: Total used space in MB of tablespace
- MaximumSize: Maximum size (in MB) of the tablespace. The maximum size is determined by looping through the tablespaces data files, as well as additional free space on the disk that would be available for the tablespace should a data file autoextend.

User Action

Perform one of the following:

- Increase the size of the tablespace by: Enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace, thereby increasing the free space in this tablespace.

- Run the Segment Advisor on the tablespace.

3.24 Tablespaces With Problem Segments

The metrics in this metric category check for the following:

- The largest chunk-free space in the tablespace. If any table, index, cluster, or rollback segment within the tablespace cannot allocate one additional extent, then an alert is generated.
- Whether any of the segments in the tablespace are approaching their maximum extents. If, for any segment, the maximum number of extents minus the number of existing extents is less than 2, an alert is generated.

Only the tablespaces with problem segments are returned as results.

3.24.1 Segments Approaching Maximum Extents

Segments nearing the upper limit of maximum extents. This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 24 Hours

Data Source

The first 10 segment names approaching their MaxExtent in the tablespace.

User Action

If possible, increase the value of the segments MAXEXTENTS storage parameter. Otherwise, rebuild the segment with a larger extent size ensuring the extents within a segment are the same size by specifying STORAGE parameters where NEXT=INITIAL and PCTINCREASE = 0.

For segments that are linearly scanned, choose an extent size that is a multiple of the number of blocks read during each multiblock read. This ensures that the Oracle multiblock read capability is used efficiently.

3.24.2 Segments Approaching Maximum Extents Count

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric checks for segments nearing the upper limit of the number of maximum extents. If the number of segments is greater than the values specified in the threshold arguments, a warning or critical alert is generated.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–17 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	After Every Sample	>	0	Not Defined	1	%value% segments in %name% tablespace approaching max extents.

Data Source

Number of segments for which the maximum number of extents minus the number of existing extents is less than 2.

For additional information about the data source, refer to the problemTbsp.pl Perl script located in the sysman/admin/scripts directory.

User Action

If possible, increase the value of the segments MAXEXTENTS storage parameter. Otherwise, rebuild the segment with a larger extent size ensuring the extents within a segment are the same size by using a locally managed tablespace. For a dictionary managed tablespace, specify STORAGE parameters where NEXT=INITIAL and PCTINCREASE = 0.

3.24.3 Segments Not Able to Extend

This metric checks for segments that cannot allocate an additional extent.

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

Metric Summary

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 24 Hours

Data Source

The first 10 segment names that cannot allocate an additional extent in the tablespace.

User Action

Perform one of the following:

- Increase the size of the tablespace by enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.

3.24.4 Segments Not Able to Extend Count

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric checks for segments that cannot allocate an additional extent. If the number of segments is greater than the values specified in the threshold arguments, a warning or critical alert is generated.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–18 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	After Every Sample	>	0	Not Defined	1	%value% segments in %name% tablespace unable to extend.

Data Source

After checking for the largest chunk free space in the tablespace, this is the number of segments that cannot allocate an additional extent.

For additional information about the data source, refer to the problemTbsp.pl Perl script located in the sysman/admin/scripts directory.

User Action

Perform one of the following:

- Increase the size of the tablespace by enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace, thereby increasing the free space in this tablespace.

3.25 User Block

This metric category contains the metrics that tell to what extent, and how consistently, a given session is blocking multiple other sessions.

3.25.1 Blocking Session Count

This is a database-level metric. For cluster databases, this metric is monitored at the cluster database target level and not by member instances.

This metric signifies that a database user is blocking at least one other user from performing an action, such as updating a table. An alert is generated if the number of consecutive blocking occurrences reaches the specified value. The sessions being blocked can come from different instances.

Note: The catblock.sql script needs to be run on the managed database prior to using the User Blocks test. This script creates some additional tables, view, and public synonyms that are required by the User Blocks test.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 3–19 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	Not Uploaded	>	11	Not Defined	3	Session %sid% blocking %value% other sessions.

Table 3–20 Metric Summary Table

Target Version	Server Evaluation Frequency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every Minute	Every 15 Minutes	After Every Sample	>	11	Not Defined	3	Generated By Database Server

Data Source

```
SELECT blocking_sid, num_blocked
  FROM ( SELECT blocking_sid, SUM(num_blocked) num_blocked
  FROM ( SELECT l.id1, l.id2,
                MAX(DECODE(l.block, 1, i.instance_name||'-'||l.sid,
                2, i.instance_name||'-'||l.sid, 0 )) blocking_sid,
                SUM(DECODE(l.request, 0, 0, 1 )) num_blocked
         FROM gv$lock l, gv$instance i
         WHERE ( l.block!= 0 OR l.request > 0 ) AND
                 l.inst_id = i.inst_id
                 GROUP BY l.id1, l.id2)
  GROUP BY blocking_sid
  ORDER BY num_blocked DESC)
  WHERE num_blocked != 0
```

User Action

Either have the user who is blocking other users rollback the transaction, or wait until the blocking transaction has been committed.

4

Database Instance

The Oracle database metrics provide for each metric the following information:

- Description
- Metric summary. The metric summary can include some or all of the following: target version, evaluation frequency, collection frequency, upload frequency, operator, default warning threshold, default critical threshold, consecutive number of occurrences preceding notification, and alert text.
- Multiple Thresholds (where applicable)
- Data source
- User action

4.1 Idle Events

The following is a list of the Idle Events.

- ARCH random i/o
- ARCH sequential i/o
- KXFX: execution message dequeue - Slaves
- LGWR random i/o
- LGWR sequential i/o
- LGWR wait for redo copy
- Null event
- PL/SQL lock timer
- PX Deq Credit: need buffer
- PX Deq: Execute Reply
- PX Deq: Execution Msg
- PX Deq: Index Merge Close
- PX Deq: Index Merge Execute
- PX Deq: Index Merge Reply
- PX Deq: Join ACK
- PX Deq: Msg Fragment
- PX Deq: Par Recov Change Vector

- PX Deq: Par Recov Execute
- PX Deq: Par Recov Reply
- PX Deq: Parse Reply
- PX Deq: Table Q Normal
- PX Deq: Table Q Sample
- PX Deq: Txn Recovery Reply
- PX Deq: Txn Recovery Start
- PX Deque wait
- PX Idle Wait
- Queue Monitor Shutdown Wait
- Queue Monitor Slave Wait
- Queue Monitor Wait
- RFS random i/o
- RFS sequential i/o
- RFS write
- SQL*Net message from client
- SQL*Net message from dblink
- STREAMS apply coord waiting for slave message
- STREAMS apply coord waiting for some work to finish
- STREAMS apply slave idle wait
- STREAMS capture process filter callback wait for ruleset
- STREAMS fetch slave waiting for txns
- WMON goes to sleep
- async disk IO
- client message
- control file parallel write
- control file sequential read
- control file single write
- db file single write
- db file parallel write
- dispatcher timer
- gcs log flush sync
- gcs remote message
- ges reconfiguration to start
- ges remote message
- io done
- jobq slave wait

- lock manager wait for remote message
- log file parallel write
- log file sequential read
- log file single write
- parallel dequeue wait
- parallel recovery coordinator waits for cleanup of slaves
- parallel query dequeue
- parallel query idle wait - Slaves
- pipe get
- pmon timer
- queue messages
- rdbms ipc message
- recovery read
- single-task message
- slave wait
- smon timer
- statement suspended, wait error to be cleared
- unread message
- virtual circuit
- virtual circuit status
- wait for activate message
- wait for transaction
- wait for unread message on broadcast channel
- wait for unread message on multiple broadcast channels
- wakeup event for builder
- wakeup event for preparer
- wakeup event for reader
- wakeup time manager

4.2 Alert Log Metrics

Alert Log metrics are made up of the following:

- Section 4.2.1, "Alert Log Metrics"
- Section 4.2.2, "Alert Log Error Status Metrics"

4.2.1 Alert Log Metrics

The Alert Log metrics are used in creating the alert log, for example, data block corruption, terminated session, and so on.

4.2.1.1 Alert Log Error Trace File

This metric is the name of the trace file (if any) associated with the logged error.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.2.1.2 Alert Log Name

This metric is the name of the alert log file.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.2.1.3 Archiver Hung Alert Log Error

This metric signifies that the archiver of the database being monitored has been temporarily suspended since the last sample time.

If the database is running in ARCHIVELOG mode, an alert is displayed when archiving is hung (ORA-00257) messages are written to the ALERT file. The ALERT file is a special trace file containing a chronological log of messages and errors.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.xs	Every 15 Minutes	After Every Sample	CONTAINS	Not Defined	ORA-	1[1]	The archiver hung at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Examine ALERT log and archiver trace file for additional information; however, the most likely cause of this message is that the destination device is out of space to store the redo log file. Verify the device specified in the initialization parameter ARCHIVE_LOG_DEST is set up properly for archiving. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.2.1.4 Data Block Corruption Alert Log Error

This metric signifies that the database being monitored has generated a corrupted block error to the ALERT file since the last sample time. The ALERT file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages are written to the ALERT file.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.xs	Every 15 Minutes	After Every Sample	CONTAINS	Not Defined	ORA-	1[1]	A data block was corrupted at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Examine ALERT log for additional information. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.2.1.5 Generic Alert Log Error

This metric signifies that the database being monitored has generated errors to the ALERT log file since the last sample time. The ALERT log file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when Oracle Exception (ORA-006xx) messages are written to the ALERT log file. A warning is displayed when other ORA messages are written to the ALERT log file.

- For all supported databases monitored by Enterprise Manager release 10.2.0.4 Management Agent:

  Alert Log Filter - up to 1024 characters

  Warning or Critical Threshold - up to 256 characters

- For all supported databases monitored by Enterprise Manager release 10.2.0.5 Managaement Agent:

  Alert Log Filter - up to 4000 characters

  Warning or Critical Threshold - up to 4000 characters

Archiver hung (ORA-00257) and data block corrupted (ORA-01578) messages are sent out as separate metrics.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.xs	Every 15 Minutes	After Every Sample	MATCH	ORA-0*(600?|7445|4[0-9][0-9][0-9])[^0-9]	Not Defined	1[1]	ORA-error stack (%errCodes%) logged in %alertLogName%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Examine ALERT log for additional information. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.2.1.6 Media Failure Alert Log Error

This metric represents the media failure alert log error.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.xs	Every 15 Minutes	After Every Sample	CONTAINS	Not Defined	ORA-	1[1]	Media failure was detected at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.2.1.7 Session Terminated Alert Log Error

This metric signifies that a session terminated unexpectedly since the last sample time. The ALERT file is a special trace file containing a chronological log of messages and errors. An alert is displayed when session unexpectedly terminated (ORA-00603) messages are written to the ALERT file.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.xs	Every 15 Minutes	After Every Sample	CONTAINS	ORA-	Not Defined	1[1]	A session was terminated at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlog.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Examine the ALERT log and the session trace file for additional information. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.2.2 Alert Log Error Status Metrics

The Alert Log Error Status metrics place all the types of alert log errors into four categories: Archiver Hung, Data Block Corruption, Session Terminated, and Generic. The metrics in this category represent whether the last scan of the alert log identified any of the aforementioned categories of error and, if so, how many.

4.2.2.1 Archiver Hung Alert Log Error Status

This metric reflects the number of Archiver Hung alert log errors witnessed the last time Enterprise Manager scanned the Alert Log.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 Minutes	After Every Sample	>	0	Not Defined	1	Archiver hung errors have been found in the alert log.

Data Source

Alert Log metric

User Action

Examine the Alert Log.

4.2.2.2 Data Block Corruption Alert Log Error Status

This metric reflects the number of Data Block Corruption alert log errors witnessed the last time Enterprise Manager scanned the Alert Log.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 Minutes	After Every Sample	>	0	Not Defined	1	Data block corruption errors have been found in the alert log.

Data Source

Alert Log metric

User Action

Examine the Alert Log.

4.2.2.3 Generic Alert Log Error Status

This metric reflects the number of Generic alert log errors witnessed the last time Enterprise Manager scanned the Alert Log.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 Minutes	After Every Sample	>	0	Not Defined	1	%value% distinct types of ORA-errors have been found in the alert log.

Data Source

Alert Log metric

User Action

Examine the Alert Log.

4.2.2.4 Media Failure Alert Log Error Status

This metric represents the media failure alert log error status.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 Minutes	After Every Sample	>	0	Not Defined	1	Media failure errors have been found in the alert log.

Data Source

Not available

User Action

No user action is required.

4.2.2.5 Session Terminated Alert Log Error Status

This metric reflects the number of Session Terminated alert log errors witnessed the last time Enterprise Manager scanned the Alert Log.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 Minutes	After Every Sample	>	0	Not Defined	1	Session terminations have been found in the alert log.

Data Source

Alert Log metric

User Action

Examine the Alert Log.

4.3 Archive Area Metrics

This metric category contains the metrics representing the utilization of the archive areas.

If the database is running in ARCHIVELOG mode, these metrics check for available redo log destinations. If the database is not running in ARCHIVELOG mode, these metrics fail to register. For each destination, this metric category returns the total, used, and free space.

Note: The metrics do not monitor an archive destination if it is set to the flash recovery area.

4.3.1 Archive Area Used (%)

The Archive Full (%) metric returns the percentage of space used on the archive area destination. If the space used is more than the threshold value given in the threshold arguments, then a warning or critical alert is generated.

If the database is not running in ARCHIVELOG mode or all archive destinations are standby databases for Oracle8*i*, this metric fails to register.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 15 Minutes	After Every Sample	>	80	Not Defined	1	%value%% of archive area %archDir% is used.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Archive Area Destination" object.

If warning or critical threshold values are currently set for any "Archive Area Destination" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Archive Area Destination" object, use the Edit Thresholds page.

Data Source

If no quota is set for archive area, the percentage is calculated using the UNIX `df -k` command.

If quota is set:

```
archive area used (%) = (total area used / total archive area) * 100
```

User Action

Verify the device specified in the initialization parameter LOG_ARCHIVE_DEST is set up properly for archiving.

There are two methods you can use to specify archive destinations. These destinations can be setup using Enterprise Manager. For each database target, you can drill-down to the database **Availability** tab, and access the **Recovery Settings** page.

- The first method is to use the LOG_ARCHIVE_DEST_n parameter (where n is an integer from 1 to 10) to specify from one to ten different destinations for archival. Each numerically-suffixed parameter uniquely identifies an individual destination, for example, LOG_ARCHIVE_DEST_1, LOG_ARCHIVE_DEST_2, and so on.
- The second method, which allows you to specify a maximum of two locations, is to use the LOG_ARCHIVE_DEST parameter to specify a primary archive destination and the LOG_ARCHIVE_DUPLEX_DEST parameter to determine an optional secondary location.

If the LOG_ARCHIVE_DEST initialization parameter is set up correctly and this metric triggers, then free up more space in the destination specified by the archive destination parameters.

4.3.2 Archive Area Used (KB)

This metric represents the total space used (in KB) on the device containing the archive destination directory.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

If no quota is set for archive area, this is calculated through the UNIX `df -k` command.

```
total area used = quota_used * db_block_size (in KB)
```

User Action

Verify the device specified in the initialization parameter LOG_ARCHIVE_DEST is set up properly for archiving.

There are two methods you can use to specify archive destinations. These destinations can be setup using Enterprise Manager. For each database target, you can drill-down to the database **Availability** tab, and access the **Recovery Settings** page.

- The first method is to use the LOG_ARCHIVE_DEST_n parameter (where n is an integer from 1 to 10) to specify from one to ten different destinations for archival. Each numerically-suffixed parameter uniquely identifies an individual destination, for example, LOG_ARCHIVE_DEST_1, LOG_ARCHIVE_DEST_2, and so on.
- The second method, which allows you to specify a maximum of two locations, is to use the LOG_ARCHIVE_DEST parameter to specify a primary archive destination and the LOG_ARCHIVE_DUPLEX_DEST parameter to determine an optional secondary location.

If the LOG_ARCHIVE_DEST initialization parameter is set up correctly and this metric triggers, then free up more space in the destination specified by the archive destination parameters.

4.3.3 Free Archive Area (KB)

When running a database in ARCHIVELOG mode, the archiving of the online redo log is enabled. Filled groups of the online redo log are archived, by default, to the destination specified by the LOG_ARCHIVE_DEST initialization parameter. If this destination device becomes full, the database operation is temporarily suspended until disk space is available.

If the database is running in ARCHIVELOG mode, this metric checks for available redo log destination devices.

If the database is not running in ARCHIVELOG mode, this metric fails to register.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 15 Minutes	After Every Sample	<	Not Defined	Not Defined	1	Archive area %archDir% has %value% free KB remaining.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Archive Area Destination" object.

If warning or critical threshold values are currently set for any "Archive Area Destination" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Archive Area Destination" object, use the Edit Thresholds page.

Data Source

If the database is in NOARCHIVELOG mode, then nothing is collected.

If the database is in ARCHIVELOG mode, log_archive_destination from v$parameter is queried to obtain the current list of archivelog destinations. The results are obtained by directly checking the disk usage (df -kl).

User Action

Verify the device specified in the initialization parameter LOG_ARCHIVE_DEST is set up properly for archiving.

There are two methods you can use to specify archive destinations. These destinations can be setup using Enterprise Manager. For each database target, you can drill-down to the database **Availability** tab, and access the **Recovery Settings** page.

- The first method is to use the LOG_ARCHIVE_DEST_n parameter (where n is an integer from 1 to 10) to specify from one to ten different destinations for archival. Each numerically-suffixed parameter uniquely identifies an individual destination, for example, LOG_ARCHIVE_DEST_1, LOG_ARCHIVE_DEST_2, and so on.
- The second method, which allows you to specify a maximum of two locations, is to use the LOG_ARCHIVE_DEST parameter to specify a primary archive destination and the LOG_ARCHIVE_DUPLEX_DEST parameter to determine an optional secondary location.

If the LOG_ARCHIVE_DEST initialization parameter is set up correctly and this metric triggers, then free up more space in the destination specified by the archive destination parameters.

4.3.4 Total Archive Area (KB)

This metric represents the total space (in KB) on the device containing the archive destination directory.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

If no quota is set for archive area, this is calculated through the UNIX `df -k` command.

If quota is set:

```
total archive area = quota_size * db_block_size (in KB)
```

User Action

Oracle recommends that multiple archivelog destinations across different disks be configured. When at least one archivelog destination gets full, Oracle recommends the following:

- If tape is being used, back up archivelogs to tape and delete the archivelogs.
- If tape is not being used, back up the database and remove obsolete files. This also removes archivelogs that are no longer needed based on the database retention policy.
- If archivelog destination quota_size is being used, raise the quota_size.

4.4 Cluster Resource

This metric collects the Resource Name of the Oracle Database if the Oracle Database is managed by the cluster.

4.4.1 Resource Name

Resource Name of the Oracle Database Resource managed by the cluster.

4.5 Collect SQL Response Time Metrics

The Collect SQL response time metrics represent the SQL response time.

4.5.1 SQL Response Time (%)

This metric represents the SQL response time.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 5 Minutes

Data Source

Not available

User Action

No user action is required.

4.6 Data Failure Metrics

The Data Failure metrics represent data failures.

4.6.1 Alert Log Name

This metric is the name of the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.6.2 Data Failure Detected

This metric signifies that a database health checker has detected one or more persistent data failures. Examples of data failures include missing files, corrupt files, inconsistent files, and corrupt blocks. The alert shows the number of data failures detected by a checker run. Details of individual data failures can be accessed from the Perform Recovery page in Enterprise Manager.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Checker run found %numberOfFailures% new persistent data failures.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Details of individual data failures can be accessed from the Perform Recovery page in Enterprise Manager. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.7 Data Guard Metrics

Data Guard metrics are made up of the following:

4.7.1 Data Guard (10*i*)

Data Guard for release 10*i* metrics monitor the overall status of the Data Guard configuration, including the primary and all standby databases.

4.7.1.1 Data Guard Status

The Data Guard Status metric checks the status of each database in the broker configuration and triggers a warning or critical alert if necessary.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every 5 Minutes	After Every Sample	CONTAINS	Warning	Error	1	The Data Guard status of %dg_ name% is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.7.1.2 Data Not Applied (logs)

The broker computes the highest applied system change number (SCN) and uses its value to find the last continuous log that was successfully archived to the standby database. Redo data in all subsequent log files are counted as logs not applied. If the primary database goes down at this point, the redo data from these log files can be applied on the standby database. If there is a gap in the log files received on the standby database, any log files received after the gap cannot be applied.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database and log apply services is currently applying log 1, log apply services can continue to apply up to log 3. Log apply services cannot apply any more log files because log 4 is missing. Even though log files 6, 7, and 9 are received, they cannot be applied and they will not be counted as data not applied.

If all the archived log files on the standby database are continuous, and standby redo logs are used, the standby redo logs are also counted as data not applied, unless real-time apply is turned on and log apply services is already working on the standby redo log files.

If the standby redo logs are multithreaded, the broker computes the highest applied SCN for every thread and totals the numbers. If there are multiple incarnations and the standby database is in a different incarnation from the primary database, each incarnation is computed separately and the results are then totaled.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every 5 Minutes	After Every Sample	>	1	3	1	Standby database %dg_name% has not applied the last %value% received logs.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.7.1.3 Data Not Applied (MB)

The broker computes the highest applied system change number (SCN) and uses its value to find the last continuous log that was archived to the standby database. The size of redo data in all subsequent log files are counted as data not applied. If the primary database goes down at this point, redo from these log files can be applied on the standby database. If there is a gap in the log files received on the standby database, any log files received after the gap cannot be applied.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database and log apply services is currently applying log 1, log apply services can continue to apply up to log 3. Log apply services cannot apply any more log files because log 4 is missing. Even though log files 6, 7, and 9 are received, they cannot be applied and they will not be counted as data not applied. In this case, the total size of log files 1, 2, and 3 is the size of Data Not Applied.

If all the archived log files on the standby database are continuous, and standby redo log files are used, the standby redo log files are also counted as data not applied, unless real-time apply is turned on and log apply services is already working on the standby redo log files. The size of an archived log file is its file size. However, the size of a standby redo log is the size of the actual redo in the log and not the file size.

If the standby redo log files are multithreaded, the broker computes the highest applied SCN for every thread and totals the numbers. If there are multiple incarnations and the standby database is in a different incarnation from the primary database, each incarnation is computed separately and the results are then totaled.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Standby database %dg_name% has not applied the last %value% megabytes of data received.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.7.1.4 Data Not Received (logs)

The broker computes the highest applied system change number (SCN) and uses its value to find the last continuous log file that was successfully archived to the standby database. Redo data in all subsequent log files, including the current online redo log file, are counted as log files for potential data loss and will be unrecoverable if the primary database goes down at this point.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database, and if log 10 is the current online log file, and if log apply services are currently applying log 1, the last continuous log after the highest applied SCN is log 3. All log files after log 3, that is log files 4 through 10, are counted as data not received. If the primary database goes down at this point, all redo data in log files 4 through 10 are lost on the standby database.

If the primary database is multithreaded (in a RAC database), the broker computes the highest applied SCN for every thread and totals the numbers. If the primary database has multiple incarnations (for example, due to a flashback operation) and the standby database is in a different incarnation from the primary database, the computation is done on each incarnation and the results are then totaled.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every 5 Minutes	After Every Sample	>	1	3	1	Standby database %dg_name% has not received the last %value% logs from the primary database.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.7.1.5 Data Not Received (MB)

The broker computes the highest applied system change number (SCN) and uses its value to find the last continuous log file that was successfully archived to the standby database. The size of redo data in all subsequent log files, including the current online redo log file, are counted as data for potential data loss and will be unrecoverable if the primary database goes down at this point. The size of an archived log file is its file size, and the size of the online redo log file is the size of the actual redo in the online log file, not the file size of the online redo log file.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database, and if log 10 is the current online log file, and if log apply services is currently applying log 1, the last continuous log after the highest applied SCN is log 3. All log files after log 3, that is log files 4 through 10, are counted as data not received and the total size of redo data in these log files is the size of Data Not Received.

If the primary database is multithreaded (in a RAC database), the broker computes the highest applied SCN for every thread and totals the numbers. If the primary database has multiple incarnations (for example, due to a flashback operation) and the standby database is in a different incarnation from the primary database, the computation is done on each incarnation and the results are then totaled.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Standby database %dg_name% has not received the last %value% megabytes of data from the primary database.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.7.2 Data Guard (for 9*i*)

Data Guard for release 9*i* metrics monitor the overall status of the Data Guard configuration, including the primary and all standby databases.

4.7.2.1 Data Guard Status

Checks the status of each database in the broker configuration.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x	Every 5 Minutes	After Every Sample	CONTAINS	Warning	Error	1	The Data Guard status of %dg_name% is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.7.2.2 Data Not Applied (logs)

The broker computes the highest applied system change number (SCN) and uses its value to find the last continuous log that was successfully archived to the standby database. Redo data in all subsequent log files are counted as logs not applied. If the primary database goes down at this point, the redo data from these log files can be applied on the standby database. If there is a gap in the log files received on the standby database, any log files received after the gap cannot be applied.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database and log apply services is currently applying log 1, log apply services can continue to apply up to log 3. Log apply services cannot apply any more log files because log 4 is missing. Even though log files 6, 7, and 9 are received, they cannot be applied and they will not be counted as data not applied.

If all the archived log files on the standby database are continuous, and standby redo logs are used, the standby redo logs are also counted as data not applied, unless real-time apply is turned on and log apply services is already working on the standby redo log files.

If the standby redo logs are multithreaded, the broker computes the highest applied SCN for every thread and totals the numbers. If there are multiple incarnations and the standby database is in a different incarnation from the primary database, each incarnation is computed separately and the results are then totaled.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x	Every 5 Minutes	After Every Sample	>	1	3	1	Standby database %dg_name% has not applied the last %value% received logs.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.7.2.3 Data Not Received (logs)

The broker computes the highest applied system change number (SCN) and uses its value to find the last continuous log file that was successfully archived to the standby database. Redo data in all subsequent log files, including the current online redo log file, are counted as log files for potential data loss and will be unrecoverable if the primary database goes down at this point.

For example, if log files 1, 2, 3, 6, 7, and 9 are received on the standby database, and if log 10 is the current online log file, and if log apply services are currently applying log 1, the last continuous log after the highest applied SCN is log 3. All log files after log 3, that is log files 4 through 10, are counted as data not received. If the primary database goes down at this point, all redo data in log files 4 through 10 are lost on the standby database.

If the primary database is multithreaded (in a RAC database), the broker computes the highest applied SCN for every thread and totals the numbers. If the primary database has multiple incarnations (for example, due to a flashback operation) and the standby database is in a different incarnation from the primary database, the computation is done on each incarnation and the results are then totaled.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x	Every 5 Minutes	After Every Sample	>	1	3	1	Standby database %dg_name% has not received the last %value% logs from the primary database.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

No user action is required.

4.7.3 Data Guard Failover Metrics

The Data Guard Failover metrics generate a critical alert on the new primary database (old standby database) if a fast-start failover (FSFO) occurs. They will generate a warning alert on the new primary database if a user-directed (manual) failover occurs. The alert can be manually cleared. If not cleared, it will be cleared automatically after a variable period of time.

4.7.3.1 Failover Occurred

This metric shows the time when a failover occurred. The value is 0 if failover has not occurred, 1 if failover has occurred. This metric is available in Data Guard version 11.1.0.x and 11.2.0.x.

This metric generates an alert on the new primary database (old standby database) if a failover occurs. Both primary and standby databases must be configured with sysdba monitoring access.

Data Source

Not available

User Action

No user action is required.

4.7.4 Data Guard Fast-Start Failover Metrics

The Data Guard Fast-Start Failover metrics monitor the status of Data Guard fast-start failover.

4.7.4.1 Fast-Start Failover Occurred

When Fast-Start Failover (FSFO) is enabled, this metric will generate a critical alert on the new primary database (old standby) if an FSFO occurs. The FSFO SCN (system change number) must be initialized to a value before the metric will alert. This usually takes one collection interval. Once an FSFO occurs and the new primary is ready, the FSFO alert fires. It then clears after one collection interval. A critical alert is configured by default.

Both primary and standby must be configured with sysdba monitoring access.

Shows the time when a fast-start failover occurred.

The value is 0 if FSFO has not occurred, 1 if FSFO has occurred.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x	Every 5 Minutes	Not Uploaded	=	Not Defined	1	1	A fast-start failover occurred at %dg_ fs_time%.om the primary database.

Data Source

Not available

User Action

Access the Grid Control Data Guard overview page to examine the current state of the Data Guard configuration.

4.7.4.2 Fast-Start Failover SCN

This metric displays the SCN (system change number) at which the standby database became the primary.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x	Every 5 Minutes

Data Source

select STANDBY_BECAME_PRIMARY_SCN from v$database;

User Action

No user action is required.

4.7.4.3 Fast-Start Failover Status

This metric displays the current status of the fast-start failover feature.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x	Every 5 Minutes

Data Source

select FS_FAILOVER_STATUS from v$database;

User Action

No user action is required.

4.7.4.4 Fast-Start Failover Time

This metric displays the time of the last fast-start failover.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x	Every 5 Minutes

Data Source

Not available

User Action

No user action is required.

4.7.5 Data Guard Fast-Start Failover Observer - 11*g* Metrics

The Data Guard Fast-Start Failover Observer metrics for 11*g* monitors the state of the fast-start failover observer.

4.7.5.1 Observer Status

This metric generates a critical alert on the primary database if the fast-start failover (FSFO) configuration is in an unobserved condition, indicating that FSFO is not currently possible.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every Minute	Not Uploaded	CONTAINS	Not Defined	Error	1	The Data Guard fast-start failover observer status is %value%.

Data Source

Not available

User Action

If the Data Guard configuration was configured in Grid Control to use the automatic Observer restart feature, the alert will clear once a new observer process is restarted. Otherwise, determine the cause of the unobserved condition, and restart the Observer process if necessary.

4.7.6 Data Guard Fast-Start Failover Observer Metrics

The Data Guard Fast-Start Failover Observer metrics monitors the state of the fast-start failover observer.

4.7.6.1 Observer Status

This metric generates a critical alert on the primary database if the fast-start failover (FSFO) configuration is in an unobserved condition, indicating that FSFO is not currently possible.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x	Every 5 Minutes	Not Uploaded	CONTAINS	Not Defined	Error	1	The Data Guard fast-start failover observer status is %value%.

Data Source

Not available

User Action

If the Data Guard configuration was configured in Grid Control to use the automatic Observer restart feature, the alert will clear once a new observer process is restarted. Otherwise, determine the cause of the unobserved condition, and restart the Observer process if necessary.

4.7.7 Data Guard Performance (sperf) Metrics

The Data Guard Performance (sperf) metrics monitor standby database performance.

4.7.7.1 Apply Lag (seconds)

This metric displays (in seconds) how far the standby is behind the primary database. This metric will generate an alert on the standby database if it falls behind more than the user-specified threshold (if any). Displays (in seconds) how far the standby is behind the primary.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The standby database is approximately %value% seconds behind the primary database.

Data Source

v$dataguard_stats

User Action

No user action is required.

4.7.7.2 Estimated Failover Time (seconds)

The approximate number of seconds it would require to failover to this standby database.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The estimated time to failover is approximately %value% seconds.

Data Source

v$dataguard_stats

User Action

No user action is required.

4.7.7.3 Redo Apply Rate (KB/second)

This metric display the redo apply rate in KB/second on this standby database.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The redo apply rate is %value% KB/sec.

Data Source

Not available

User Action

No user action is required.

4.7.7.4 Transport Lag (seconds)

The metric represents the approximate number of seconds of redo not yet available on this standby database. This may be because the redo has not yet been shipped or there may be a gap. This metric will generate an alert on the standby database if it falls behind more than the user-specified threshold (if any).

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The are approximately %value% seconds of redo not yet available on this standby databse.

Data Source

v$dataguard_stats

User Action

No user action is required.

4.7.8 Data Guard Performance (sperf 112) Metrics

The Data Guard Performance (sperf_112) metrics monitor standby database performance for databases 11.2 and higher.

4.7.8.1 Apply Lag (seconds)

This metric displays (in seconds) how far the standby is behind the primary database. This metric will generate an alert on the standby database if it falls behind more than the user-specified threshold (if any). Displays (in seconds) how far the standby is behind the primary.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The standby database is approximately %value% seconds behind the primary database.

Data Source

v$dataguard_stats

User Action

No user action is required.

4.7.8.2 Apply Lag Data Refresh Time

This metric represents the local time at the standby database when the data used to compute the apply lag was received from the primary database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The standby database is approximately %value% seconds behind the primary database.

Data Source

v$dataguard_stats

User Action

No user action is required.

4.7.8.3 Estimated Failover Time (seconds)

The approximate number of seconds it would require to failover to this standby database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The estimated time to failover is approximately %value% seconds.

Data Source

v$dataguard_stats

User Action

No user action is required.

4.7.8.4 Redo Apply Rate (KB/second)

This metric display the redo apply rate in KB/second on this standby database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The redo apply rate is %value% KB/sec.

Data Source

Not available

User Action

No user action is required.

4.7.8.5 Transport Lag (seconds)

The metric represents the approximate number of seconds of redo not yet available on this standby database. This may be because the redo has not yet been shipped or there may be a gap. This metric will generate an alert on the standby database if it falls behind more than the user-specified threshold (if any).

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The are approximately %value% seconds of redo not yet available on this standby databse.

Data Source

v$dataguard_stats

User Action

No user action is required.

4.7.8.6 Transport Lag Data Refresh Time

The metric represents the local time at the standby database when the data used to compute the transport lag was received from the primary database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The are approximately %value% seconds of redo not yet available on this standby databse.

Data Source

v$dataguard_stats

User Action

No user action is required.

4.7.9 Data Guard Performance (pperf) Metrics

The Data Guard Performance (pperf) metrics monitor the primary database redo generation rate.

4.7.9.1 Redo Generation Rate (KB/second)

This metric monitors the primary database rego generation rate.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	The redo generation rate is %value% KB/sec.

Data Source

Not available

User Action

No user action is required.

4.7.10 Data Guard Status Metrics

The Data Guard metrics monitor the status of the databases in the Data Guard configuration.

For information about Data Guard metrics, see the "Managing Data Guard Metrics" section of the *Oracle10i Data Guard Broker* book.

4.7.10.1 Data Guard Status

Use the Data Guard Status metric to check the status of each database in the Data Guard configuration.

By default, a critical and warning threshold value was set for this metric column. Alerts will be generated when threshold values are reached. You can edit the value for a threshold as required.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	CONTAINS	Warning	Error	1	The Data Guard status of %dg_ name% is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Name" object.

If warning or critical threshold values are currently set for any "Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

Perform the following steps:

1. Go to the Grid Control Data Guard overview pagae to obtain more information on a warning or error status in the Data Guard configuration.
2. Examine the database alert logs and the Data Guard broker logs for additional information.

For information about Data Guard metrics, see the "Managing Data Guard Metrics" section of the *Oracle10i Data Guard Broker* book.

4.8 Database Metrics

Database metrics are made up of the following:

- Section 4.8.1, "Database Files Metrics"
- Section 4.8.2, "Database Job Status Metrics"
- Section 4.8.3, "Database Limits Metrics"
- Section 4.8.4, "Database Replay Metrics"
- Section 4.8.5, "Database Replay Client Metrics"
- Section 4.8.6, "Database Services Metrics"
- Section 4.8.7, "Database Vault Metrics"

4.8.1 Database Files Metrics

Database Files metrics represent the average file read time and average file write time for the database files.

4.8.1.1 Average File Read Time (centi-seconds)

This metric represents the average file read time, measured in hundredths of a second.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 10 Minutes	Not Defined	After Every Sample	>	Not Defined	Not Defined	1	Generated By Database Server

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "File Name" object.

If warning or critical threshold values are currently set for any "File Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "File Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.8.1.2 Average File Write Time (centi-seconds)

This metric represents the average file write time, measured in hundredths of a second.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 10 Minutes	Not Defined	After Every Sample	>	Not Defined	Not Defined	1	Generated By Database Server

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "File Name" object.

If warning or critical threshold values are currently set for any "File Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "File Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.8.2 Database Job Status Metrics

The Database Job Status metrics represent the health of database jobs registered through the DBMS_JOB interface.

4.8.2.1 Broken Job Count

The Oracle Server job queue is a database table that stores information about local jobs such as the PL/SQL call to execute for a job such as when to run a job. Database replication is also managed by using the Oracle job queue mechanism using jobs to push deferred transactions to remote master sites, to purge applied transactions from the deferred transaction queue or to refresh snapshot refresh groups.

A job can be broken in two ways:

- Oracle has failed to successfully execute the job after sixteen attempts.
- The job has been explicitly marked as broken by using the procedure DBMS_JOB.BROKEN.

This metric checks for broken DBMS jobs. A critical alert is generated if the number of broken jobs exceeds the value specified by the threshold argument.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	Not Uploaded	>	0	Not Defined	1	%value% job(s) are broken.

Data Source

```
SELECT COUNT(*)
  FROM dba_jobs
  WHERE broken [less] [greater] 'N'
```

User Action

Check the ALERT log and trace files for error information. Correct the problem that is preventing the job from running. Force immediate re-execution of the job by calling DBMS_JOB.RUN.

4.8.2.2 Failed Job Count

The Oracle Server job queue is a database table that stores information about local jobs such as the PL/SQL call to execute for a job such as when to run a job. Database replication is also managed by using the Oracle job queue mechanism using jobs to push deferred transactions to remote master sites, to purge applied transactions from the deferred transaction queue or to refresh snapshot refresh groups.

If a job returns an error while Oracle is attempting to execute it, the job fails. Oracle repeatedly tries to execute the job doubling the interval of each attempt. If the job fails sixteen times, Oracle automatically marks the job as broken and no longer tries to execute it.

This metric checks for failed DBMS jobs. An alert is generated if the number of failed job exceeds the value specified by the threshold argument.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	Not Uploaded	>	0	Not Defined	1	%value% job(s) are broken.

Data Source

```
SELECT COUNT(*)
  FROM dba_jobs
  WHERE NVL(failures, 0) <  > 0
```

User Action

Check the ALERT log and trace files for error information. Correct the problem that is preventing the job from running.

4.8.3 Database Limits Metrics

Database Limits metrics represent the percentage of resource limitations at which the Oracle Server is operating.

4.8.3.1 Current Logons Count

This metric represents the current number of logons.

Note: Unlike most metrics, which accept thresholds as real numbers, this metric can only accept an integer as a threshold.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	3	Generated By Database Server

Data Source

logons current

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.8.3.2 Current Open Cursors Count

This metric represents the current number of opened cursors.

Note: Unlike most metrics, which accept thresholds as real numbers, this metric can only accept an integer as a threshold.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	1200	Not Defined	3	Generated By Database Server

Data Source

opened cursors current

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.8.3.3 Lock Limit Usage (%)

The DML_LOCKS initialization parameter specifies the maximum number of DML locks. The purpose of DML locks is to guarantee the integrity of data being accessed concurrently by multiple users. DML locks prevent destructive interference of simultaneous conflicting DML and/or DDL operations.

This metric checks for the utilization of the lock resource against the values (percentage) specified by the threshold arguments. If the percentage of all active DML locks to the limit set in the DML_LOCKS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated.

If DML_LOCKS is 0, this test fails to register. A value of 0 indicates that enqueues are disabled.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 15 Minutes	After Every Sample	>	80	Not Defined	3	%target% has reached %value%% of the lock limit.

Data Source

```
SELECT resource_name name,
  100*DECODE(initial_allocation, ' UNLIMITED', 0, current_utilization /
  initial_allocation) usage
FROM v$resource_limit
WHERE LTRIM(limit_value)
  != '0' AND LTRIM(initial_allocation) != '0' AND resource_name = 'dml_locks'
```

User Action

Increase the DML_LOCKS instance parameter by 10%.

4.8.3.4 Process Limit Usage (%)

The PROCESSES initialization parameter specifies the maximum number of operating system user processes that can simultaneously connect to a database at the same time. This number also includes background processes utilized by the instance.

This metric checks for the utilization of the process resource against the values (percentage) specified by the threshold arguments. If the percentage of all current processes to the limit set in the PROCESSES initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	3	%target% has reached %value%% of the process limit.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	3	Generated By Database Server

Data Source

```
SELECT resource_name name,
  100*DECODE(initial_allocation, ' UNLIMITED', 0, current_utilization) != '0'
  AND resource_name = 'processes'
```

User Action

Verify that the current PROCESSES instance parameter setting has not exceeded the operating system-dependent maximum. Increase the number of processes to be at least 6 + the maximum number of concurrent users expected to log in to the instance.

4.8.3.5 Session Limit Usage (%)

The SESSIONS initialization parameter specifies the maximum number of concurrent connections that the database will allow.

This metric checks for the utilization of the session resource against the values (percentage) specified by the threshold arguments. If the percentage of the number of sessions, including background processes, to the limit set in the SESSIONS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 15 Minutes	After Every Sample	>	90	97	3	%target% has reached %value%% of the session limit.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	90	97	3	Generated By Database Server

Data Source

```
SELECT resource_name name,
  100*DECODE(initial_allocation, ' UNLIMITED', 0, current_utilization) != '0'
  AND resource_name = 'sessions'
```

User Action

Increase the SESSIONS instance parameter. For XA environments, confirm that SESSIONS is at least 2.73 * PROCESSES. For shared server environments, confirm that SESSIONS is at least 1.1 * maximum number of connections.

4.8.3.6 User Limit Usage (%)

The LICENSE_MAX_SESSIONS initialization parameter specifies the maximum number of concurrent user sessions allowed simultaneously.

This metric checks whether the number of users logged on is reaching the license limit. If the percentage of the number of concurrent user sessions to the limit set in the LICENSE_MAX_SESSIONS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated. If LICENSE_MAX_SESSIONS is not explicitly set to a value, the test does not trigger.

Note: This metric is most useful when session licensing is enabled. Refer to the *Oracle Server Reference Manual* for more information on LICENSE_MAX_SESSIONS and LICENSE_MAX_USERS.

Note: Unlike most metrics, which accept thresholds as real numbers, this metric can only accept an integer as a threshold.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	3	%target% has reached %value%%% of the user limit.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	3	Generated By Database Server

Data Source

```
SELECT 'user' name,
  100*DECODE(session_max, 0, 0, sessions_current/session_max) usage
  FROM v$license
```

User Action

This typically indicates that the license limit for the database has been reached. The user will need to acquire additional licenses, then increase LICENSE_MAX_ SESSIONS to reflect the new value.

4.8.4 Database Replay Metrics

This metric shows the current status (on/off) of database workload capture and replay.

4.8.4.1 Workload Capture Status

This metric shows if database workload capture is in progress.

Metric Summary for Database Control and Grid Control

This metric is available for Oracle Database 11*g* Release 2.

Data Source

Server-generated alert triggered by the target database when a capture is started.

User Action

No user action is required.

4.8.4.2 Workload Replay Status

This metric shows if database workload replay is in progress.

Metric Summary for Database Control and Grid Control

This metric is available for Oracle Database 11*g* Release 2.

Data Source

Server-generated alert triggered by the target database when a replay is started.

User Action

No user action is required.

4.8.5 Database Replay Client Metrics

These metrics show the resource usage of the replay clients during database workload replay.

4.8.5.1 Average I/O Latency (milliseconds)

This metric reflects the average response time for a single I/O for a database replay client.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	null

Data Source

Server-generated alert triggered by the target database when an alarming condition is detected in a replay client.

User Action

Run the calibrate utility of the replay client and restart a replay with the suggested number of replay clients, distributed between machines with the necessary capacity.

4.8.5.2 Replay Threads (%) Performing I/O

This metric represents the number of replay client connections performing I/O operation concurrently.

Metric Summary for Database Control and Grid Control

The rest of the information in this section is only valid for this metric when it appears in either the Enterprise Manager Grid Control or the Enterprise Manager Database Control (if applicable).

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	null

Data Source

Server-generated alert triggered by the target database when an alarming condition is detected in a replay client.

User Action

Run the calibrate utility of the replay client and restart a replay with the suggested number of replay clients, distributed between machines with the necessary capacity.

4.8.5.3 Replay Threads (%) Using CPU

This metric represents the number of replay client connections using the CPU concurrently.

Metric Summary for Database Control and Grid Control

The rest of the information in this section is only valid for this metric when it appears in either the Enterprise Manager Grid Control or the Enterprise Manager Database Control (if applicable).

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	null

Data Source

Server-generated alert triggered by the target database when an alarming condition is detected in a replay client.

User Action

Run the calibrate utility of the replay client and restart a replay with the suggested number of replay clients, distributed between machines with the necessary capacity.

4.8.6 Database Services Metrics

The Database Services metrics include the service CPU time and service rresponse time.

4.8.6.1 Service CPU Time (per user call) (microseconds)

This metric represents the average CPU time, in microseconds, for calls to a particular database service.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	1	Generated By Database Server

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Service Name" object.

If warning or critical threshold values are currently set for any "Service Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Service Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.8.6.2 Service Response Time (per user call) (microseconds)

This metric represents the average elapsed time, in microseconds, for calls to a particular database service.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	1	Generated By Database Server

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Service Name" object.

If warning or critical threshold values are currently set for any "Service Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Service Name" object, use the Edit Thresholds page.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.8.7 Database Vault Metrics

The Database Vault metrics include the following:

4.8.7.1 Database Vault Attempted Violations - Command Rules

This metric is used to enable Database Vault Security Analyst to keep a watch on the violation attempts against the Database Vault database. Database Vault Security Analyst can pick the command rules he would like to get alerted on and even further filter them based on the different types of attempts by using error codes. This metric is not enabled out of the box; the user needs to enable it from Metrics and Policy Settings page. By default, this metric is collected every 1 hour, but the user can set his own collection frequency.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour	Not Uploaded	MATCH	Not Defined	Not Defined	1[1]	%ACTION_ OBJECT_NAME% got violated at %VIOLATIONTIM ESTAMP%

[1] Once an alert is triggered for this metric, it must be manually cleared

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Database Vault Command Rule " and "Violation Time" objects.

If warning or critical threshold values are currently set for any unique combination of "Database Vault Command Rule " and "Violation Time" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Database Vault Command Rule " and "Violation Time" objects, use the Edit Thresholds page.

Data Source

The attempted violations are picked up from the target's database vault audit trail. Only audit entries related to command rule, which represent failed attempts to execute a SQL, are selected.

User Action

To know more about the violations, for example, the command that was violated, which database user triggered the violation, what action trigged this violation, and at what time this violation happened, login to the target's Database Vault Home Page and use the Attempted Violations charts.

4.8.7.2 Database Vault Attempted Violations - Realms

This metric is used to enable Database Vault Security Analyst to keep a watch on the violation attempts against the Database Vault database. Database Vault Security Analyst can pick the realms he would like to get alerted on and even further filter them based on the different types of attempts by using error codes. This metric is not enabled out of the box; the user needs to enable it from Metrics and Policy Settings page. By default, this metric is collected every 1 hour, but the user can set his own collection frequency.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour	Not Uploaded	MATCH	Not Defined	Not Defined	1[1]	%ACTION_ OBJECT_NAME% got violated at %VIOLATIONTIM ESTAMP%

[1] Once an alert is triggered for this metric, it must be manually cleared

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Database Vault Realm " and "Violation Time" objects.

If warning or critical threshold values are currently set for any unique combination of "Database Vault Realm " and "Violation Time" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Database Vault Realm " and "Violation Time" objects, use the Edit Thresholds page.

Data Source

The attempted violations are picked up from the target's Database Vault audit trail. Only audit entries related to realms, which represent failed attempts to execute a SQL, are selected.

User Action

To know more about the violations, for example, the realm that was violated, which database user triggered the violation, what action trigged this violation, and at what time this violation happened, login to the target's Database Vault Home Page and use the Attempted Violations charts.

4.8.7.3 Database Vault Configuration Issues Count - Command Rules

Once the Database Vault policies are defined and configured to protect the database, further user actions over the course of time can disturb these configurations. This metric tracks the users' actions and raises an alert when there is a misconfiguration on a Command Rule that needs administrator attention. This metric is enabled out of the box. By default this metric is collected every 1 hour, but the user can set his own collection frequency.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour	After Every Sample	>	Not Defined	0	1	%ACTION_ OBJECT_NAME% has configuration issues.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Database Vault Command Rule " object.

If warning or critical threshold values are currently set for any "Database Vault Command Rule " object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Database Vault Command Rule " object, use the Edit Thresholds page.

Data Source

The configuration issues are picked from scanning the realm and command rule definitions.

User Action

To know the cause of the command rule misconfiguration, navigate to the target's Database Vault Home page, launch Database Vault Administrator, and view the Database Vault Configuration Issues Reports. These alerts are automatically cleared when the configuration issue is resolved.

4.8.7.4 Database Vault Configuration Issues Count - Realms

Once the Database Vault policies are defined and configured to protect the database, further user actions over the course of time can disturb these configurations. This metric tracks the users' actions and raises an alert when there is a misconfiguration on a Realm that needs administrator attention. This metric is enabled out of the box. By default this metric is collected every 1 hour, but the user can set his own collection frequency.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour	After Every Sample	>	Not Defined	0	1	%ACTION_ OBJECT_NAME% has configuration issues.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Database Vault Realm " object.

If warning or critical threshold values are currently set for any "Database Vault Realm " object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Database Vault Realm " object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

Data Source

The configuration issues are picked from scanning the realm and ruleset definitions.

User Action

To know the cause of the realm misconfiguration, navigate to the target's Database Vault Home page, launch Database Vault Administrator, and view the Database Vault Configuration Issues Reports. These alerts are automatically cleared when the configuration issue is resolved.

4.8.7.5 Database Vault Policy Changes Count

After the Database Vault policies are defined, further changes to it is tracked by this metric. On any changes to the Database Vault policies, this metric will raise an alert. This metric is enabled out of the box. By default this metric is collected every 1 hour, but the user can set his own collection frequency.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Hour	After Every Sample	>	Not Defined	0	1[1]	%POLICY_ CATEGORY_ NAMES% has Policy changes

[1] Once an alert is triggered for this metric, it must be manually cleared

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "DV Policy Change Category" and "DV Policy Change Time" objects.

If warning or critical threshold values are currently set for any unique combination of "DV Policy Change Category" and "DV Policy Change Time" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "DV Policy Change Category" and "DV Policy Change Time" objects, use the Edit

Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

The policy changes are picked up from scanning the records in the Database Audit Trail related to Database Vault Schemas.

User Action

To know more about the policy changes, for example which object was changed, which database user changed the policy, what was the user action, and at what time this policy was changed, login to the target's Database Vault Home Page and view the Policy Changes Report.

4.8.8 DB Managed by Single Instance

This metric collects the configuration information for an Oracle Database for Single Instance High Availability (HA) registration.

4.8.8.1 CRS Home Directory

Oracle Home directory if a Single Instance HA is installed on the machine.

4.8.8.2 DB Managed by Single Instance HA

Indicates if the Database is managed by Single Instance HA. If the Oracle Database is not managed by Single Instance HA, indicates if a Single Instance HA is available for Oracle Database registration.

4.9 Deferred Transactions Metrics

The Deferred Transactions metrics are associated with this distributed database's deferred transactions.

4.9.1 Deferred Transaction Count

Oracle uses deferred transactions to propagate data-level changes asynchronously among master sites in an advanced replication system as well as from an updatable snapshot to its master table.

This metric checks for the number of deferred transactions. An alert is generated if the number of deferred transactions exceeds the value specified by the threshold argument.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	Not Uploaded	>	100	Not Defined	3	Number of deferred transactions is %value%.

Data Source

```
SELECT count(*) FROM sys.deftran
```

User Action

When the advanced replication facility pushes a deferred transaction to a remote site, it uses a distributed transaction to ensure that the transaction has been properly committed at the remote site before the transaction is removed for the queue at the local site. If transactions are not being pushed to a given remote site, verify that the destination for the transaction was correctly specified. If you specify a destination database when calling DBMS_DEFER_SYS.SCHEDULE_EXECUTION using the DBLINK parameter or DBMS_DEFER_SYS.EXECUTE using the DESTINATION parameter, make sure the full database link is provided.

Wrong view destinations can lead to erroneous deferred transaction behavior. Verify the DEFCALLEST and DEFTRANDEST views are the definitions from the CATREPC.SQL not the ones from CATDEFER.SQL.

4.9.2 Deferred Transaction Error Count

Oracle uses deferred transactions to propagate data-level changes asynchronously among master sites in an advanced replication system as well as from an updatable snapshot to its master table. If a transaction is not successfully propagated to the remote site, Oracle rolls back the transaction, logs the transaction in the SYS.DEFERROR view in the remote destination database.

This metric checks for the number of transactions in SYS.DEFERROR view and raises an alert if it exceeds the value specified by the threshold argument.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	Not Uploaded	>	0	Not Defined	3	Number of deferred transactions with errors is %value%.

Data Source

```
SELECT count(*) FROM sys.deferror
```

User Action

An error in applying a deferred transaction may be the result of a database problem, such as a lack of available space in the table is to be updated or may be the result of an unresolved insert, update or delete conflict. The SYS.DEFERROR view provides the ID of the transaction that could not be applied. Use this ID to locate the queued calls associated with the transaction. These calls are stored in the SYS.DEFCALL view. You can use the procedures in the DBMS_DEFER_QUERY package to determine the arguments to the procedures listed in the SYS.DEFCALL view.

4.10 Dump Area Metrics

The Dump Area metrics check for the percentage of used space of the dump destination devices.

4.10.1 Dump Area Directory

This metric is the directory represented by this metric index's dump destination.

Each server and background process can write to an associated trace file to log messages and errors.

Background processes and the ALERT file are written to the destination specified by BACKGROUND_DUMP_DEST. Trace files for server processes are written to the destination specified by USER_ DUMP_DEST.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

data from v$parameter

User Action

Verify the device specified in the initialization parameters BACKGROUND_DUMP_ DEST, USER_DUMP_DEST, and CORE_DUMP_DEST are set up properly for archiving.

If the BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST initialization parameters are set up correctly and this metric triggers, then free up more space in the destination specified by the dump destination parameters.

4.10.2 Dump Area Used (%)

This metric returns the percentage of used space of the dump area destinations.

If the space used is more than the threshold value given in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 15 Minutes	After Every Sample	>	95	Not Defined	1	%value%% of %dumpType% dump area is used.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Type of Dump Area" object.

If warning or critical threshold values are currently set for any "Type of Dump Area" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Type of Dump Area" object, use the Edit Thresholds page.

Data Source

Calculated using the UNIX `df -k` command.

- Critical threshold: Percentage of free space threshold for critical alert.
- Warning threshold: Percentage of free space threshold for warning alert.

User Action

Verify the device specified in the initialization parameters BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST are set up properly for archiving.

If the BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST initialization parameters are set up correctly and this metric triggers, then free up more space in the destination specified by the dump destination parameters.

4.10.3 Dump Area Used (KB)

This metric represents the total space used (in KB) on the device containing the dump destination directory.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

Calculated using the UNIX `df -k` command.

User Action

Verify the device specified in the initialization parameters BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST are set up properly for archiving.

If the BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST initialization parameters are set up correctly and this metric triggers, then free up more space in the destination specified by the dump destination parameters

4.10.4 Free Dump Area (KB)

Each server and background process can write to an associated trace file in order to log messages and errors. Background processes and the ALERT file are written to the destination specified by BACKGROUND_DUMP_DEST.

Trace files for server processes are written to the destination specified by USER_DUMP_DEST.

This metric checks for available free space on these dump destination devices. If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 15 Minutes	After Every Sample	<	2000	Not Defined	1	%value%%% free KB remains in %dumpType% dump area.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Type of Dump Area" object.

If warning or critical threshold values are currently set for any "Type of Dump Area" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Type of Dump Area" object, use the Edit Thresholds page.

Data Source

Calculated using the UNIX `df -k` command.

User Action

Verify the device specified in the initialization parameters BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST are set up properly for archiving.

If the BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST initialization parameters are set up correctly and this metric triggers, then free up more space in the destination specified by the dump destination parameters

4.10.5 Total Dump Area (KB)

This metric represents the total space (in KB) available on the device containing the dump destination directory.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

Calculated using the UNIX `df -k` command.

User Action

Verify the device specified in the initialization parameters BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST are set up properly for archiving.

If the BACKGROUND_DUMP_DEST, USER_DUMP_DEST, and CORE_DUMP_DEST initialization parameters are set up correctly and this metric triggers, then free up more space in the destination specified by the dump destination parameters.

4.11 Efficiency Metrics

This metric category contains the metrics that have traditionally been considered to represent the efficiency of some resource. Interpreting the wait interface is generally accepted as a much more accurate approach to measuring efficiency, and is recommended as an alternative to these hit ratios.

4.11.1 Buffer Cache Hit (%)

This metric represents the data block buffer cache efficiency, as measured by the percentage of times the data block requested by the query is in memory.

Effective use of the buffer cache can greatly reduce the I/O load on the database. If the buffer cache is too small, frequently accessed data will be flushed from the buffer cache too quickly which forces the information to be re-fetched from disk. Since disk access is much slower than memory access, application performance will suffer. In addition, the extra burden imposed on the I/O subsystem could introduce a bottleneck at one or more devices that would further degrade performance.

This test checks the percentage of buffer requests that were already in buffer cache. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Buffer cache hit ratio is %value%%%.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

((DeltaLogicalGets - (DeltaPhysicalReads - DeltaPhysicalReadsDirect)) / DeltaLogicalGets) * 100 where:

- DeltaLogicalGets: difference in 'select value from v$sysstat where name='session logical reads'' between sample end and start
- DeltaPhysicalReads: difference in 'select value from v$sysstat where name='physical reads'' between sample end and start
- DeltaPhysicalReadsDirect: difference in 'select value from v$sysstat where name='physical reads direct'' between sample end and start (Oracle8*i*)

User Action

A low buffer cache hit ratio means that the server must often go to disk to retrieve the buffers required to satisfy a query. The queries that perform the most physical reads lower the numerical value of this statistic. Typically queries that perform full table scans force large amounts of buffers into the cache, aging out other buffers that may be required by other queries later. The Top Sessions page sorted by Physical Reads will show the sessions performing the most reads and through further drilldown their associated queries can be identified. Similarly, the Top SQL page sorted by Physical Reads shows which SQL statements are performing the most physical reads. The statements performing the most I/O should be looked at for tuning.

The difference between the two is that the Top Sessions chart shows the sessions that are responsible for the physical reads at any given moment. The Top SQL view shows all SQL that is still in the cache. The top statement may not be executing currently, and thus not responsible for the current poor buffer cache hit ratio.

If the queries seem to be well tuned, the size of the buffer cache also determines how often buffers need to be fetched from disk. The DB_BLOCK_BUFFERS initialization parameter determines the number of database buffers available in the buffer cache. It is one of the primary parameters that contribute to the total memory requirements of the SGA on the instance. The DB_BLOCK_BUFFERS parameter, together with the DB_BLOCK_SIZE parameter, controls the total size of the buffer cache. Since DB_BLOCK_SIZE can only be specified when the database is first created, normally the size of the buffer cache size is controlled using the DB_BLOCK_BUFFERS parameter.

Consider increasing the DB_BLOCK_BUFFERS initialization parameter to increase the size of the buffer cache. This increase allows the Oracle Server to keep more

information in memory, thus reducing the number of I/O operations required to do an equivalent amount of work using the current cache size.

4.11.2 CPU Usage (per second)

This metric represents the CPU usage per second by the database processes, measured in hundredths of a second. A change in the metric value may occur because of a change in either workload mix or workload throughput being performed by the database. Although there is no *correct* value for this metric, it can be used to detect a change in the operation of a system. For example, an increase in Database CPU usage from 500 to 750 indicates that the database is using 50% more CPU. (*No correct value* means that there is no single value that can be applied to any database. The value is a characteristic of the system and the applications running on the system.)

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. ADDM can help to identify database operations that are consuming CPU. ADDM reports are available from a number of locations including the Database Home page and Advisor Central.

4.11.3 CPU Usage (per transaction)

This metric represents the average CPU usage per transaction expressed as a number of seconds of CPU time. A change in this metric can occur either because of changing workload on the system, such as the addition of a new module, or because of a change in the way that the workload is performed in the database, such as changes in the plan for a SQL statement. The threshold for this metric should be set based on the actual values observed on your system.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. ADDM will provide information about which operations are using the CPU resources.

4.11.4 Cursor Cache Hit (%)

This metric represents the percentage of soft parses satisfied within the session cursor cache.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

```
session cursor cache hits / (parse count (total) - parse count (hard))
```

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.5 Data Dictionary Hit (%)

This metric represents dictionary cache efficiency as measured by the percentage of requests against the dictionary data that were already in memory. It is important to determine whether the misses on the data dictionary are actually affecting the performance of the Oracle Server. The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache, and the other cache structures that are specific to a particular instance configuration.

Misses on the data dictionary cache are to be expected in some cases. Upon instance startup, the data dictionary cache contains no data, so any SQL statement issued is likely to result in cache misses. As more data is read into the cache, the likelihood of cache misses should decrease. Eventually the database should reach a steady state in which the most frequently used dictionary data is in the cache. At this point, very few cache misses should occur. To tune the cache, examine its activity only after your application has been running.

This test checks the percentage of requests against the data dictionary that were found in the Shared Pool. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Data dictionary hit ratio is %value%%.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

(Gets/Misses) * 100 where:

- Misses: select sum(getmisses) from v$rowcache
- Gets: select sum(gets) from v$rowcache

User Action

If the percentage of gets is below 90% to 85%, consider increasing SHARED_POOL_ SIZE to decrease the frequency in which dictionary data is being flushed from the shared pool to make room for new data. To increase the memory available to the cache, increase the value of the initialization parameter SHARED_POOL_SIZE.

4.11.6 Database CPU Time (%)

This metric represents the percentage of database call time that is spent on the CPU. Although there is no *correct* value for this metric, it can be used to detect a change in the operation of a system, for example, a drop in Database CPU time from 50% to 25%. (*No correct value* means that there is no single value that can be applied to any

database. The value is a characteristic of the system and the applications running on the system.)

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

Not available

User Action

Investigate the change is CPU usage by using Automatic Database Diagnostic Monitor (ADDM). ADDM reports are available from a number of locations including the Database Home page and Advisor Central. Examine the report for increased time spent in wait events.

4.11.7 Library Cache Hit (%)

This metric represents the library cache efficiency, as measured by the percentage of times the fully parsed or compiled representation of PL/SQL blocks and SQL statements are already in memory.

The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache and the other cache structures that are specific to a particular instance configuration.

The shared pool mechanism can greatly reduce system resource consumption in at least three ways: Parse time is avoided if the SQL statement is already in the shared pool.

Application memory overhead is reduced, since all applications use the same pool of shared SQL statements and dictionary resources.

I/O resources are saved, since dictionary elements that are in the shared pool do not require access.

If the shared pool is too small, users will consume additional resources to complete a database operation. For library cache access, the overhead is primarily the additional CPU resources required to re-parse the SQL statement.

This test checks the percentage of parse requests where cursor already in cache If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Library cache hit ratio is %value%%%.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

(DeltaPinHits / DeltaPins) * 100 where:

- DeltaPinHits: difference in 'select sum(pinhits) from v$librarycache' between sample end and start
- DeltaPins: difference in 'select sum(pins) from v$librarycache' between sample end and start

User Action

The Top Sessions page sorted by Hard Parses lists the sessions incurring the most hard parses. Hard parses occur when the server parses a query and cannot find an exact match for the query in the library cache. You can avoid hard parses by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this page can identify the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements that can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

4.11.8 Library Cache Miss (%)

This metric represents the percentage of parse requests where the cursor is not in the cache.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

```
1 - pinhits / pins
```

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.9 Parallel Execution Downgraded (per second)

This metric represents the number of times per second parallel execution was requested and the degree of parallelism was reduced because of insufficient parallel execution servers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

```
(parallel operations downgraded 1 to 25 percent
+ parallel operations downgraded 25 to 50 percent
+ parallel operations downgraded 50 to 75 percent
+ parallel operations downgraded 75 to 99 percent)
/ time
```

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.10 Parallel Execution Downgraded 25% or more (per second)

Number of times per second parallel execution was requested and the degree of parallelism was reduced to 25% and more because of insufficient parallel execution servers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

```
(parallel operations downgraded 25 to 50 percent
+ parallel operations downgraded 50 to 75 percent
+ parallel operations downgraded 75 to 99 percent)
/ time
```

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.11 Parallel Execution Downgraded 50% or more (per second)

Number of times per second parallel execution was requested and the degree of parallelism was reduced to 50% and more because of insufficient parallel execution servers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

```
(parallel operations downgraded 50 to 75 percent
+ parallel operations downgraded 75 to 99 percent)
/ time
```

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.12 Parallel Execution Downgraded 75% or more (per second)

Number of times per second parallel execution was requested and the degree of parallelism was reduced to 75% or more because of insufficient parallel execution servers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

```
(parallel operations downgraded 75 to 99 percent) / time
```

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.13 Parallel Execution Downgraded to Serial (per second)

Number of times per second parallel execution was requested but execution was serial because of insufficient parallel execution servers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

parallel operations downgraded to serial / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.14 Parallel Execution Downgraded to Serial (per transaction)

Number of times per transaction parallel execution was requested but execution was serial because of insufficient parallel execution servers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Data Source

parallel operations downgraded to serial / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.15 PGA Cache Hit (%)

This metric represents the total number of bytes processed in the PGA versus the total number of bytes processed plus extra bytes read/written in extra passes.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.16 Redo Log Allocation Hit (%)

Redo log entries contain a record of changes that have been made to the database block buffers. The log writer (LGWR) process writes redo log entries from the log buffer to a redo log file. The log buffer should be sized so that space is available in the log buffer for new entries, even when access to the redo log is heavy. When the log buffer is undersized, user process will be delayed as they wait for the LGWR to free space in the redo log buffer.

The redo log buffer efficiency, as measured by the hit ratio, records the percentage of times users did not have to wait for the log writer to free space in the redo log buffer.

This metric monitors the redo log buffer hit ratio (percentage of success) against the values specified by the threshold arguments. If the number of occurrences is smaller than the values specified, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Buffer cache hit ratio is %value%%.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

```
100 * (redo_entries_delta - redo_space_requests_delta)
/redo_entries_delta
where:
```

- redo_enties_delta = difference between "SELECT value FROM v$sysstat WHERE name = 'redo entries'" at the beginning and ending of the interval
- redo_space_requests_delta = difference between "SELECT value FROM v$sysstat WHERE name = 'redo log space requests'" at the beginning and ending of the interval

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when buffering redo entries to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter in order to increase the size of the redo log buffer. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

Note: For Oracle Management Agent release 9*i*, this metric has been obsoleted. It is recommended that you use the Redo NoWait Ratio metric. This metric is kept for backward compatibility with older versions of the Management Agent.

4.11.17 Response Time (per transaction)

This metric represents the time spent in database operations per transaction. It is derived from the total time that user calls spend in the database (DB time) and the number of commits and rollbacks performed. A change in this value indicates that either the workload has changed or that the databases ability to process the workload has changed because of either resource constraints or contention.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page. Changes in the response time per transaction will appear as increased time spent in the database, either on CPU or in wait events and ADDM will report the sources of contention for both hardware and software resources.

4.11.18 Row Cache Miss Ratio (%)

This metric represents the percentage of row cache miss ratio.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.11.19 Sorts in Memory (%)

This metric represents the sort efficiency as measured by the percentage of times sorts were performed in memory as opposed to going to disk.

For best performance, most sorts should occur in memory because sorts to disks are less efficient. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption.

This test checks the percentage of sorts performed in memory rather than to disk. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x;	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	%value%% of sorts are performed in memory.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

(DeltaMemorySorts / (DeltaDiskSorts + DeltaMemorySorts)) * 100 where:

- DeltaMemorySorts: difference in 'select value from v$sysstat where name='sorts (memory)'' between sample end and start
- DeltaDiskSorts: difference in 'select value from v$sysstat where name='sorts (disk)'' between sample end and start

User Action

The sessions that are performing the most sorts should be identified such that the SQL they are executing can be further identified. The sort area sizes for the database may be sized correctly, and the application SQL may be performing unwanted or excessive sorts. The sessions performing the most sorts are available through the Top Sessions page sorted by Disk Sorts.

Further drilldown into the session performing the most disk sorts with the Current SQL page shows you the SQL statement responsible for the disk sorts.

The Top SQL page sorted by Sorts provides a mechanism to quickly display the SQL statements in the cache, presented in sorted order by their number sort operations. This is an alternative to viewing a sort of current sessions. It allows you to view sort activity via SQL statements and contains cumulative statistics for all executions of that statement.

If excessive sorts are taking place on disk and the queries are correct, consider increasing the SORT_AREA_SIZE initialization parameter to increase the size of the sort area. A larger sort area allows the Oracle Server to maintain sorts in memory, reducing the number of I/O operations required to do an equivalent amount of work using the current sort area size.

4.12 Failed Logins Metrics

The Failed Logins metrics check for the number of failed logins on the target database. This check is performed every ten minutes and returns the number of failed logins for that ten-minute interval. This metric will only work for databases where the audit_trail initialization parameter is set to DB or XML and the session is being audited.

4.12.1 Failed Login Count

This metric checks for the number of failed logins on the target database. This check is performed every ten minutes and returns the number of failed logins for that ten-minute interval. This metric will only work for databases where the audit_trail initialization parameter is set to DB or XML and the session is being audited.

If the failed login count crosses the values specified in the threshold arguments, then a warning or critical alert is generated. Since it is important to know every time a significant number of failed logins occurs on a system, this metric will fire a new alert for any ten-minute interval where the thresholds are crossed. The user can manually clear these alerts, they will not automatically clear after the next collection.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 30 Minutes	After Every Sample	>=	150	300	1[1]	There have been %value% failed login attempts in the last %failed_ login_interval_ min% minutes.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time" object.

If warning or critical threshold values are currently set for any "Time" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time" object, use the Edit Thresholds page.

Data Source

The database stores login information in different views, based on the audit_trail setting. The database views used are:

- DB or DB_EXTENDED: DBA_AUDIT_SESSION
- XML (10*g* Release 2 only): DBA_COMMON_AUDIT_TRAIL

User Action

No user action is required.

4.13 Flash Recovery Metrics

The Flash Recovery metrics relate to the flash recovery area.

4.13.1 Flash Recovery Area

This metric returns the Flash Recovery Area Location.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

```
SELECT value
  FROM v$parameter
  WHERE name='db_recovery_file_dest';
```

User Action

No user action is required.

4.13.2 Flash Recovery Area Size

This metric returns the Flash Recovery Area Size.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

```
SELECT value
  INTO 1_flash_recovery_size
  FROM v$parameter
  WHERE name='db_recovery_file_dest_size';
```

User Action

No user action is required.

4.13.3 Flashback On

This metric returns whether or not flashback logging is enabled - YES, NO, or RESTORE POINT ONLY. For the RESTORE POINT ONLY option, flashback is ON but you can only flashback to guaranteed restore points.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

```
SELECT flashback_on
  FROM v$database;
```

User Action

No user action is required.

4.13.4 Log Mode

This metric returns the log mode of the database - ARCHIVELOG or NOARCHIVELOG.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

```
SELECT log_mode
  FROM v$database;
```

User Action

No user action is required.

4.13.5 Non-Reclaimable Flash Recovery Area (%)

This metric represents the percentage of space non-reclaimable (spaced used minus space reclaimable) in the flash recovery area.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

```
Non-reclaimable = space used - space reclaimable
```

```
Space Used:
  SELECT SUM(PERCENT_SPACE_USED
     FROM v$flash_recovery_area_usage;

Space Reclaimable:
  SELECT SUM(PERCENT_SPACE_RECLAIMABLE)
     FROM v$flash_recovery_area_usage;
```

User Action

No user action is required.

4.13.6 Oldest Flashback Time

This metric returns the oldest point-in-time to which you can flashback your database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

```
SELECT to_char(oldest_flashback_time, 'YYYY-MM-DD HH24:MI:SS')
  FROM v$flashback_database_log;
```

User Action

No user action is required.

4.13.7 Reclaimable Flash Recovery Area (%)

This metric represents the percentage of space reclaimable in the flash recovery area.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

```
Space Reclaimable:
  SELECT SUM(PERCENT_SPACE_RECLAIMABLE)
     FROM v$flash_recovery_area_usage;
```

User Action

No user action is required.

4.13.8 Usable Flash Recovery Area (%)

This metric represents the percentage of space usable in the flash recovery area. The space usable is composed of the space that is free in addition to the space that is reclaimable.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

```
SELECT (CASE WHEN PERCENT_USED > 100 THEN 0 ELSE (100-PERCENT_USED) END)
PERCENT_FREE
   FROM (SELECT (SUM(PERCENT_SPACE_USED)-SUM(PERCENT_SPACE_RECLAIMABLE))
PERCENT_USED
   FROM V$FLASH_RECOVERY_AREA_USAGE);
```

User Action

No user action is required.

4.14 Global Cache Statistics Metrics

The Global Cache Statistics metrics are associated with global cache statistics.

4.14.1 Global Cache Average Convert Time (centi-seconds)

This metric represents the average convert time, measured in hundredths of a second.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every 3 Samples	>	0.3	0.6	2	Global cache converts time is %value% cs.

Data Source

global cache convert time * 10 / global cache converts

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.14.2 Global Cache Average CR Block Request Time (centi-seconds)

This metric represents the average time, measured in hundredths of a second, that CR block was received.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every 3 Samples	>	0.5	1	1	Global cache CR Block request time is %value% cs.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every 3 Samples	>	1	2	1	Generated By Database Server

Data Source

global cache CR block receive time * 10 / global cache current blocks received

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.14.3 Global Cache Average Current Block Request Time (centi-seconds)

This metric represents the average time, measured in hundredths of a second, to get a current block.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every 3 Samples	>	0.5	1	1	Global cache CR Block request time is %value% cs.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every 3 Samples	>	1	2	1	Generated By Database Server

Data Source

global cache current block send time * 10 / global cache current blocks served

User Action

Specific to your site.

4.14.4 Global Cache Average Get Time (centi-seconds)

This metric represents the average get time, measured in hundredths of a second.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every 3 Samples	>	0.3	0.6	2	Global cache gets time is %value% cs.

Data Source

global cache get time * 10 / global cache gets

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.14.5 Global Cache Blocks Corrupt

This metric represents the number of blocks that encountered a corruption or checksum failure during interconnect over the user-defined observation period.

Note: Unlike most metrics, which accept thresholds as real numbers, this metric can only accept an integer as a threshold.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every 3 Samples	>	0	0	1[1]	Total global cache blocks corrupt is %value%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every 3 Samples	>	0	0	1[1]	Generated By Database Server

[1] Once an alert is triggered for this metric, it must be manually cleared.

Data Source

global cache blocks corrupted

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.14.6 Global Cache Blocks Lost

This metric represents the number of global cache blocks lost over the user-defined observation period.

Note: Unlike most metrics, which accept thresholds as real numbers, this metric can only accept an integer as a threshold.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every 3 Samples	>	1	3	1[1]	Total global cache block lost is %value%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every 3 Samples	>	1	3	1[1]	Generated By Database Server

[1] Once an alert is triggered for this metric, it must be manually cleared.

Data Source

global cache blocks lost

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.15 Health Check Metrics

Health Check metrics show the status of the database instance. It shows whether the instance is Up, Down, Mounted, Unmounted, or in another problem condition. The data returned is the true state of the database, regardless of listener status.

4.15.1 Instance State

Internal number used by the database

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 seconds

Data Source

Memory-mapped file $ORACLE_HOME/dbs/hc_.dat

User Action

No user action is required.

4.15.2 Instance Status

This metric will return 0 if the instance is down, and 1 if the instance is up. If the instance is down, the reason 'Abnormal Termination or Instance Shutdown', will appear in the State Description column.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Seconds	Not Uploaded	=	Not Defined	0	1	The instance is down, and health check reported %text%.

Data Source

Memory-mapped file $ORACLE_HOME/dbs/hc_.dat

User Action

Consult the corrective action on the database home page. Corrective action could include starting up the database.

4.15.3 Maintenance

This metric will return 0 if the instance is in any maintenance state, and 1 otherwise. Possible maintenance states are Read-only, Restricted Access, and Quiesced.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Seconds	Not Uploaded	=	0	Not Defined	1	The database is in the following maintenance states: %text%.

Data Source

Memory-mapped file $ORACLE_HOME/dbs/hc_.dat

User Action

No user action is required.

4.15.4 Mounted

This metric will return 0 if the instance is in a Mounted state, and 1 otherwise.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Seconds	Not Uploaded	=	0	Not Defined	1	The database has been started and is in mounted state.

Data Source

Memory-mapped file $ORACLE_HOME/dbs/hc_.dat

User Action

No user action is required.

4.15.5 State Description

If the instance is down, unavailable, or in a maintenance state, this will display which state it is in.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Seconds

Data Source

Memory-mapped file $ORACLE_HOME/dbs/hc_.dat

User Action

Consult the corrective action on the database home page. Corrective action could include starting up the database.

4.15.6 Unavailable

This metric will return 0 if the instance is in any unavailable state, and 1 otherwise. Possible unavailable states are Corrupted Controlfile, Corrupted Dictionary, Inaccessible Logfile, Stuck Archiver, Instance Recovery, and Cluster Reconfiguration.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Seconds	Not Uploaded	=	0	Not Defined	1	The database is not available due to the following conditions: %text%.

Data Source

Memory-mapped file $ORACLE_HOME/dbs/hc_.dat

User Action

Consult the corrective action on the database home page. Corrective action could include starting up the database.

4.15.7 Unmounted

This will return 0 is the instance is in an Unmounted state, and 1 otherwise.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Seconds	Not Uploaded	=	0	Not Defined	1	The instance has been started in no-mount state.

Data Source

Memory-mapped file $ORACLE_HOME/dbs/hc_.dat

User Action

No user action is required.

4.16 Incident Metrics

The incident metrics include the following:

- Section 4.16.1, "Incident"
- Section 4.16.2, "Incident Status"

4.16.1 Incident

This metric category contains the metrics representing incidents, for example, generic internal error, access violation, and so on as recorded in the database alert log file. The alert log file has a chronological log of messages and errors.

Each metric signifies that the database being monitored has detected a critical error condition about the database and has generated an incident to the alert log file since the last sample time. The Support Workbench in Enterprise Manager contains more information about each generated incident.

4.16.1.1 Access Violation

This metric signifies that the database has generated an incident due to some memory access violation. This type of incident is typically related to Oracle Exception messages such as ORA-3113 and ORA-7445. The database can also generate this type of incident when it detects a SIGSEGV or SIGBUS signals.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	An access violation detected in %alertLogName% at time/line number: %tmeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.2 Alert Log Error Trace File

This metric is the name of the trace file (if any) associated with the logged incident.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.16.1.3 Alert Log Name

This metric is the name of the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.16.1.4 Cluster Error

This metric signifies that the database has generated an incident due to a member evicted from the group by a member of the cluster database. This type of incident is typically related to Oracle Exception message ORA-29740.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A cluster error detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.
[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.5 Deadlock

This metric signifies that the database has generated an incident due to a deadlock detected while trying to lock a library object. This type of incident is typically related to Oracle Exception message ORA-4020.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A deadlock detected in $alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.
[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.6 File Access Error

This metric signifies that the database has generated an incident due to failure to read a file at the time. This type of incident is typically related to Oracle Exception message ORA-376.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A file access error detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.
[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.7 Generic Incident

This metric signifies that the databse has generated an incident due to some database error.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Incident (%errCodes%) detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.
[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.8 Generic Internal Error

This metric signifies that the database has generated an incident due to an internal database error. This type of incident is typically related to Oracle Exception message ORA-600 or ORA-0060*.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Internal error (%errCodes%) detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.9 Impact

This metric is the impact of an incident. For a Generic Internal Error incident, the impact describes how the incident may affect the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.16.1.10 Incident ID

This metric is a number identifying an incident. The Support Workbench in Enterprise Manager uses this ID to specify an incident.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.16.1.11 Inconsistent DB State

This metric signifies that the database has generated an incident due to an inconsistent database state such an invalid ROWID. This type of incident is typically related to Oracle Exception message ORA-1410.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	An inconsistent DB state detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.12 Internal SQL Error

This metric signifies that the database has generated an incident due to an internal SQL error. This type of incident is typically related to Oracle Exception message ORA-604.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	An internal SQL error detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.
[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.13 Oracle Data Block Corruption

This metric signifies that the database has generated an incident due to an ORACLE data block corruption. This type of incident is typically related to Oracle Exception message ORA-1578.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	An Oracle data block corruption detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident. **Note:** This event does not automatically clear since there is no automatic way of

determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.14 Out of Memory

This metric signifies that the database has generated an incident due to failure to allocate memory. This type of incident is typically related to Oracle Exception message ORA-4030 or ORA-4031.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Out of memory detected in %alertLogName% at tme/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.15 Redo Log Corruption

This metric signifies that the database has generated an incident due to an error with the redo log. This type of incident is typically related to Oracle Exception message ORA-353, ORA-355, or ORA-356.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A redo log corruption detected in %alertLogName% at time/line number: %timeLome%/

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.1.16 Session Terminated

This metric signifies that the database has generated an incident due to an unexpected session termination. This type of incident is typically related to Oracle Exception message ORA-603.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A session termination detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the incident.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.16.2 Incident Status

Incident Status metrics represent whether the last scan of the alert log identified each type of incident and, if so, how many.

4.16.2.1 Access Violation Status

This metric reflects the number of Access Violation incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Access violation errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.2 Cluster Error Status

This metric reflects the number of Cluster Error incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Cluster errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.3 Deadlock Status

This metric reflects the number of Deadlock incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Deadlocks have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.4 File Access Error Status

This metric reflects the number of File Access Error incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	File access errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.5 Generic Incident Status

This metric reflects the number of Generic Incident incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	%value% distinct types of incidents have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.6 Generic Internal Error Status

This metric reflects the number of Generic Internal Error incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Generic internal errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.7 Inconsistent DB State Status

This metric reflects the number of Inconsistent DB State incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Incident DB state errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.8 Internal SQL Error Status

This metric reflects the number of Internal SQL Error incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Internal SQL errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.9 Oracle Data Block Corruption Status

This metric reflects the number of Oracle Data Block Corruption incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Oracle data block corruption errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.10 Out of Memory Status

This metric reflects the number of Out of Memory Status incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Out of memory errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.11 Redo Log Corruption Status

This metric reflects the number of Redo Log Corruption incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Redo log corruption errors have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.16.2.12 Session Terminated Status

This metric reflects the number of Session Terminated incidents witnessed the last time Enterprise Manager scanned the alert log.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Session terminations have been found in the alert log.

Data Source

Incident metric

User Action

User Support Workbench in Enterprise Manager to examine the details of the incidents.

4.17 Interconnect Metrics

The Interconnect metrics include the following:

- Section 4.17.1, "Interconnect Metrics"
- Section 4.17.2, "Interconnect Traffic"

4.17.1 Interconnect Metrics

Interconnect metrics collect the information of network interfaces used by cluster database instances as internode communication.

4.17.1.1 Interface Type

Cluster database instances should use private interconnects for internode communication. This metric monitors whether the network interface used by the cluster instance is a private one. If the network interface is known to be public, a critical alert is generated. If the network interface type is unknown, a warning alert is generated.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 12 Hours	After Every Sample	=	Unknown	Public	1	The instance is using interface '%if_name%' of type '%value%'.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Interface Name" object.

If warning or critical threshold values are currently set for any "Interface Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Interface Name" object, use the Edit Thresholds page.

Data Source

V$CLUSTER_INTERCONNECTS

V$CONFIGURED_INTERCONNECTS

User Action

Use oifcfg in the CRS home to correctly configure the private interfaces in OCR.

4.17.2 Interconnect Traffic

Interconnect Traffic metrics monitor the internode data transfer rate of cluster database instances.

4.17.2.1 Transfer Rate (MB/s)

This metric collects the internode communication traffic of a cluster database instance. This is an estimation using the following formula:

```
(gc cr blocks received/sec + gc current blocks received/sec + gc cr blocks
```

```
served/sec + gc current blocks served/sec) * db_block_size
+
( messages sent directly/sec + messages send indirectly/sec + messages
received/sec ) * 200 bytes
```

The critical and warning thresholds of this metric are not set by default. Users can set them according to the speed of their cluster interconnects.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Not Defined

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Instance Name" object.

If warning or critical threshold values are currently set for any "Instance Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Instance Name" object, use the Edit Thresholds page.

Data Source

V$SYSSTAT

V$DLM_MISC

V$PARAMETER

User Action

No user action is required.

4.18 Invalid Objects Metrics

The Invalid Objects metrics include the following:

- Section 4.18.1, "Invalid Objects"
- Section 4.18.2, "Invalid Objects by Schema"

4.18.1 Invalid Objects

The Invalid Objects metrics represent the metrics associated with invalid objects.

4.18.1.1 Total Invalid Object Count

This metric represents the total invalid object count.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	Not Uploaded	>	Not Defined	Not Defined	1	%value% object(s) are invalid in the database.

Data Source

SYS.OBJ$ and SYS.USER$ tables

User Action

Specific to your site.

4.18.2 Invalid Objects by Schema

The Invalid Objects by Schema metrics represent the number of invalid objects in each schema.

4.18.2.1 Owner's Invalid Object Count

This metric represents the invalid object count by owner.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	Not Uploaded	>	2	Not Defined	1	%value% object(s) are invalid in the %owner% schema.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Invalid Object Owner" object.

If warning or critical threshold values are currently set for any "Invalid Object Owner" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Invalid Object Owner" object, use the Edit Thresholds page.

Data Source

SYS.OBJ$ and SYS.USER$ tables

User Action

View the status of the database objects in the schema identified by the Invalid Object Owner metric. Recompile objects as necessary.

4.19 Key Profiles Metrics

The Key Profiles metrics include the following:

- Section 4.19.1, "key_profiles_count"
- Section 4.19.2, "key_profiles_enable"

4.19.1 key_profiles_count

This metric proivdes the count of key profiles.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 60 Minutes

Data Source

Not available

User Action

Specific to your site.

4.19.2 key_profiles_enable

This metric denotes the key profiles enabled.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 60 Minutes

Data Source

Not available

User Action

Specific to your site.

4.20 Messages Metrics

The Message metrics include the following:

- Section 4.20.1, "Messages in the Buffered Queue"

Section 4.20.2, "Messages in the Persistent Queue"

- Section 4.20.3, "Messages in the Persistent Queue Per Subscriber"
- Section 4.20.4, "Messages Per Queue"
- Section 4.20.5, "Messages Per Queue Per Subscriber"

4.20.1 Messages in the Buffered Queue

The Messages in the Buffered Queue metrics monitor the age and state of the first (top of the queue) message for each buffered queue in the database except for the system queues. Queues that are in the schema of SYS, SYSTEM, DBSNMP, and SYSMAN are defined as system level queues.

4.20.1.1 Age of the First Messsage in Buffered Queue Per Queue (Seconds)

This metric gives the age (in seconds) of the first message in the buffered queue for all non-system queues in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	>=	Not Defined	Not Defined	1	Age of first message in %schema%.%queue_name% buffered queue is %value% seconds.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name" and "Queue Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects, use the Edit Thresholds page.

Data Source

This metric is calculated by finding the age of the first message in all the subscribers of the queue and then the oldest amongst all is taken.

The following views/tables are used for the calculation:

1. <SCHEMA>.AQ$<QUEUE_TABLE>
2. v$buffered_queues

User Action

When using buffered queues for storing and propagating messages, monitor this metric to get the age of first message in the queue.

4.20.1.2 State of the First Message in Buffered Queue Per Queue

This metric gives the state of the first message in the buffered queue for all non-system queues in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 30 Minutes

Data Source

This metric is calculated by finding the age of the first message in all the subscribers of the queue and then the oldest amongst all is computed. Finally the state of this oldest message is fetched.

The following views/tables are used for the calculation:

1. <SCHEMA>.AQ$<QUEUE_TABLE>
2. v$buffered_queues

User Action

When using buffered queues for storing and propagating messages, monitor this metric to get the state of first message in the queue.

4.20.2 Messages in the Persistent Queue

The Messages in the Persistent Queue metrics monitor the age and state of the first (top of the queue) message for each persistent queue in the database except for the system queues. Queues that are in the schema of SYS, SYSTEM, DBSNMP, and SYSMAN are defined as system level queues.

4.20.2.1 Age of the First Messsage in Persistent Queue Per Queue (Seconds)

This metric gives the age (in seconds) of the first message in the persistent queue for all non-system queues in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	>=	Not Defined	Not Defined	1	Age of first message in %schema%.%queue_name% queue is %value% seconds.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name" and "Queue Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects, use the Edit Thresholds page.

Data Source

This metric is calculated by finding the age of the first message in all the subscribers of the queue and then the oldest amongst all is taken.

The following views/tables are used for the calculation:

1. <SCHEMA>.AQ$_<QUEUE_TABLE>_S
2. <SCHEMA>.AQ$_<QUEUE_TABLE>_I
3. <SCHEMA>.AQ$<QUEUE_TABLE>

User Action

When using persistent queues for storing and propagating messages, monitor this metric to get the age of first message in the queue.

4.20.2.2 State of the First Message in Persistent Queue Per Queue

This metric gives the state of the first message in the persistent queue for all non-system queues in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 30 Minutes

Data Source

This metric is calculated by finding the age of the first message in all the subscribers of the queue and then the oldest amongst all is computed. Finally the state of this oldest message is fetched.

The following views/tables are used for the calculation:

1. <SCHEMA>.AQ$_<QUEUE_TABLE>_S

2. <SCHEMA>.AQ$_<QUEUE_TABLE>_I
3. <SCHEMA>.AQ$<QUEUE_TABLE>

User Action

When using persistent queues for storing and propagating messages, monitor this metric to get the state of first message in the queue.

4.20.3 Messages in the Persistent Queue Per Subscriber

The Messages in the Persistent Queue Per Subscsriber metrics monitor the age and state of the first (top of the queue) message for each persistent queue per queue subscriber in the database except for the system queues. Queues that are in the schema of SYS, SYSTEM, DBSNMP, and SYSMAN are defined as system level queues.

4.20.3.1 Age of the First Message in Persistent Queue Per Subscriber (seconds)

This metric gives the age (in seconds) of the first message in the persistent queue per subscriber for all non-system queues in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 30 Minutes

Data Source

This is calculated using the ENQ_TIME of the messages in the queue per subscriber and then the oldest amongst all per subscriber is taken.

The following views/tables are used for the calculation:

1. <SCHEMA>.AQ$_<QUEUE_TABLE>_S
2. <SCHEMA>.AQ$_<QUEUE_TABLE>_I
3. <SCHEMA>.AQ$<QUEUE_TABLE>

User Action

When using persistent queues for storing and propagating messages, monitor this metric to get the age of first message in the queue per subscriber.

4.20.3.2 State of the First Message In Persistent Queue Per Subscriber

This metric gives the state of the first message in the persistent queue per subscriber for all non-system queues in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 30 Minutes

Data Source

This metric is calculated by finding the age of the first message in the subscriber of the queue and then the oldest amongst all is computed. Finally the state of this oldest message is fetched. .

The following views/tables are used for the calculation:

1. <SCHEMA>.AQ$_<QUEUE_TABLE>_S
2. <SCHEMA>.AQ$_<QUEUE_TABLE>_I
3. <SCHEMA>.AQ$<QUEUE_TABLE>

User Action

When using persistent queues for storing and propagating messages, monitor this metric to get the state of first message in the queue per subscriber.

4.20.4 Messages Per Queue

The Messages Per Queue metrics monitor the messages for each queue in the database except for system queues. Queues that are in the schema of SYS, SYSTEM, DBSNMP, and SYSMAN are defined as system level queues.

4.20.4.1 Average Age of Messages Per Queue (Seconds)

This metric shows the average age of all the messages in the queue for all non-system queues in seconds.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	>=	Not Defined	Not Defined	1	Average age of messages in %schema%.%queue_name% queue is %value% seconds.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name" and "Queue Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects, use the Edit Thresholds page.

Data Source

The average is calculated using SYSDATE and ENQ_TIME column from the following view: <SCHEMA>.AQ$<QUEUE_TABLE_NAME>.

This is a dynamic view that is created by default by the Oracle database when the user creates a queue table and queue.

User Action

When using queues for storing and propagating messages, monitor this metric to get the average age of messages in the queue.

4.20.4.2 Messages Processed Per Queue (%)

This metric gives the messages processed percentage for the queue. Messages processed percent is calculated as the percent of the total number messages processed/dequeued to the total number of messages received/enqueued.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Messages processed for queue %schema%.%queue_name% queue is %value% percent.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name" and "Queue Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects, use the Edit Thresholds page.

Data Source

CNUM_MSGS, EXPIRED_MSGS, NUM_MSGS columns from V$BUFFERED_QUEUES and ENQUEUED_MSGS and DEQUEUED_MSGS from V$PERSISTENT_QUEUES is used to compute this value.

User Action

When using queues for storing and propagating messages, monitor this metric to get the messages processed percent (or throughput) for the queue.

4.20.4.3 Messages Processed Per Queue (%) Per Minute in the Last Interval

This metric gives the messages processed percentage per minute in the last collection interval of the metric for the queue.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Messages processed per minute in the last interval for queue %schema%.%queue_name% is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name" and "Queue Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects, use the Edit Thresholds page.

Data Source

This metric is calculated as processed percent obtained in Messages Processed Per Queue (%) metric per metric collection interval.

User Action

When using queues for storing and propagating messages, monitor this metric to get the messages processed percent (or throughput) per minute in the last collection interval for the queue.

4.20.4.4 Total Messages Processed Per Minute in the Last Interval

This metric gives the total number of messages processed per minute in the last collection interval of the metric for the queue.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Total messages processed per minute in the last interval for queue %schema%.%queue_name% is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name" and "Queue Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects, use the Edit Thresholds page.

Data Source

This metric is calculated as the rate of total messages processed per minute per metric collection interval.

User Action

When using queues for storing and propagating messages, monitor this metric to get the total number of messages processed/dequeued per minute in the last collection interval for the queue.

4.20.4.5 Total Messages Received Per Minute in the Last Interval

This metric gives the total number of messages received or enqueued into the queue per minute in the last collection interval of the metric.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Total messages received per minute in the last interval for queue %schema%.%queue_name% is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name" and "Queue Name" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name" and "Queue Name" objects, use the Edit Thresholds page.

Data Source

This metric is calculated as the rate of total messages received/enqueued per minute per metric collection interval.

User Action

When using queues for storing and propagating messages, monitor this metric to get the total number of messages received/enqueued per minute in the last collection interval for the queue.

4.20.4.6 Total Number of Messages Processed

This metric gives the total number of messages processed or dequeued from the queue.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 30 Mintes

Data Source

This metric is calculated as the sum of (CNUM_MSGS-EXPIRED_MSGS-NUM_MSGS) from V$BUFFERED_QUEUES and DEQUEUED_MSGS from V$PERSISTENT_QUEUES.

User Action

When using queues for storing and propagating messages, monitor this metric to get the total number of messages processed/dequeued in the queue.

4.20.4.7 Total Number of Messages Received

This metric gives the total number of messages received or enqueued into the queue.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 30 Mintes

Data Source

This metric is calculated as the sum of CNUM_MSGS from V$BUFFERED_QUEUES and ENQUEUED_MSGS from V$PERSISTENT_QUEUES.

User Action

When using queues for storing and propagating messages, monitor this metric to get the total number of messages received/enqueued into the queue.

4.20.5 Messages Per Queue Per Subscriber

The Messages Per Queue Per Subscriber metrics monitor the messages for each queue subscriber in the queue in the database except for system queues. Queues that are in the schema of SYS, SYSTEM, DBSNMP, and SYSMAN are defined as system level queues.

4.20.5.1 Average Age of Messages Per Queue Per Subscriber (Seconds)

This metric shows the average age of all the messages in the queue per subscriber for all non-system queues in seconds.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	>=	Not Defined	Not Defined	1	Average age of messages for the subscriber %subs_ name% %subs_ address% in %schema%.%queue _name% queue is %value% seconds.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, use the Edit Thresholds page.

Data Source

The average is calculated using SYSDATE, ENQ_TIME, and CONSUMER_NAME columns from the following view: <SCHEMA>.AQ$<QUEUE_TABLE_NAME>.

This is a dynamic view that is created by default by the Oracle database when the user creates a queue table and queue.

User Action

When using queues for storing and propagating messages, monitor this metric to get the average age of messages in the queue per subscriber.

4.20.5.2 Messages Processed Per Queue (%) Per Subscriber Per Minute in the Last Interval

This metric gives the messages processed percentage per minute in the last collection interval of the metric for the queue and queue subscriber.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Messages processed per minute in the last interval for the subscriber %subs_name% %subs_address% in %schema%.%queue_name% is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, use the Edit Thresholds page.

Data Source

This metric is calculated as processed percent obtained in Messages Processed Per Queue Per Subscriber (%) metric per metric collection interval.

User Action

When using queues for storing and propagating messages, monitor this metric to get the messages processed percent (or throughput) per minute in the last collection interval for the queue per subscriber.

4.20.5.3 Messages Processed Per Queue Per Subscriber(%)

This metric gives the messages processed percentage for the queue per subscriber. Messages processed percent is calculated as the percent of the total number messages

processed/dequeued per queue per subscriber to the total number of messages received/enqueued per queue per subscriber.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Messages processed for queue %schema%.%queue_name% queue is %value% percent.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, use the Edit Thresholds page.

Data Source

CNUM_MSGS, EXPIRED_MSGS, NUM_MSGS columns from V$BUFFERED_SUBSCRIBERS and ENQUEUED_MSGS and DEQUEUED_MSGS from V$PERSISTENT_SUBSCRIBERS is used to compute this value.

User Action

When using queues for storing and propagating messages, monitor this metric to get the messages processed percent (or throughput) for the queue per subscriber.

4.20.5.4 Total Messages Processed Per Queue Per Subscsriber Per Minute in the Last Interval

This metric gives the total number of messages processed/dequeued per minute in the last collection interval of the metric for the queue at the subscriber level.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Total messages processed per minute in the last interval for the subscriber %subs_name% %subs_address% in %schema%.%queue_name% queue is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, use the Edit Thresholds page.

Data Source

This metric is calculated as the rate of total messages processed per minute per metric collection interval for the queue and the queue subscriber.

User Action

When using queues for storing and propagating messages, monitor this metric to get the total number of messages processed/dequeued per minute in the last collection interval for the queue and queue subscriber.

4.20.5.5 Total Messages Received Per Queue Per Subscriber Per Minute in the Last Interval

This metric gives the total number of messages received or enqueued into the queue subscriber of the queue per minute in the last collection interval of the metric.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.2.0.x	Every 30 Minutes	After Every Sample	<=	Not Defined	Not Defined	1	Total messages received per minute in the last interval for the subscriber %subs_ name% %subs_ address% in %schema%.%queue _name% queue is %value%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects.

If warning or critical threshold values are currently set for any unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Schema Name", "Queue Name", "Subscriber Name", and "Subscriber Address" objects, use the Edit Thresholds page.

Data Source

This metric is calculated as the rate of total messages received/enqueued per minute per metric collection interval for the queue and queue subscriber.

User Action

When using queues for storing and propagating messages, monitor this metric to get the total number of messages received/enqueued per minute in the last collection interval for the queue subscriber of the queue.

4.20.5.6 Total Number of Messages Processed

This metric gives the total number of messages processed or dequeued from the queue subscriber of the queue.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 30 Mintes

Data Source

This metric is calculated as the sum of (CNUM_MSGS-EXPIRED_MSGS-NUM_MSGS) from V$BUFFERED_SUBSCRIBERS and DEQUEUED_MSGS from V$PERSISTENT_ SUBSCRIBERS.

User Action

When using queues for storing and propagating messages, monitor this metric to get the total number of messages processed/dequeued in the queue subscriber of the queue.

4.20.5.7 Total Number of Messages Received

This metric gives the total number of messages received or enqueued into the queue per subscriber.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.2.0.x	Every 30 Mintes

Data Source

This metric is calculated as the sum of CNUM_MSGS from V$BUFFERED_SUBSCRIBERS and ENQUEUED_MSGS from V$PERSISTENT_SUBSCRIBERS.

User Action

When using queues for storing and propagating messages, monitor this metric to get the total number of messages received/enqueued into the queue per queue subscriber.

4.21 OCM Instrumentation

This metric determines whether the database has been instrumented with Oracle Configuration Manager (OCM). Oracle Configuration Manager is used to personalize the support experience by collecting configuration information and uploading it to the Oracle repository.

When customer configuration data is uploaded on a regular basis, customer support representatives can analyze this data and provide better service to the customers. For example, when a customer logs a service request, he can associate the configuration data directly with that service request. The customer support representative can then view the list of systems associated with the customer and solve problems accordingly.

4.21.1 Instrumentation Present

This metric determines whether the database has been instrumented with Oracle Configuration Manager.

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 24 Hours

Data Source

Not available

User Action

No user action is required.

4.21.2 Need to Instrument with OCM

This metric determines that Oracle Configuration Manager needs to be instrumented in the database.

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	After Every Sample	=	1	Not Defined	1	OCM Instrumentation should be installed in database. Please use $ORACLE_HOME/ccr/admin/scripts/installCCRSQL script with collectconfig parameter.

Data Source

Not available

User Action

Install Oracle Configuration Manager (OCM) in the database.

4.21.3 OCM Configured

This metric determines the Oracle Configuration Manager is configured.

Metric Summary for Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 24 Hours

Data Source

Not available

User Action

No user action is required.

4.22 Operational Error Metrics

The Operational Error metrics include the following:

4.22.1 Operational Error

This metric category contains the metrics representing errors that may affect the operation of the database, for example, archiver hung, media failure, and so on as recorded in the database alert log file. The alert log file has a chronological log of messages and errors.

Each metric signifies that the database being monitored has detected a critical error condition that may affect the normal operation of the database and has generated an error message to the alert log file since the last sample time. The Support Workbench in Enterprise Manager may contain more information about the error.

4.22.1.1 Alert Log Error Trace File

This metric is the name of the trace file (if any) associated with the logged error.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.22.1.2 Alert Log Name

This metric is the name of the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

No user action is required.

4.22.1.3 Archiver Hung

This metric signifies that the archiver of the database being monitored has been temporarily suspended since the last sample time.

If the database is running in ARCHIVELOG mode, an alert is displayed when archiving is hung (ORA-00257 or ORA-16038) messages are written to the alert file. The alert file is a special trace file containing a chronological log of messages and errors.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Archiver hang detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error; however, the most likely cause of this message is that the destination device is out of space to store the redo log file. Verify the device specified in the initialization parameter ARCHIVE_LOG_DEST is set up properly for archiving. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.22.1.4 Data Block Corruption

This metric signifies that the database being monitored has generated a corrupted block error (ORA-01157 or ORA-27048) to the alert file since the last sample time. The alert file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages are written to the alert file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	A datablock corruption detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.22.1.5 Generic Operational Error

This metric signifies that the database being monitored has generated some error that may affect the normal operation of the database to the alert file since the last sample time. The alert file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages are written to the alert file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Operational error (%errCodes%) detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.22.1.6 Media Failure

This metric signifies that the database being monitored has generated a media failure error (ORA-01242 or ORA-01243) to the alert file since the last sample time. The alert file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages are written to the alert file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	MATCH	Not Defined	.[1]	1[2]	Media Failure detected in %alertLogName% at time/line number: %timeLine%.

[1] Once an alert is triggered for this metric, it must be manually cleared.

[2] Once an alert is triggered for this metric, it must be manually cleared.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Time/Line Number" object.

If warning or critical threshold values are currently set for any "Time/Line Number" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Time/Line Number" object, use the Edit Thresholds page.

Data Source

$ORACLE_HOME/sysman/admin/scripts/alertlogAdr.pl where $ORACLE_HOME refers to the home of the Oracle Management Agent.

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.
Note: This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

4.22.2 Operational Error Status

The Operational Error Status metrics place all the types of alert log errors into four categories: Archiver Hung, Data Block Corruption, Media Failure, and Generic Operational Error. The metrics in this category represent whether the last scan of the alert log identified any of the aforementioned categories of error and, if so, how many.

4.22.2.1 Archiver Hung Status

This metric reflects the number of Archiver Hung operational errors witnessed the last time Enterprise Manager scanned the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Archiver hung errors have been found in the alert log.

Data Source

Operational Error metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

4.22.2.2 Data Block Corruption Status

This metric reflects the number of Data Block Corruption operational errors witnessed the last time Enterprise Manager scanned the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Data block corruption errors have been found in the alert log.

Data Source

Operational Error metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

4.22.2.3 Generic Operational Error Status

This metric reflects the number of Generic Operation Error errors witnessed the last time Enterprise Manager scanned the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	%value% distinct types of operational errors have been found in the alert log.

Data Source

Operational Error metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

4.22.2.4 Media Failure Status

This metric reflects the number of Media Failure errors witnessed the last time Enterprise Manager scanned the alert log file.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	0	1	Media failure errors have been found in the alert log.

Data Source

Operational Error metric

User Action

Use Support Workbench in Enterprise Manager to examine the details of the error.

4.23 Recovery Metrics

The Recovery metrics include the following:

- Section 4.23.1, "Recovery"
- Section 4.23.2, "Recovery Area"

4.23.1 Recovery

Recovery metrics are related to database recovery.

4.23.1.1 Corrupt Data Block Count

This metric represents the count of corrupt data blocks.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 Minutes	After Every Sample	>	Not Defined	0	1	Number of corrupt data blocks is %value%.

Data Source

```
SELECT nvl(sum(blocks), 0)
  FROM v$database_block_corruption;
```

User Action

Perform a database recovery.

4.23.1.2 Datafiles Need Media Recovery

This metric represents the count of datafiles that need recovery.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 Minutes	After Every Sample	>	Not Defined	0	1	Number of datafiles needing media recovery is %value%.

Data Source

```
SELECT count(file#)
  INTO 1_datafiles_need_recovery
  FROM v$datafile_header
  WHERE recover ='YES';
```

User Action

Perform a database recovery.

4.23.1.3 Missing Media File Count

This metric returns the count of missing media files.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x	Every 15 Minutes	After Every Sample	>	Not Defined	0	1	Number of missing media files is %value%.

Data Source

```
SELECT count(file#)
  INTO 1_missing_media_files
  FROM v$datafile_header
  WHERE error is not null AND error is 'OFFLINE NORMAL';
```

User Action

perform a database recovery.

4.23.2 Recovery Area

Recovery Area metrics are related to the recovery area.

This metric is evaluated by the server periodically every 15 minutes or during a file creation, whichever occurs first. It is also printed in the alert log. The Critical Threshold is set for less than 3% and the Warning Threshold is set for less than 15%. It is not user customizable. The user is alerted the first time the alert occurs and the alert is not cleared until the available space rises above 15%.

4.23.2.1 Recovery Area Free Space (%)

This metric represents the recovery area free space as a percentage.

Metric Summary for Database Control and Grid Control

This metric is collected for target versions: 10.1.0.x, 10.2.0.x, 11.1.0.x, and 11.2.0.x.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.24 Response Metrics

Response metrics represent the responsiveness of the Oracle Server, with respect to a client.

4.24.1 State

This metric represents the state of the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	CONTAINS	MOUNTED	Not Defined	1	The database status is %value%..

Data Source

Not available

User Action

Specific to your site.

4.24.2 Status

This metric checks whether a new connection can be established to a database. If the maximum number of users is exceeded or the listener is down, this test is triggered.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	=	Not Defined	0	1	Failed to connect to database instance %oraerr%.

Data Source

Perl returns 1 when a connection can be made to the database (using Management Agent monitoring connection details), 0 otherwise.

User Action

Check the status of the listener to make sure it is running on the node where the event was triggered. If the listener is running, check to see if the number of users is at the session limit. **Note:** The choice of user credentials for the Probe metric should be considered. If the preferred user has the RESTRICED SESSION privilege, the user will be able to connect to a database even if the LICENSE_MAX_SESSIONS limit is reached.

4.24.3 User Logon Time (msec)

This metric represents the amount of time the agent takes to make a connection to the database, measured in milliseconds.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	>	1000	Not Defined	6	User logon time is %value% msecs.

Data Source

Number of milliseconds (as measured in the Perl script) to connect to the database.

User Action

No user action is required.

4.25 Segment Advisor Recommendations Metrics

Oracle uses the Automatic Segment Advisor job to detect segment issues regularly within maintenance windows. It determines whether the segments have unused space that can be released. The Number of recommendations is the number of segments that have Reclaimable Space. The recommendations come from all runs of the automatic segment advisor job and any user scheduled segment advisor jobs.

4.25.1 Number of recommendations

Oracle uses the Automatic Segment Advisor job to detect segment issues regularly within maintenance windows. It determines whether the segments have unused space that can be released. The Number of recommendations is the number of segments that have Reclaimable Space. The recommendations come from all runs of the automatic segment advisor job and any user scheduled segment advisor jobs.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric’s value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 60 Minutes

Data Source
Not available

User Action
Oracle recommends shrinking or reorganizing these segments to release unused space.

4.26 Session Suspended Metrics

Session Suspended metrics represent the number of resumable sessions that are suspended due to some correctable error.

4.26.1 Session Suspended by Data Object Limitation

This metric represents the session suspended by data object limitation.

Metric Summary for Database Control
This metric is collected for the following targets: 10.1.0.x, 10.2.0.x, 11.1.0.x, and 11.2.0.x.

Data Source
Not available

User Action
View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.26.2 Session Suspended by Quota Limitation

This metric represents the session suspended by quota limitation.

Metric Summary for Database Control and Grid Control
This metric is collected for the following targets: 10.1.0.x, 10.2.0.x, 11.1.0.x, and 11.2.0.x.

Data Source
Not available

User Action
View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.26.3 Session Suspended by Rollback Segment Limitation

This metric represents the session suspended by rollback segment limitation.

Metric Summary for Database Control and Grid Control
This metric is collected for the following targets: 10.1.0.x, 10.2.0.x, 11.1.0.x, and 11.2.0.x.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.26.4 Session Suspended by Tablespace Limitation

This metric represents the session suspended by tablespace limitation.

Metric Summary for Database Control and Grid Control

This metric is collected for the following targets: 10.1.0.x, 10.2.0.x, 11.1.0.x, and 11.2.0.x.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.27 SGA Pool Wastage Metrics

SGA Pool Wastage metrics represent the percentage of the various pools in the SGA that are being wasted.

4.27.1 Java Pool Free (%)

This metric represents the percentage of the Java Pool that is currently marked as free.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 15 Minutes	After Every Sample	<	Not Defined	Not Defined	2	%value%% of the Java pool is free.
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	%value%% of the Java pool is free.

Data Source

((Free/Total)*100) where:

- Free: select sum(decode(name,'free memory',bytes)) from v$sgastat where pool = 'java pool'
- Total: select sum(bytes) from v$sgastat where pool = 'java pool'

User Action

If this pool size is too small, the database JVM (Java Virtual Machine) may not have sufficient memory to satisfy future calls, leading potentially to unexpected database request failures.

4.27.2 Large Pool Free (%)

This metric represents the percentage of the Large Pool that is currently marked as free.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 15 Minutes	After Every Sample	<	Not Defined	Not Defined	2	%value%% of the Java pool is free.
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	%value%% of the Java pool is free.

Data Source

((Free/Total)*100) where:

- Free: select sum(decode(name,'free memory',bytes)) from v$sgastat where pool = 'large pool'
- Total: select sum(bytes) from v$sgastat where pool = 'large pool'

User Action

Consider enlarging the large pool or utilizing it more sparingly. This reduces the possibility of large memory areas competing with the library cache and dictionary cache for available memory in the shared pool.

4.27.3 Shared Pool Free (%)

This metric represents the percentage of the Shared Pool that is currently marked as free.

This test checks the percentage of Shared Pool that is currently free. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 15 Minutes	After Every Sample	<	Not Defined	Not Defined	2	%value%% of the shared pool is free.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

((Free/Total)*100) where:

- free: select sum(decode(name,'free memory',bytes)) from v$sgastat where pool = 'shared pool'
- total: select sum(bytes) from v$sgastat where pool = 'shared pool'

User Action

If the percentage of Free Memory in the Shared Pool rises above 50%, too much memory has been allocated to the shared pool. This extra memory could be better utilized by other applications on the machine. In this case the size of the Shared Pool should be decreased. This can be accomplished by modifying the shared_pool_size initialization parameter.

4.28 Snapshot Too Old

The Snapshot Tool Old metrics represent the snapshots that are too old due to rollback segment limit or tablespace limit.

4.28.1 Snapshot Too Old Due to Rollback Segment Limit

This metric represents the snapshot too old because of the rollback segment limit.

Metric Summary for Database Control and Grid Control

This metric is collected for the following targets: 10.1.0.x, 10.2.0.x, 11.1.0.x, and 11.2.0.x.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.28.2 Snapshot Too Old Due to Tablespace Limit

This metric represents the snapshot too old because of the tablespace limit.

Metric Summary for Database Control and Grid Control

This metric is collected for the following targets: 10.1.0.x, 10.2.0.x, 11.1.0.x, and 11.2.0.x.

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.29 SQL Response Time

The SQL Response Time metrics approximate the responsiveness of SQL.

4.29.1 Baseline SQL Response Time

This metric contains the response time of the baseline.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 5 Minutes

Data Source

Not available

User Action

No user action is required.

4.29.2 Current SQL Response Time

This metric contains the response time of the latest collection.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 5 Minutes

Data Source

Not available

User Action

No user action is required.

4.29.3 SQL Response Time (%)

SQL Response Time is the average elapsed time per execution of a representative set of SQL statements, relative to a baseline. It is expressed as a percentage.

This metric is not available in versions 8.1.7 and earlier.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	>	500	Not Defined	4	SQL response time is %value%% of baseline.

Data Source

PL/SQL packaged procedure `mgmt_response.get_metric_curs`

User Action

If the SQL Response Time is less than 100%, then SQL statements are taking less time to execute when compared to the baseline. Response Time greater than 100% indicates that the database is not performing well when compared to the baseline.

SQL Response Time is a percentage of the baseline, not a simple percentage. So, for example, 100% of baseline means the SQL Response Time is the same as the baseline. 200% of baseline means the SQL Response Time is two times slower than the baseline. 50% of baseline means SQL Response Time is two times faster than baseline. A warning threshold of 200% indicates that the database is two times slower than the baseline, while a critical threshold of 500% indicates the database is 5 times slower than the baseline.

Representative statements are selected when two V$SQL snapshots are taken. All calculations are based on the deltas between these two snapshots. First, the median elapsed_time/execution for all statements that were executed in the time interval between the two snapshots are calculated. Then all statements that have an elapsed_ time/execution > median elapsed_time/execution are taken, and the top 25 most frequently executed statements are displayed.

Pre-requisites for Monitoring SQL Response Time

Some tables and a PL/SQL package must be installed on the monitored database. This can be done by going to the database targets page and pressing the Configure button for your database. If a database has not been configured, the message "Not configured" will be displayed for SQL Response Time.

Configuring the Baseline

The baseline is configured on demand, automatically. The first time the agent calls the stored procedure to get the value of the metric, a snapshot of V$SQL is taken. The second time, another snapshot is taken. Then the representative statements are picked and stored in a table. The next time the agent requests the value of the metric, we are able to calculate and return the relative SQL response time.

Because of baseline configuration, there will be a delay between the time the database is configured and the value of the metric is displayed. During this period, the message of the collection status will be displayed for SQL Response Time.

Enterprise Manager will automatically configure the baseline against which SQL Response Time will be compared. However, in order for the SQL Response Time metric to be truly representative, the DBA must reconfigure the baseline at a time when the load on the database is typical.

To reconfigure the baseline, click on the link titled "Edit Reference Collection" located next to the SQL Response Time value on the Database Home Page. The SQL statements used for tracking the SQL Response Time and baseline values are displayed. Click **Reset Reference Collection**. This clears the list of statements and the baseline values. Enterprise Manager will then automatically reconfigure the baseline within minutes.

If the database was lightly loaded at the time the baseline was taken, then the metric can indicate that the database is performing poorly under typical load when such is not the case. In this case, the DBA must reset the baseline. If the DBA has never manually reset the baseline, then the metric value will not be representative.

4.30 Streams Metrics

The Streams metrics include the following:

4.30.1 Streams Apply Aborted

The Streams Apply Aborted metrics check for the Streams Apply processes.

4.30.1.1 Streams Apply Process Aborted

This metric detects when a Streams Apply process configured on this database aborts. This metric indicates a critical error.

Data Source

The DBA_APPLY view STATUS column indicates "ABORTED" if the apply process has aborted.

User Action

Obtain the exact error message in dba_apply, take the appropriate action for this error, then restart the apply process using dbms_apply_adm.start_apply.

Using the DBA_APPLY_ERROR view, identify the specific change record which encountered an error(MESSAGE_NUMBER) within a failed transaction and the complete error message (ERROR_MESSAGE). Detailed information about the transaction can be found using Enterprise Manager or by using the scripts described in the documentation Displaying Detailed Information about Apply Errors.

If DBA_APPLY error message is ORA-26714, then consider setting the 'DISABLE_ON_ERROR' apply parameter to 'N' to avoid aborting on future user errors.

4.30.1.2 Streams Apply Process Error

This metric indicates that the apply process encountered an error when it was applying a transaction.

Data Source

Not available.

User Action

Look at the contents of the error queue as well as dba_apply_error to determine the cause of the error. Once the errors are resolved, reexecute them using dbms_apply_adm.execute_error or dbms_apply_adm.execute_all_errors.

4.30.2 Streams Apply Coordinator Statistics

This metric shows statistics about the transactions processed by the coordinator process of each apply process. The **Total Number of Transactions Received** field shows the total number of transactions received by a coordinator process. The **Number of Transactions Assigned** field shows the total number of transactions assigned by a coordinator process to apply servers. The **Total Number of Transactions Applied** field shows the total number of transactions successfully applied by the apply process.

The values for an apply process are reset to zero if the apply process is restarted.

4.30.2.1 Total Number of Transactions Assigned

This metric shows statistics about the total number of transactions assigned by the coordinator process to apply servers since the apply process last started. For target version 10.1.0.x, the collection frequency for this metric is every 10 minutes.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The TOTAL_ASSIGNED column in the following query shows this metric for an apply process:

```
SELECT APPLY_NAME, TOTAL_RECEIVED, TOTAL_ASSIGNED, TOTAL_APPLIED
  FROM V$STREAMS_APPLY_COORDINATOR;
```

User Action

When an apply process is enabled, monitor this metric to ensure that the apply process assigning transactions to apply servers.

4.30.2.2 Rate of Transactions Applied (per Sec)

Rate (per second) at which transactions are applied by the apply process.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 5 Minutes

Data Source

Target database, gv%streams_apply_coordinator table

User Action

No user action is required.

4.30.2.3 Rate of Transactions Assigned (per Sec)

Rate (per second) at which transactions are assigned to the apply servers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 5 Minutes

Data Source

Target database, gv%streams_apply_coordinator table

User Action

No user action is required.

4.30.2.4 Rate of Transactions Received (per Sec)

Rate (per second) at which apply coordinator is receiving the transactions.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Target database, gv%streams_apply_coordinator table

User Action

No user action is required.

4.30.2.5 Total Number of Transactions Applied

This metric shows statistics about the total number of transactions applied by the apply process since the apply process last started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The TOTAL_APPLIED column in the following query shows this metric for an apply process:

```
SELECT APPLY_NAME, TOTAL_RECEIVED, TOTAL_ASSIGNED, TOTAL_APPLIED
  FROM V$STREAMS_APPLY_COORDINATOR;
```

User Action

When an apply process is enabled, monitor this metric to ensure that the apply process is applying transactions.

4.30.2.6 Total Number of Transactions Received

This metric shows statistics about the total number of transactions received by the coordinator process since the apply process last started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The TOTAL_RECEIVED column in the following query shows this metric for an apply process:

```
SELECT APPLY_NAME, TOTAL_RECEIVED, TOTAL_ASSIGNED, TOTAL_APPLIED
  FROM V$STREAMS_APPLY_COORDINATOR;
```

User Action

When an apply process is enabled, monitor this metric to ensure that the apply process is receiving transactions.

4.30.3 Streams Apply Errors

This metric collects information about Apply Errors and Error transactions.

4.30.3.1 Error Message

This metric is the error message of the error raised by the transaction.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is target database, dba_apply_error table.

User Action

No user action is required.

4.30.3.2 Error Number

This metric is the error code of the error raised by the transaction.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is target database, dba_apply_error table.

User Action

No user action is required.

4.30.3.3 Local Transaction ID

This metric is the local transaction ID for the error transaction.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is target database, dba_apply_error table.

User Action

No user action is required.

4.30.3.4 Message Count

This metric is the total number of events inside the error transaction.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is target database, dba_apply_error table.

User Action

No user action is required.

4.30.3.5 Source Transaction ID

This metric is the original transaction ID at the source database, for the error transaction.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is target database, dba_apply_error table.

User Action

No user action is required.

4.30.4 Streams Apply Queue - Buffered

The Streams Apply Queue - Buffered metrics show the current total number of messages in a buffered queue to be dequeued by each apply process and the total number of messages to be dequeued by each apply process that have spilled from memory into the persistent queue table.

4.30.4.1 Apply Queue - Cumulative Number of Messages

This metric is the cumulative total number of messages enqueued to the apply queue since the database last started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is target database, gv$buffered_queues, gv$buffered_ subscribers tables.

User Action

No user action is required.

4.30.4.2 Apply Queue - Cumulative Number of Spilled Messages

This metric is the current number of overflow messages spilled to disk from the buffered queue since the database last started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is target database, gv$buffered_queues, gv$buffered_ subscribers tables.

User Action

No user action is required.

4.30.4.3 Apply Queue - Number of Messages

This metric shows information about the number of messages in a buffered queue to be dequeued by the apply process. This number includes both messages in memory and messages spilled from memory.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The NUM_MSGS column in the following query shows this metric for an apply process:

```
SELECT APPLY_NAME, S.NUM_MSGS NUM_MSGS, Q.SPILL_MSGS SPILL_MSGS
  FROM DBA_APPLY A, V$BUFFERED_QUEUES Q,V$BUFFERED_SUBSCRIBERS S
  WHERE A.QUEUE_NAME = S.QUEUE_NAME AND A.QUEUE_OWNER = S.QUEUE_SCHEMA
  AND A.QUEUE_NAME = Q.QUEUE_NAME
  AND A.QUEUE_OWNER = Q.QUEUE_SCHEMA
  AND S.SUBSCRIBER_ADDRESS IS NULL;
```

User Action

When an apply process is enabled, monitor this metric to ensure that the apply process is dequeuing messages.

4.30.4.4 Apply Queue - Number of Spilled Messages

This metric shows information about the number of messages to be dequeued by the apply process that have spilled from memory to the queue spill table. Messages in a buffered queue can spill from memory into the queue spill table if they have been staged in the buffered queue for a period of time without being dequeued, or if there is not enough space in memory to hold all of the messages.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The SPILL_MSGS column in the following query shows this metric for an apply process:

```
SELECT APPLY_NAME, S.NUM_MSGS NUM_MSGS, Q.SPILL_MSGS SPILL_MSGS
  FROM DBA_APPLY A, V$BUFFERED_QUEUES Q,V$BUFFERED_SUBSCRIBERS S
  WHERE A.QUEUE_NAME = S.QUEUE_NAME AND A.QUEUE_OWNER = S.QUEUE_SCHEMA
  AND A.QUEUE_NAME = Q.QUEUE_NAME
  AND A.QUEUE_OWNER = Q.QUEUE_SCHEMA
  AND S.SUBSCRIBER_ADDRESS IS NULL;
```

User Action

The number of spilled messages should be kept as low as possible for the best performance. A high number of spilled messages might result in the following cases:

- There might be a problem with an apply process that applies messages captured by the capture process. When this happens, the number of messages can build in a queue because they are not being consumed. In this case, make sure the relevant apply processes are enabled, and correct any problems with these apply processes.
- The Streams pool may be too small to hold the captured messages. In this case, increase the size of the Streams pool. If the database is Oracle Database 10*g* release 2 (10.2) or higher, then you can configure Automatic Shared Memory Management to manage the size of the Streams pool automatically. Set the SGA_TARGET initialization parameter to use Automatic Shared Memory Management.

4.30.4.5 Streams Apply - (%) Cumulative Spilled Messages

This metric is the cumulative percentage of overflow messages spilled to disk from the buffered queue since the database last started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is target database, gv$buffered_queues, gv$buffered_ subscribers tables.

User Action

Apply Queue spilling usually indicates transactions are staying longer in memory. Either increase Streams Pool size and/or increase Apply Parallelism to speed up Apply processing.

4.30.4.6 Streams Apply - (%) Spilled Messages

This metric usually indicats that transactions are staying longer in memory.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	60	80	1	Spilled messages for Apply process [%APPLY_ NAME%] queue is %value% percent.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Apply Name" object.

If warning or critical threshold values are currently set for any "Apply Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Apply Name" object, use the Edit Thresholds page.

Data Source

Data source for this metric is target database, gv$buffered_queues, gv$buffered_ subscribers tables.

User Action

Either increase Streams Pool size and /or increase Apply Parallelism to speed up Apply processing.

4.30.5 Streams Apply Queue - Persistent

This metric shows the number of messages in a persistent queue in READY state and WAITING state for each apply process.

4.30.5.1 Number of Ready Messages

This metric shows the number of messages in a persistent queue that are ready to be dequeued by the apply process. The apply process has not yet attempted to dequeue these messages.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The data source includes the following data dictionary views: DBA_QUEUES, DBA_APPLY, and AQ$*queue_table_name*.

User Action

Monitor this metric to ensure that the apply process is dequeuing messages that are ready.

4.30.5.2 Streams Apply - (%) Messages in Waiting State

This metric shows the percentage of messages in a wait state.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	75	90	1	Messages waiting for Apply process [%APPLY_NAME%] queue is %value% percent.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Apply Name" and "Messages Delivery Mode" objects.

If warning or critical threshold values are currently set for any unique combination of "Apply Name" and "Messages Delivery Mode" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Apply Name" and "Messages Delivery Mode" objects, use the Edit Thresholds page.

Data Source

The data source for this metric is Target Database and Apply Queue.

User Action

No user action is required.

4.30.5.3 Number of Waiting Messages

This metric shows the number of messages in a persistent queue that are waiting to be dequeued by the apply process. The apply process has attempted to dequeue these messages at least once, and the apply process failed. The apply process might attempt to dequeue a waiting message again.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The data source includes the following data dictionary views: DBA_QUEUES, DBA_APPLY, and AQ$*queue_table_name*.

User Action

The messages in WAITING might have been enqueued with a delay attribute set. In this case, after the specified delay period is finished, the messages will be ready to dequeue.

4.30.6 Streams Apply Reader Statistics Metrics

The reader server for an apply process dequeues messages from the queue. The reader server computes dependencies between LCRs and assembles messages into transactions. The reader server then returns the assembled transactions to the coordinator, which assigns them to idle apply servers.

This metric shows the total number of messages dequeued by the reader server for the apply process since the last time the apply process was started.

4.30.6.1 Rate at Which Messages Are Being Dequeued (per Sec)

The reader server for an apply process dequeues messages from the queue. The reader server computes dependencies between LCRs and assembles messages into transactions. The reader server then returns the assembled transactions to the coordinator, which assigns them to idle apply servers.

This metric shows the rate at which messages are being dequeued by the reader server for the apply process since the last time the apply process was started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

For this metric, the data source is Target database, gv$streams_apply_reader view.

User Action

No user action is required.

4.30.6.2 Rate at Which Messages Are Getting Spilled (per Sec)

The reader server for an apply process dequeues messages from the queue. The reader server computes dependencies between LCRs and assembles messages into transactions. The reader server then returns the assembled transactions to the coordinator, which assigns them to idle apply servers.

This metric shows the rate at which message are getting spilled (per second) by the reader server for the apply process since the last time the apply process was started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Total number of spilled messages for Apply Process [%APPLY_ NAME%] is %value% .

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Apply Name" object.

If warning or critical threshold values are currently set for any "Apply Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Apply Name" object, use the Edit Thresholds page.

Data Source

For this metric, the data source is Target database, gv$streams_apply_reader view.

User Action

No user action is required.

4.30.6.3 Total Number of Messages Dequeued

The reader server for an apply process dequeues messages from the queue. The reader server computes dependencies between LCRs and assembles messages into transactions. The reader server then returns the assembled transactions to the coordinator, which assigns them to idle apply servers.

This metric shows the total number of messages dequeued by the reader server for the apply process since the last time the apply process was started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The TOTAL_MESSAGES_DEQUEUED column in the following query shows this metric for an apply process:

```
SELECT APPLY_NAME, TOTAL_MESSAGES_DEQUEUED FROM V$STREAMS_APPLY_READER;
```

User Action

When an apply process is enabled, monitor this metric to ensure that the apply process is dequeuing messages.

4.30.6.4 Total Number of Spilled Messages

The reader server for an apply process dequeues messages from the queue. The reader server computes dependencies between LCRs and assembles messages into transactions. The reader server then returns the assembled transactions to the coordinator, which assigns them to idle apply servers.

This metric shows the total number of messages spilled by the reader server for the apply process since the last time the apply process was started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

For this metric, the data source is Target database, gv$streams_apply_reader view.

User Action

No user action is required.

4.30.7 Streams Capture Aborted

The Streams Capture Aborted metrics check for the Streams Capture processes.

4.30.7.1 Streams Capture Process Aborted

This metric detects when a Streams Capture process configured on this database aborts. This metric indicates a critical error.

Data Source

Not available

User Action

Obtain the exact error message in dba_capture, take the appropriate action for this error, and restart the capture process using dbms_capture_adm.start_capture.

4.30.8 Streams Capture Message Statistics Metrics

The Streams Capture Message Statistics metrics show the number of messages captured and the number of messages enqueued by each capture process since the capture process last started.

The **Total Messages Captured** field shows the total number of redo entries passed by LogMiner to the capture process for detailed rule evaluation. A capture process converts a redo entry into a message and performs detailed rule evaluation on the message when capture process prefiltering cannot discard the redo entry. After detailed rule evaluation, the message is enqueued if it satisfies the capture process rule sets, or the message is discarded if it does not satisfy the capture process rule sets. The **Total Messages Enqueued** field shows the total number of messages enqueued. The number of captured messages captured can be higher than the number of enqueued messages.

The total messages enqueued includes enqueued logical change records (LCRs) that encapsulate data manipulation language (DML) and data definition language (DDL) changes. The total messages enqueued also includes messages that contain transaction control statements. These messages contain directives such as COMMIT and ROLLBACK. Therefore, the total messages enqueued is higher than the number of row changes and DDL changes enqueued by a capture process.

4.30.8.1 Message Capture Rate (per Sec)

This metric shows the number of messages captured by each capture process since the capture process last started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

For this metric, the data source is Target database, gv$streams_capture view.

User Action

No user action is required.

4.30.8.2 Messages Enqueue Rate (per Sec)

This metric shows the number of messages enqueued by each capture process since the capture process last started.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Not available

User Action

Specific to your site.

4.30.8.3 Total Messages Captured

This metric shows information about the number of redo entries passed by LogMiner to the capture process for detailed rule evaluation. A capture process converts a redo entry into a message and performs detailed rule evaluation on the message when capture process prefiltering cannot discard the change.

After detailed rule evaluation, the message is enqueued if it satisfies the capture process rule sets, or the message is discarded if it does not satisfy the capture process rule sets.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The TOTAL_MESSAGES_CAPTURED column in the following query shows this metric for a capture process:

```
SELECT CAPTURE_NAME, TOTAL_MESSAGES_CAPTURED, TOTAL_MESSAGES_ENQUEUED
  FROM V$STREAMS_CAPTURE;
```

User Action

When a capture process is enabled, monitor this metric to ensure that the capture process is scanning redo entries.

4.30.8.4 Total Messages Enqueued

This metric shows information about the number of messages enqueued by a capture process. The number of messages enqueued includes logical change records (LCRs) that encapsulate data manipulation language (DML) and data definition language (DDL) changes. The number of messages enqueued also includes messages that contain transaction control statements. These messages contain directives such as COMMIT and ROLLBACK. Therefore, the number of messages enqueued is higher than the number of row changes and DDL changes enqueued by a capture process.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The TOTAL_MESSAGES_ENQUEUED column in the following query shows this metric for a capture process:

```
SELECT CAPTURE_NAME, TOTAL_MESSAGES_CAPTURED, TOTAL_MESSAGES_ENQUEUED
  FROM V$STREAMS_CAPTURE;
```

User Action

When a capture process is enabled, monitor this metric to ensure that the capture process is enqueuing messages. If you know that there were source database changes that should be captured by the capture process, and the capture process is not capturing these changes, then there might be a problem with the rules used by the capture process.

4.30.9 Streams Capture Queue Statistics Metrics

This metric shows the current total number of messages in a buffered queue that were enqueued by each capture process and the total number of messages enqueued by each capture process that have spilled from memory into the queue spill table.

If queue publishers other than the capture process enqueue messages into a buffered queue, then the values shown can include messages from these other queue publishers.

4.30.9.1 Capture Queue - Cumulative Number of Messages

This metric shows information about the cumulative number of messages enqueued by a capture process in a buffered queue.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Not available

User Action

Specific to your site.

4.30.9.2 Capture Queue - Cumulative Number of Spilled Messages

This metric shows information about the cumulative number of spilled messages enqueued by a capture process in a buffered queue.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Not available

User Action

Specific to your site.

4.30.9.3 Capture Queue - Number of Messages

This metric shows information about the number of messages enqueued by a capture process in a buffered queue. This number includes both messages in memory and messages spilled from memory.

If queue publishers other than the capture process enqueue messages into a buffered queue, then the values shown can include messages from these other queue publishers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The NUM_MSGS column in the following query shows this metric for a capture process:

```
SELECT CAPTURE_NAME, P.NUM_MSGS NUM_MSGS, Q.SPILL_MSGS SPILL_MSGS
  FROM V$BUFFERED_PUBLISHERS P, V$BUFFERED_QUEUES Q, DBA_CAPTURE C
  WHERE C.QUEUE_NAME = P.QUEUE_NAME
    AND C.QUEUE_OWNER = P.QUEUE_SCHEMA
    AND C.QUEUE_NAME = Q.QUEUE_NAME
    AND C.QUEUE_OWNER = Q.QUEUE_SCHEMA
    AND C.CAPTURE_NAME = P.SENDER_NAME
    AND P.SENDER_ADDRESS IS NULL
    AND P.SENDER_PROTOCOL = 1;
```

User Action

When a capture process is enabled, monitor this metric to ensure that the capture process enqueuing messages.

4.30.9.4 Capture Queue - Number of Spilled Messages

This metric shows information about the number of messages enqueued by a capture process that have spilled from memory to the queue spill table. Messages in a buffered queue can spill from memory into the queue spill table if they have been staged in the buffered queue for a period of time without being dequeued, or if there is not enough space in memory to hold all of the messages.

If queue publishers other than the capture process enqueue messages into a buffered queue, then the values shown can include messages from these other queue publishers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The SPILL_MSGS column in the following query shows this metric for a capture process:

```
SELECT CAPTURE_NAME, P.NUM_MSGS NUM_MSGS, Q.SPILL_MSGS SPILL_MSGS
  FROM V$BUFFERED_PUBLISHERS P, V$BUFFERED_QUEUES Q, DBA_CAPTURE C
  WHERE C.QUEUE_NAME = P.QUEUE_NAME
    AND C.QUEUE_OWNER = P.QUEUE_SCHEMA
    AND C.QUEUE_NAME = Q.QUEUE_NAME
    AND C.QUEUE_OWNER = Q.QUEUE_SCHEMA
    AND C.CAPTURE_NAME = P.SENDER_NAME
    AND P.SENDER_ADDRESS IS NULL
    AND P.SENDER_PROTOCOL = 1;
```

User Action

The number of spilled messages should be kept as low as possible for the best performance. A high number of spilled messages can result in the following cases:

- There might be a problem with a propagation that propagates the messages captured by the capture process, or there might be a problem with an apply process that applies messages captured by the capture process. When this happens, the number of messages can build in a queue because they are not being consumed. In this case, make sure the relevant propagations and apply processes are enabled, and correct any problems with these propagations and apply processes.
- The Streams pool might be too small to hold the captured messages. In this case, increase the size of the Streams pool. If the database is Oracle Database 10*g* release 2 (10.2) or higher, then you can configure Automatic Shared Memory Management to manage the size of the Streams pool automatically. Set the SGA_TARGET initialization parameter to use Automatic Shared Memory Management.

4.30.9.5 Streams Capture - (%) Cumulative Spilled Messages

The percentage of Cumulative spilled messages indicate the messages are staying in memory longer. It can also indicate that the Propagation or Apply Process is slow to consume the enqueued messages.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Data source for this metric is Target database, gv$buffered_queues table.

User Action

No user action is required.

4.30.9.6 Streams Capture - (%) Spilled Messages

Queue spill indicates the messages are staying in memory longer. It can also indicate that the Propagation or Apply Process is slow to consume the enqueued messages.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	60	80	1	Spilled messages for Capture process %CAPTURE_ NAME% queue is %value% percent.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Capture Name" object.

If warning or critical threshold values are currently set for any "Capture Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Capture Name" object, use the Edit Thresholds page.

Data Source

Target database, gv$buffered_queues table

User Action

Increase Streams Pool Size to avoid queue spills.

4.30.10 Streams Latency and Throughput

The Streams Latency and Throughput metrics collect information about latency and throughtput for each capture, propagation and apply component in the database. Latency and throughput are improtant indicators for the overall performance of the streams path.

4.30.10.1 Streams - Latency (seconds)

High Latency indicates tha the components are slw.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	300	900	1	Latency for Streams %streams_process_type% Process %streams_process_name% is %value% seconds.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Streams Process Name" and "Streams Process Type" objects.

If warning or critical threshold values are currently set for any unique combination of "Streams Process Name" and "Streams Process Type" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Streams Process Name" and "Streams Process Type" objects, use the Edit Thresholds page.

Data Source

Data source for this metric is target database, gv$streams_capture, gv$propagation_sender, and gv$streams_apply_server views.

User Action

Identify and correct the least performing component in the streams configuration.

4.30.10.2 Streams - Throughput (message/sec)

This metric collects information about throughput for each capture, propagation and apply component in the database

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	1	Throughtput for Streams %streams_process_type% Process %streams_process_name% is %value% messages/sec.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Streams Process Name" and "Streams Process Type" objects.

If warning or critical threshold values are currently set for any unique combination of "Streams Process Name" and "Streams Process Type" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Streams Process Name" and "Streams Process Type" objects, use the Edit Thresholds page.

Data Source

Not available

User Action

Specific to your site

4.30.10.3 Total Messages

This metric collects the total number of messages for each capture, propagation and apply component in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Not available

User Action

Specific to your site.

4.30.11 Streams Pool Usage Metrics

The Streams Pool Usage metrics check for the memory usage of the Streams pool.

4.30.11.1 Streams Pool Full

This alert is generated when the memory usage of the Streams pool has exceeded the percentage specified by the STREAMS_POOL_USED_PCT metric. This alert can be

raised only if the database is not using Automatic Memory Management or Automatic Shared Memory Management.

Metric Summary for Database Control and Grid Control

This metric is available in target versions 11.1.0.x and 11.2.0.x

Data Source

Not available

User Action

If the currently running workload is typical, consider increasing the size of the Streams pool.

4.30.12 Streams Processes Count Metrics

This metric shows the total number of Streams capture processes, propagations, and apply processes at the local database. This metric also shows the number of capture processes, propagations, and apply processes that have encountered errors.

4.30.12.1 Number of Apply Processes Having Errors

This metric shows the number of apply processes that have encountered errors at the local database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The information in this metric is in the DBA_APPLY data dictionary view.

User Action

If an apply process has encountered errors, then correct the conditions that caused the errors.

4.30.12.2 Number of Capture Processes Having Errors

This metric shows the number of capture processes that have encountered errors at the local database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The information in this metric is in the DBA_CAPTURE data dictionary view.

User Action

If a capture process has encountered errors, then correct the conditions that caused the errors.

4.30.12.3 Number of Apply Processes

This metric shows the number of apply processes at the local database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The information in this metric is in the DBA_APPLY data dictionary view.

User Action

Use this metric to determine the total number of apply processes at the local database.

4.30.12.4 Number of Capture Processes

This metric shows the number of capture processes at the local database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The information in this metric is in the DBA_CAPTURE data dictionary view.

User Action

Use this metric to determine the total number of capture processes at the local database.

4.30.12.5 Number of Propagation Jobs

This metric shows the number of propagations at the local database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The information in this metric is in the DBA_PROPAGATION data dictionary view.

User Action

Use this metric to determine the total number of propagations at the local database.

4.30.12.6 Number of Propagations Having Errors

This metric shows the number of propagations that have encountered errors at the local database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

The information in this metric is in the DBA_PROPAGATION data dictionary view.

User Action

If a propagation has encountered errors, then correct the conditions that caused the errors.

4.30.12.7 Total Number of Propagation Errors

This metric provides the total number of propagation errors.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Target database, DBA_Propagation view

User Action

No user action is required.

4.30.13 Streams Processes Status Metrics

This metric collects the current status and number of errors for each capture, propagation and apply process in the database.

4.30.13.1 Streams Process Errors

This metric collects the number of errors for each capture, propagation and apply process in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	0	Not Defined	1	Stream component %streams_process_name% has %value% errors.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Streams Process Name" and "Streams Process Type" objects.

If warning or critical threshold values are currently set for any unique combination of "Streams Process Name" and "Streams Process Type" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Streams Process Name" and "Streams Process Type" objects, use the Edit Thresholds page.

Data Source

Not available

User Action

Specific to your site.

4.30.13.2 Streams Process Status

This metric collects the current status and number of errors for each capture, propagation, and apply process in the database.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	=	DISABLED	ABORTED	1	Status for Streams process %streams_process_name% is %streams_process_status%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Streams Process Name" and "Streams Process Type" objects.

If warning or critical threshold values are currently set for any unique combination of "Streams Process Name" and "Streams Process Type" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Streams Process Name" and "Streams Process Type" objects, use the Edit Thresholds page.

Data Source

Target database, DBA_CAPTURE, dba_propagation, dba_apply views

User Action

Analyze status change reason and enable the disabled / aborted component.

4.30.14 Streams Propagation Messages State Stats

This metric collects the number of messages in Ready and Waiting state for each Propagation process.

4.30.14.1 Number of Ready Messages

This metric collects the number of messages in Ready state for each Propagation process.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Target database, source and destination queues

User Action

No user action is required.

4.30.14.2 Number of Waiting Messages

This metric collects the number of messages in Waiting state for each Propagation process.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Target database, source and destination queues

User Action

No user action is required.

4.30.14.3 Streams Prop - (%) Messages in Waiting State

This metric collects the percentage of messages in Waiting state for each Propagation process.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	75	90	1	Messages waiting for %PROPAGATION_NAME% queue is %value% percent.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Propagation Name" and "Messages Delivery Mode" objects.

If warning or critical threshold values are currently set for any unique combination of "Propagation Name" and "Messages Delivery Mode" objects, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each unique combination of "Propagation Name" and "Messages Delivery Mode" objects, use the Edit Thresholds page.

Data Source

Target database, source and destination queues

User Action

No user action is required.

4.30.15 Streams Propagation - Queue Propagation Metrics

This metric collects propagation statistics in terms of number of messages and number of Kbytes propagated by each propagation process.

4.30.15.1 Message Propagation Rate (per Sec)

This metric collects propagation statistics in terms of the rate of messages propagated by each propagation process.

Metric Summary for Database Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Target database - DBA_PROPAGATION

User Action

No user action is required.

4.30.15.2 Rate of KBytes Propagated (per Sec)

This metric collects propagation statistics in terms of the rate of Kbytes propagated by each propagation process.

Metric Summary for Database Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Target database - DBA_PROPAGATION

User Action

No user action is required.

4.30.15.3 Total Number of KBytes Propagated

This metric collects propagation statistics in terms of total number of Kbytes propagated by each propagation process.

Metric Summary for Database Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Target database - DBA_PROPAGATION

User Action

No user action is required.

4.30.15.4 Total Number of Messages Propagated

This metric collects propagation statistics in terms of the total number of messages propagated by each propagation process.

Metric Summary for Database Control

The following table shows how often the metric's value is collected

Target Version	Collection Frequency
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes

Data Source

Target database - DBA_PROPAGATION

User Action

No user action is required.

4.30.16 Streams Propagation Aborted

The Streams Propagation Aborted metrics check for the Streams Propagation processes.

4.30.16.1 Streams Propagation Process Aborted

This metric detected when a Streams Propagation process configured on this database aborts. This alert indicates a critical error.

Data Source

Not Available

User Action

Obtain the exact error message in dba_queue_schedules, take the appropriate action for this error, and restart the propagation process using dbms_propagation_adm.start_propagation.

4.31 Suspended Session Metrics

This metric category contains the metrics that represent the number of resumable sessions that are suspended due to some correctable error.

4.31.1 Suspended Session Count

This metric represents the number of resumable sessions currently suspended in the database.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x	Every 5 Minutes	Not Uploaded	>	0	Not Defined	1	%value% session(s) are suspended.

Data Source

```
SELECT count(*)
  FROM v$resumable
  WHERE status = 'SUSPENDED' and enabled = 'YES'
```

User Action

Query the v$resumable view to see what the correctable errors are that are causing the suspension. The way to correct each error depends on the nature of the error.

4.32 System Metrics

The System metrics include the following:

- Section 4.32.1, "System Response Time Per Call"
- Section 4.32.2, "System Sessions Waiting"

4.32.1 System Response Time Per Call

The System Response Time Per Call metrics represent the system response time.

4.32.1.1 Response Time (centi-seconds per call)

This metric represents the average time taken for each call (both user calls and recursive calls) within the database. A change in this value indicates that either the workload has changed or that the database's ability to process the workload has changed because of either resource constraints or contention.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	1	Not Defined

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.32.2 System Sessions Waiting

The System Sessions Waiting metrics represent the number of sessions waiting.

4.32.2.1 Waiting Session Count

This metric represents the number of sessions waiting at the sample time.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	Not Defined	Not Defined	3	%value% sessions are waiting.

Data Source

```
SELECT count(*)
  FROM v$session_wait
  WHERE wait_time = 0 and event not in IdleEvents
```

See the Section 4.1, "Idle Events" for additional information.

User Action

When this count is high, the system is doing more waiting than anything else. Evaluate the various types of wait activity using the real-time and historical performance monitoring capabilities of Enterprise Manager.

4.33 Tablespaces Metrics

The Tablespaces metrics include the following:

- Section 4.33.1, "Tablespace Allocation Metrics"
- Section 4.33.2, "Tablespaces Full Metrics"
- Section 4.33.3, "Tablespaces Full (Dictionary Managed) Metrics"
- Section 4.33.4, "Tablespaces With Problem Segments Metrics"

4.33.1 Tablespace Allocation Metrics

The Tablespace Allocation metrics check the amount of space used and the amount of space allocated to each tablespace. The used space can then be compared to the allocated space to determine how much space is unused in the tablespace. This metric is not intended for alerts. Rather it is intended for reporting. Historical views of unused allocated free space can help DBAs to correctly size their tablespaces, eliminating wasted space.

4.33.1.1 Tablespace Allocated Space (MB)

The allocated space of a tablespace is the sum of the current size of its datafiles. A portion of this allocated space is used to store data while some may be free space. If segments are added to a tablespace, or if existing segments grow, they will use the allocated free space. The allocated free space is only available to segments within the tablespace. If, over time, the segments within a tablespace are not using this free space, then the allocated free space is being unused.

This metric calculates the space allocated for each tablespace. It is not intended to generate alerts. Rather it should be used in conjunction with the Allocated Space Used (MB) metric to produce an historical view of the amount of space being used and unused by each tablespace.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 7 Hours

Data Source

Tablespace Allocated Space (MB) is calculated by looping through the tablespace's data files and totalling the size of the data files.

User Action

Specific to you site.

4.33.1.2 Tablespace Used Space (MB)

The allocated space of a tablespace is the sum of the current size of its datafiles. Some of this allocated space is used to store data and some of it may be free space. If segments are added to a tablespace, or if existing segments grow, they will use the allocated free space. The allocated free space is only available to segments within the tablespace. If, over time, the segments within a tablespace are not using this free space, then the allocated free space is being wasted.

This metric calculates the space used for each tablespace. It is not intended to generate alerts. Rather it should be used in conjunction with the Tablespace Allocated Space (MB) metric to produce an historical view of the amount of space being used and unused by each tablespace.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 7 Hours

Data Source

Tablespace Used Space (MB) is Tablespace Allocated Space (MB) - Tablespace Allocated Free Space (MB) where:

- Tablespace Allocated Space (MB) is calculated by looping through the tablespace's data files and totaling the size of the data files.
- Tablespace Allocated Free Space (MB) is calculated by looping through the tablespace's data files and totaling the size of the free space in each data file.

User Action

Specific to you site.

4.33.2 Tablespaces Full Metrics

The Tablespaces Full metrics check for the amount of space used by each tablespace. The used space is then compared to the available free space to determine tablespace fullness. The available free space takes into account the maximum data file size as well as available disk space. This means that a tablespace will not be flagged as full if datafiles can extend and there is enough disk space available for them to extend.

4.33.2.1 Tablespace Free Space (MB)

As segments within a tablespace grow, the available free space decreases. If there is no longer any available free space, meaning datafiles have hit their maximum size or there is no more disk space, then the creation of new segments or the extension of existing segments will fail.

This metric checks for the total available free space in each tablespace. This metric is intended for larger tablespaces, where the Available Space Used (%) metric is less meaningful. If the available free space falls below the size specified in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 30 Minutes	After Every Sample	less than or equal to	Not Defined	Not Defined	1	Tablespace [%name%] has [%value% mbytes] free
10.2.0.x; 11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	less than or equal to	Not Defined	Not Defined	1	Not Defined

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Tablespace Name" object.

If warning or critical threshold values are currently set for any "Tablespace Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Tablespace Name" object, use the Edit Thresholds page.

Data Source

MaximumSize - Total Used Space where:

- TotalUsedSpace: total used space in MB of tablespace
- MaximumSize: Maximum size (in MB) of the tablespace. The maximum size is determined by looping through the tablespaces data files, as well as additional free space on the disk that would be available for the tablespace should a data file autoextend.

User Action

Perform one of the following:

- Increase the size of the tablespace by: Enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace, thus increasing the free space in this tablespace.
- Run the Segment Advisor on the tablespace.

4.33.2.2 Tablespace Space Used (%)

As segments within a tablespace grow, the available free space decreases. If there is no longer any available free space, meaning datafiles have hit their maximum size or there is no more disk space, then the creation of new segments or the extension of existing segments will fail.

This metric checks the Available Space Used (%) for each tablespace. If the percentage of used space is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 30 Minutes	After Every Sample	greater than or equal to	85	97	1	Tablespace [%name%] is [%value% percent] full

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 10 Minutes	Not Defined	After Every Sample	>=	85	97	1	Generated By Database Server

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Tablespace Name" object.

If warning or critical threshold values are currently set for any "Tablespace Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Tablespace Name" object, use the Edit Thresholds page.

Data Source

(TotalUsedSpace / MaximumSize) * 100 where:

- TotalUsedSpace: total used space in MB of tablespace
- MaximumSize: Maximum size (in MB) of the tablespace. The maximum size is determined by looping through the tablespace's data files.

For additional information about the data source, refer to the fullTbsp.pl Perl script located in the sysman/admin/scripts directory.

User Action

Perform one of the following:

- Increase the size of the tablespace by: Enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace, thus increasing the free space in this tablespace.
- Run the Segment Advisor on the tablespace.

4.33.3 Tablespaces Full (Dictionary Managed) Metrics

The Tablespaces Full (Dictionary Managed) metrics check for the amount of space used by each tablespace. The used space is then compared to the available free space to determine tablespace fullness. The available free space takes into account the maximum data file size as well as available disk space. This means that a tablespace will not be flagged as full if datafiles can extend and there is enough disk space available for them to extend.

4.33.3.1 Tablespace Free Space (MB) (Dictionary Managed)

As segments within a tablespace grow, the available free space decreases. If there is no longer any available free space, meaning datafiles have hit their maximum size or there is no more disk space, then the creation of new segments or the extension of existing segments will fail.

This metric checks for the total available free space in each tablespace. This metric is intended for larger tablespaces, where the Available Space Used (%) metric is less meaningful. If the available free space falls below the size specified in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 30 Minutes	After Every Sample	less than or equal to	Not Defined	Not Defined	1	Tablespace [%name%] has [%value% mbytes] free

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Tablespace Name" object.

If warning or critical threshold values are currently set for any "Tablespace Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Tablespace Name" object, use the Edit Thresholds page.

Data Source

MaximumSize - Total Used Space where:

- TotalUsedSpace: total used space in MB of tablespace
- MaximumSize: Maximum size (in MB) of the tablespace. The maximum size is determined by looping through the tablespaces data files, as well as additional free space on the disk that would be available for the tablespace should a data file autoextend.

User Action

Perform one of the following:

- Increase the size of the tablespace by: Enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace, thus increasing the free space in this tablespace.
- Run the Segment Advisor on the tablespace.

4.33.3.2 Tablespace Space Used (%) (Dictionary Managed)

As segments within a tablespace grow, the available free space decreases. If there is no longer any available free space, meaning datafiles have hit their maximum size or there is no more disk space, then the creation of new segments or the extension of existing segments will fail.

This metric checks the Available Space Used (%) for each tablespace. If the percentage of used space is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 30 Minutes	After Every Sample	greater than or equal to	85	97	1	Tablespace [%name%] is [%value% percent] full

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Tablespace Name" object.

If warning or critical threshold values are currently set for any "Tablespace Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Tablespace Name" object, use the Edit Thresholds page.

Data Source

Total Used Space / MaximumSize * 100 where:

- TotalUsedSpace: total used space in MB of tablespace
- MaximumSize: Maximum size (in MB) of the tablespace. The maximum size is determined by looping through the tablespaces data files.

User Action

Perform one of the following:

- Increase the size of the tablespace by: Enabling automatic extension for one of its existing data files, manually resizing one of its existing data files, or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace, thus increasing the free space in this tablespace.
- Run the Segment Advisor on the tablespace.

4.33.4 Tablespaces With Problem Segments Metrics

The Tablespaces With Problem Segments metrics check for the following:

- The largest chunk-free space in the tablespace. If any table, index, cluster, or rollback segment within the tablespace cannot allocate one additional extent, then an alert is generated.
- Whether any of the segments in the tablespace are approaching their maximum extents. If, for any segment, the maximum number of extents minus the number of existing extents is less than 2, then an alert is generated.

Only the tablespaces with problem segments are returned as results.

4.33.4.1 Segments Approaching Maximum Extents

Segments which are nearing the upper limit of maximum extents.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 24 Hours

Data Source

The first 10 segments names which are approaching their MaxExtent in the tablespace.

User Action

If possible, increase the value of the segments MAXEXTENTS storage parameter.

Otherwise, rebuild the segment with a larger extent size ensuring the extents within a segment are the same size by specifying STORAGE parameters where NEXT=INITIAL and PCTINCREASE = 0.

For segments that are linearly scanned, choose an extent size that is a multiple of the number of blocks read during each multiblock read. This will ensure that the Oracle multiblock read capability is used efficiently.

4.33.4.2 Segments Approaching Maximum Extents Count

This metric checks for segments which are nearing the upper limit of the number of maximum extents. If the number of segments is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	After Every Sample	>	0	Not Defined	1	%value% segments in %name% tablespace approaching max extents.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Tablespace Name" object.

If warning or critical threshold values are currently set for any "Tablespace Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Tablespace Name" object, use the Edit Thresholds page.

Data Source

Number of segments for which the maximum number of extents minus the number of existing extents is less than 2.

For additional information about the data source, refer to the problemTbsp.pl Perl script located in the sysman/admin/scripts directory.

User Action

If possible, increase the value of the segments MAXEXTENTS storage parameter.

Otherwise, rebuild the segment with a larger extent size ensuring the extents within a segment are the same size by using a locally managed tablespace. In the case of a dictionary managed tablespace, specify STORAGE parameters where NEXT=INITIAL and PCTINCREASE = 0.

4.33.4.3 Segments Not Able to Extend

Segments which cannot allocate an additional extent.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 24 Hours

Data Source

The first 10 segments names which cannot allocate an additional extent in the tablespace.

User Action

Perform one of the following:

- Increase the size of the tablespace by enabling automatic extension for one of its existing data files, manually resizing one of its existing data files. or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.

4.33.4.4 Segments Not Able to Extend Count

This metric checks for segments which cannot allocate an additional extent. If the number of segments is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 24 Hours	After Every Sample	>	0	Not Defined	1	%value% segments in %name% tablespace unable to extends.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Tablespace Name" object.

If warning or critical threshold values are currently set for any "Tablespace Name" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Tablespace Name" object, use the Edit Thresholds page.

Data Source

After checking for the largest chunk free space in the tablespace, this is the number of segments which cannot allocate an additional extent.

For additional information about the data source, refer to the problemTbsp.pl Perl script located in the sysman/admin/scripts directory.

User Action

Perform one of the following:

- Increase the size of the tablespace by enabling automatic extension for one of its existing data files, manually resizing one of its existing data files. or adding a new data file.
- If the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace.
- Relocate segments to another tablespace thus increasing the free space in this tablespace.

4.34 Throughput Metrics

The Throughput metrics represent rates of resource consumption, or throughput.

4.34.1 All Sessions

This metric represents the number of users logged on at the sampling time.

Metric Summary for Dabase Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes

Data Source

```
SELECT value
```

```
FROM v$sysstat
WHERE name = 'logons current';
```

User Action

No user action is necessary.

4.34.2 Average Active Sessions

This metric represents the average active sessions at a point in time. It is the number of sessions that are either working or waiting.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Data Source

Not available

User Action

No user action is required.

4.34.3 Average Synchronous Single-Block Read Latency (ms)

The average latency in milliseconds of a synchronous single-block read. Synchronous single-block reads are a reasonably accurate way of assessing the performance of the storage subsystem. High latencies are typically caused by a high I/O request load. Excessively high CPU load can also cause the latencies to increase.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Data Source

v$sysmetric

User Action

First, verify that your storage subsystem is not operating with component failures, for example, disk, network, or HBA failures. If no issues are found, consider upgrading your storage subsystem.

4.34.4 BG Checkpoints (per second)

This metric represents the BG checkpoints per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

Not available

User Action

Specific to your site.

4.34.5 Branch Node Splits (per second)

Number of times per second an index branch block was split because of the insertion of an additional value.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

branch node splits / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.6 Branch Node Splits (per transaction)

Number of times per transaction an index branch block was split because of the insertion of an additional value.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

branch node splits / transaction

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.7 Consistent Read Blocks Created (per second)

This metric represents the number of current blocks per second cloned to create consistent read (CR) blocks.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

CR blocks created / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.8 Consistent Read Blocks Created (per transaction)

This metric represents the number of current blocks per transaction cloned to create consistent read (CR) blocks.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

CR blocks created / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.9 Consistent Read Changes (per second)

This metric represents the number of times per second a user process has applied rollback entries to perform a consistent read on the block.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

consistent changes / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.10 Consistent Read Changes (per transaction)

This metric represents the number of times per transaction a user process has applied rollback entries to perform a consistent read on the block.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

consistent changes / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.11 Consistent Read Gets (per second)

This metric represents the number of times per second a consistent read was requested for a block.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

consistent gets / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.12 Consistent Read Gets (per transaction)

This metric represents the number of times per transaction a consistent read was requested for a block.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

consistent gets / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.13 Consistent Read Undo Records Applied (per second)

This metric represents the number of undo records applied for consistent read per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

current blocks converted for CR / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.14 Consistent Read Undo Records Applied (per transaction)

This metric represents the consistent read undo records applied per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

Not available

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.15 Cumulative Logons (per second)

This metric represents the number of logons per second during the sample period.

This test checks the number of logons that occurred per second during the sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	100	Not Defined	2	Cumulative logon rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>=	100	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	100	Not Defined	2	Cumulative logon rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>=	100	Not Defined	2	Generated By Database Server

Data Source

DeltaLogons / Seconds where:

- DeltaLogons: difference in 'select value from v$sysstat where name='logons cumulative'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

A high logon rate may indicate that an application is inefficiently accessing the database. Database logon's are a costly operation. If an application is performing a logon for every SQL access, that application will experience poor performance as well as affect the performance of other applications on the database. If there is a high logon rate, try to identify the application that is performing the logons to determine if it could be redesigned such that session connections could be pooled, reused, or shared.

4.34.16 Cumulative Logons (per transaction)

This metric represents the number of logons per transaction during the sample period.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the number of logons that occurred per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Cumulataive logon rate is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Cumulative logon rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaLogons / Transactions where:

- DeltaLogons: difference in 'select value from v$sysstat where name='logons cumulative'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

A high logon rate may indicate that an application is inefficiently accessing the database. Database logon's are a costly operation. If an application is performing a logon for every SQL access, that application will experience poor performance as well as affect the performance of other applications on the database. If there is a high logon rate try to identify the application that is performing the logons to determine if it could be redesigned such that session connections could be pooled, reused or shared.

4.34.17 Database Block Changes (per second)

This metric represents the total number of changes per second that were part of an update or delete operation that were made to all blocks in the SGA.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

db block changes / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.18 Database Block Changes (per transaction)

This metric represents the total number of changes per transaction that were part of an update or delete operation that were made to all blocks in the SGA.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

db block changes / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.19 Database Block Gets (per second)

This metric represents the number of times per second a current block was requested.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

db block gets / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.20 Database Block Gets (per transaction)

This metric represents the number of times per transaction a current block was requested.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

db block gets / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.21 Database Time (centiseconds per second)

This metic denotes the database time.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Data Source

Not available

User Action

Specific to your site.

4.34.22 DBWR Checkpoints (per second)

This metric represents the number of times, per second, during this sample period DBWn was asked to scan the cache and write all blocks marked for a checkpoint.

The database writer process (DBWn) writes the contents of buffers to datafiles. The DBWn processes are responsible for writing modified (dirty) buffers in the database buffer cache to disk.

When a buffer in the database buffer cache is modified, it is marked dirty. The primary job of the DBWn process is to keep the buffer cache clean by writing dirty buffers to disk. As user processes dirty buffers, the number of free buffers diminishes. If the number of free buffers drops too low, user processes that must read blocks from disk into the cache are not able to find free buffers. DBWn manages the buffer cache so that user processes can always find free buffers.

When the Oracle Server process cannot find a clean reusable buffer after scanning a threshold of buffers, it signals DBWn to write. When this request to make free buffers is received, DBWn writes the least recently used (LRU) buffers to disk. By writing the least recently used dirty buffers to disk, DBWn improves the performance of finding free buffers while keeping recently used buffers resident in memory. For example, blocks that are part of frequently accessed small tables or indexes are kept in the cache so that they do not need to be read in again from disk. The LRU algorithm keeps more

frequently accessed blocks in the buffer cache so that when a buffer is written to disk, it is unlikely to contain data that may be useful soon.

Additionally, DBWn periodically writes buffers to advance the checkpoint that is the position in the redo log from which crash or instance recovery would need to begin.

This test checks the number of times DBWR was asked to advance the checkpoint. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	DBWR checkpoint rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	DBWR checkpoint rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaCheckpoints / Seconds where:

- DeltaCheckpoints: difference in 'select value from v$sysstat where name='DBWR checkpoints'' between sample end and start
- Seconds: number of seconds in sample period

User Action

A checkpoint tells the DBWR to write out modified buffers to disk. This write operation is different from the make free request in that the modified buffers are not marked as free by the DBWR process. Dirty buffers may also be written to disk at this time and freed.

The write size is dictated by the _db_block_checkpoint_batch parameter. If writing, and subsequently waiting for checkpoints to complete is a problem, the checkpoint completed event displays in the Top Waits page sorted by Time Waited or the Sessions Waiting for this Event page.

If the database is often waiting for checkpoints to complete you may want to increase the time between checkpoints by checking the init.ora parameter db_block_checkpoint_batch: select name, value, is default from v$parameter where name = db_block_checkpoint_batch. The value should be large enough to take advantage of parallel writes. The DBWR uses a write batch that is calculated like this: (db_files * db_file_simultaneous_writes)/2 The write_batch is also limited by two other factors:

- A port specific limit on the numbers of I/Os (compile time constant).
- 1/4 of the number of buffers in the SGA.

The db_block_checkpoint_batch is always smaller or equal to the _db_block_write_batch. You can also consider enabling the check point process.

4.34.23 Enqueue Deadlocks (per second)

This metric represents the number of times per second that a process detected a potential deadlock when exchanging two buffers and raised an internal, restartable error.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

enqueue deadlocks / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.24 Enqueue Deadlocks (per transaction)

This metric represents the number of times per transaction that a process detected a potential deadlock when exchanging two buffers and raised an internal, restartable error.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

enqueue deadlocks / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.25 Enqueue Requests (per second)

This metric represents the total number of table or row locks acquired per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

enqueue requests / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.26 Enqueue Requests (per transaction)

This metric represents the total number of table or row locks acquired per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

enqueue requests / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.27 Enqueue Timeout (per second)

This metric represents the total number of table and row locks (acquired and converted) per second that time out before they could complete.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

enqueue timeouts / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.28 Enqueue Timeout (per transaction)

This metric represents the total number of table and row locks (acquired and converted) per transaction that timed out before they could complete.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

enqueue timeouts / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.29 Enqueue Waits (per second)

This metric represents the total number of waits per second that occurred during an enqueue convert or get because the enqueue get was deferred.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

enqueue waits / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.30 Enqueue Waits (per transaction)

This metric represents the total number of waits per transaction that occurred during an enqueue convert or get because the enqueue get was deferred.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

enqueue waits / transaction

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.31 Executes (per second)

This metric represents the rate of SQL command executions over the sampling interval.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaExecutions / Seconds where:

- DeltaExecutions: difference in 'select value from v$sysstat where name='execute count'' between end and start of sample period.
- Seconds: number of seconds in sample period

User Action

No user action is necessary.

4.34.32 Executes Performed without Parses (%)

This metric represents the percentage of statement executions that do not require a corresponding parse. A perfect system would parse all statements once and then execute the parsed statement over and over without reparsing. This ratio provides an indication as to how often the application is parsing statements as compared to their overall execution rate. A higher number is better.

This test checks the percentage of executes that do not require parses. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Only %value%% of executes are performed without parses.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Only %value%% of executes are performed without parses.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

((DeltaExecuteCount - (DeltaParseCountTotal)) / DeltaExecuteCount) * 100 where:

- DeltaParseCountTotal: difference in 'select value from v$sysstat where name='parse count (total)'' between sample end and start
- DeltaExecuteCount: difference in 'select value from v$sysstat where name='execute count'' between sample end and start

User Action

An execute to parse ratio of less than 70% indicates that the application may be parsing statements more often than it should. Reparsing the statement, even if it is a soft parse, requires a network round trip from the application to the database, as well as requiring the processing time to locate the previously compiled statement in the cache. Reducing network round trips and unnecessary processing improves application performance.

Use the Top Sessions page sorted by Parses to identify the sessions responsible for the bulk of the parse activity within the database. Start with these sessions to determine whether the application could be modified to make more efficient use of its cursors.

4.34.33 Full Index Scans (per second)

This metric represents the number of fast full index scans per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

index fast full scans (full) / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.34 Full Index Scans (per transaction)

This metric represents the number of fast full index scans per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

index fast full scans (full) / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.35 Hard Parses (per second)

This metric represents the number of hard parses per second during this sample period. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement.

Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations that will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps, which the optimizer will evaluate when generating an execution plan for the cursor.

This test checks the number of parses of statements that were not already in the cache. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Hard parse rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Hard parse rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaParses / Seconds where:

- DeltaParses: difference in 'select value from v$sysstat where name='parse count (hard)'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

If there appears to be excessive time spent parsing, evaluate SQL statements to determine those that can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some

combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The Top Sessions page sorted by Hard Parses will show you which sessions are incurring the most hard parses. Hard parses happen when the server parses a query and cannot find an exact match for the query in the library cache. Hard parses can be avoided by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this page may lead you to the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

4.34.36 Hard Parses (per transaction)

This metric represents the number of hard parses per second during this sample period. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement.

Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the number of hard parses per second during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Hard parse rate is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Hard parse rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaParses / Transactions where:

- DeltaParses: difference in 'select value from v$sysstat where name='parse count (hard)'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

If there appears to be excessive time spent parsing, evaluate SQL statements to determine which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of

the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The Top Sessions page sorted by Hard Parses will show you which sessions are incurring the most hard parses. Hard parses happen when the server parses a query and cannot find an exact match for the query in the library cache. Hard parses can be avoided by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this page may lead you to the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

4.34.37 I/O Megabytes (per second)

The total I/O throughput of the database for both reads and writes in megabytes per second. A very high value indicates that the database is generating a significant volume of I/O data.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Data Source

v$sysmetric

User Action

A high I/O throughput value is not in itself problematic. However, if high I/O latencies (for example, Synchronous Single-Block Read Latencies are causing a performance problem, then reducing the total I/O throughput may help. The source of the I/O throughput can be investigated by viewing a breakdown by either Component or Resource Consumer Group.

4.34.38 I/O Requests (per second)

This metric represents the total rate of I/O read and write requests for the database.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Data Source

v$sysmetric

User Action

A high I/O request rate is not in itself problematic. However, if high I/O latencies (for example, Synchronous Single-Block Read Latencies are causing a performance problem, then reducing the total I/O request rate may help. The source of the I/O requests can be investigated by viewing a breakdown by either Component or Resource Consumer Group.

4.34.39 Leaf Node Splits (per second)

Number of times per second an index leaf node was split because of the insertion of an additional value.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

leaf node splits / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.40 Leaf Node Splits (per transaction)

Number of times per transaction an index leaf node was split because of the insertion of an additional value.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

leaf node splits / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.41 Network Bytes (per second)

This metric represents the total number of bytes sent and received through the SQL Net layer to and from the database.

This test checks the network read/write per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the Number of Occurrences parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Bytes transmitted via SQL*Net is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Bytes transmitted via SQL*Net is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

(DeltaBytesFromClient+DeltaBytesFromDblink+DeltaBytesToClient+DeltaBytesToDblink) / Seconds where:

- Delta Bytes From Client: difference in 'select s.value from v$sysstat s, visitation n where n.name='bytes received via SQL*Net from client' and n.statistic#=s.statistic#' between end and start of sample period
- DeltaBytesFromClient: difference in 'select s.value from v$sysstat s, v$statname n where n.name='bytes received via SQL*Net from dblink' and n.statistic#=s.statistic#' between end and start of sample period
- DeltaBytesFromClient: difference in 'select s.value from v$sysstat s, v$statname n where n.name='bytes sent via SQL*Net to client' and n.statistic#=s.statistic#' between end and start of sample period
- DeltaBytesFromClient: difference in 'select s.value from v$sysstat s, v$statname n where n.name='bytes sent via SQL*Net to dblink' and n.statistic#=s.statistic#' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

This metric represents the amount of network traffic in and out of the database. This number may only be useful when compared to historical levels to understand network traffic usage related to a specific database.

4.34.42 Number of Transactions (per second)

This metric represents the total number of commits and rollbacks performed during this sample period.

This test checks the number of commits and rollbacks performed during sample period. If the value is greater than or equal to the threshold values specified by the

threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Transaction rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>=	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Transaction rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>=	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaCommits + DeltaRollbacks where:

- DeltaCommits: difference of 'select value from v$sysstat where name='user commits'' between sample end and start

- DeltaRollbacks: difference of 'select value from v$sysstat where name='user rollbacks'' between sample end and start

User Action

This statistic is an indication of how much work is being accomplished within the database. A spike in the transaction rate may not necessarily be bad. If response times stay close to normal, it means your system can handle the added load. Actually, a drop in transaction rates and an increase in response time may be indicators of problems. Depending upon the application, transaction loads may vary widely across different times of the day.

4.34.43 Open Cursors (per second)

This metric represents the total number of cursors opened per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

opened cursors cumulative / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.44 Open Cursors (per transaction)

This metric represents the total number of cursors opened per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

opened cursors cumulative / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.45 Parse Failure Count (per second)

This metric represents the total number of parse failures per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

parse count (failures) / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.46 Parse Failure Count (per transaction)

This metric represents the total number of parse failures per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

parse count (failures) / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.47 Physical Reads (per second)

This metric represents the number of data blocks read from disk per second during this sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then searches the disk if it is not already in memory. Reading data blocks from disk is much more inefficient than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization.

This test checks the data blocks read from disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Physical reads are %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Physical reads are %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaPhysicalReads / Seconds where:

- DeltaPhysicalReads: difference in 'select s.value from v$sysstat s, v$statname n where n.name='physical reads' and n.statistic#=s.statistic#' between sample end and start
- Seconds: number of seconds in sample period

User Action

Block reads are inevitable so the aim should be to minimize unnecessary IO. This is best achieved by good application design and efficient execution plans. Changes to execution plans can yield profound changes in performance. Tweaking at system level usually only achieves percentage gains.

To view I/O on a per session basis to determine which sessions are responsible for your physical reads, you should visit the Top Sessions page sorted by Physical Reads. This approach allows you to identify problematic sessions and then drill down to their current SQL statement and perform tuning from there.

To identify the SQL that is responsible for the largest portion of physical reads, visit the Top SQL page sorted by Physical Reads. This page allows you to quickly determine which SQL statements are the causing your I/O activity. From this display you can view the full text of the SQL statement.

The difference between the two methods for identifying problematic SQL is that the Top Sessions view displays sessions that are performing the most physical reads at the moment. The Top SQL view displays the SQL statements that are still in the SQL cache that have performed the most I/O over their lifetime. A SQL statement could show up in the Top SQL view that is not currently being executed.

If the SQL statements are properly tuned and optimized, consider the following suggestions. A larger buffer cache may help - test this by actually increasing DB_BLOCK_BUFFERS. Do not use DB_BLOCK_LRU_EXTENDED_STATISTICS, as this may introduce other performance issues. Never increase the SGA size if it may induce additional paging or swapping on the system.

A less obvious issue which can affect the I/Orates is how well data is clustered physically. For example, assume that you frequently fetch rows from a table where a column is between two values via an index scan. If there are 100 rows in each index

block then the two extremes are: 1.Each of the table rows is in a different physical block (100 blocks need to be read for each index block). 2.The table rows are all located in the few adjacent blocks (a handful of blocks need to be read for each index block).

Pre-sorting or reorganizing data can improve this situation in severe situations as well.

4.34.48 Physical Reads (per transaction)

This metric represents the number of disk reads per transaction during the sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then goes to disk if it is not in memory already. Reading data blocks from disk is much more expensive than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the data blocks read from disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Physical reads are %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Physical reads are %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaReads / Transactions where:

- DeltaReads: difference in 'select value from v$sysstat where name='physical reads'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

Block reads are inevitable so the aim should be to minimize unnecessary IO. This is best achieved by good application design and efficient execution plans. Changes to execution plans can yield orders of magnitude changes in performance. Tweaking at system level usually only achieves percentage gains.

To identify the SQL that is responsible for the largest portion of physical reads, visit the Top SQL page sorted by Physical Reads. This view will allow you to quickly determine which SQL statements are causing the I/O activity. From this display you can view the full text of the SQL statement.

To view I/O on a per session basis to determine which sessions are responsible for your physical reads, you can visit the Top Sessions page sorted by Physical Reads. This approach allows you to identify problematic sessions and then drill down to their current SQL statement to perform tuning.

If the SQL statements are properly tuned and optimized the following suggestions may help. A larger buffer cache may help - test this by actually increasing DB_ BLOCK_BUFFERS and not by using DB_BLOCK_LRU_EXTENDED_STATISTICS. Never increase the SGA size if it will induce additional paging or swapping on the system.

A less obvious issue which can affect the I/Orates is how well data is clustered physically. For example, assume that you frequently fetch rows from a table where a column is between two values via an index scan. If there are 100 rows in each index block then the two extremes are: 1. Each of the table rows is in a different physical block (100 blocks need to be read for each index block). 2. The table rows are all located in the few adjacent blocks (a handful of blocks need to be read for each index block).

Pre-sorting or reorganizing data can help to tackle this in severe situations as well.

4.34.49 Physical Reads Direct (per second)

This metric represents the number of direct physical reads per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

physical reads direct / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.50 Physical Reads Direct (per transaction)

This metric represents the number of direct physical reads per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

physical reads direct / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.51 Physical Reads Direct Lobs (per second)

This metric represents the number of direct large object (LOB) physical reads per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

physical reads direct (lob) / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.52 Physical Reads Direct Lobs (per transaction)

This metric represents the number of direct large object (LOB) physical reads per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

physical reads direct (lob) / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.53 Physical Writes (per second)

This metric represents the number of disk writes per second during the sample period. This statistic represents the rate of database blocks written from the SGA buffer cached to disk by the DBWR background process, and from the PGA by processes performing direct writes.

This test checks the data blocks written disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Physical writes are %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Physical writes are %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaWrites / Seconds where:

- DeltaWrites: difference in 'select value from v$sysstat where name='physical writes" between end and start of sample period
- Seconds: number of seconds in sample period

User Action

Because this statistic shows both DBWR writes as well as direct writes by sessions, you should view the physical writes directly to determine where the write activity is actually occurring. If the physical writes direct value comprises a large portion of the writes, then there are probably many sorts or writes to temporary tablespaces occurring.

If the majority of the writes are not direct, they are being performed by the DBWR writes process. This is only be a problem if log writer or redo waits are showing up in the Sessions Waiting for this Event page or the Top Waits page sorted by Time Waited.

4.34.54 Physical Writes (per transaction)

This metric represents the number of disk writes per transaction during the sample period.

The value of this statistic is zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name is a better indicator of current performance.

This test checks the data blocks written disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Physical writes are %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Physical writes are %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaWrites / Transactions where:

- DeltaWrites: difference in 'select value from v$sysstat where name='physical writes'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

Because this statistic shows both DBWR writes as well as direct writes by sessions, you should view the physical writes directly to determine where the write activity is really occurring. If the physical writes direct value comprises a large portion of the writes, then there are likely many sorts or writes to temporary tablespaces that are occurring.

If the majority of the writes are not direct, they are being performed by the DBWR writes process. This will typically only be a problem if log writer or redo waits are showing up in the Sessions Waiting for this Event page or the Top Waits page sorted by Time Waited.

4.34.55 Physical Writes Direct (per second)

This metric represents the number of direct physical writes per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

physical writes direct / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central on the Database Home page.

4.34.56 Physical Writes Direct (per transaction)

This metric represents the number of direct physical writes per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

physical writes direct / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.57 Physical Writes Direct Lobs (per second)

This metric represents the number of direct large object (LOB) physical writes per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

physical writes direct (lob) / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.58 Physical Writes Direct Lobs (per transaction)

This metric represents the number of direct large object (LOB) physical writes per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

physical writes direct (lob) / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.59 Recursive Calls (per second)

This metric represents the number of recursive calls, per second during the sample period.

Sometimes, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:

- When data dictionary information is not available in the data dictionary cache and must be retrieved from disk
- In the firing of database triggers
- In the execution of DDL statements
- In the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- In the enforcement of referential integrity constraints

This test checks the number of recursive SQL calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Recursive call rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Recursive call rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaRecursiveCalls / Seconds where:

- DeltaRecursiveCalls: difference in 'select value from v$sysstat where name='recursive calls'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

If the Oracle Server appears to be making excessive recursive calls while your application is running, determine what activity is causing these recursive calls. If you determine that the recursive calls are caused by dynamic extension, either reduce the frequency of extension by allocating larger extents or, if you are using Oracle8*i*, considering taking advantage of locally managed tablespaces.

4.34.60 Recursive Calls (per transaction)

This metric represents the number of recursive calls, per second during the sample period.

Sometimes, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:

- When data dictionary information is not available in the data dictionary cache and must be retrieved from disk
- In the firing of database triggers
- In the execution of DDL statements

- In the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- In the enforcement of referential integrity constraints

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the number of calls that result in changes to internal tables. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Recursive call rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Recursive rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaRecursiveCalls / Transactions where:

- DeltaRecursiveCalls: difference in 'select value from v$sysstat where name='recursive calls'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

If the Oracle Server appears to be making excessive recursive calls while your application is running, determine what activity is causing these recursive calls. If you determine that the recursive calls are caused by dynamic extension, either reduce the frequency of extension by allocating larger extents or, if you are using Oracle8*i*, considering taking advantage of locally managed tablespaces.

4.34.61 Redo Generated (per second)

This metric represents the amount of redo, in bytes, generated per second during this sample period.

The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries can be used for database recovery if necessary.

This test checks the amount of redo in bytes generated per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Redo generated is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Redo generated is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaRedoSize / Seconds where:

- DeltaRedoSize: difference in 'select value from v$sysstat where name='redo size'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when redo entries are buffered to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer should waiting be a problem. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

4.34.62 Redo Generated (per transaction)

This metric represents the amount of redo, in bytes, generated per transaction during this sample period.

The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries are used for database recovery, if necessary.

The value of this statistic is zero if there have been no write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the amount of redo in bytes generated per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Redo generated is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Redo generated is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaRedoSize / DeltaTransactions where:

- DeltaRedoSize: difference in 'select value from v$sysstat where name='redo size'' between end and start of sample period
- Transactions: difference in 'select value from v$sysstat where name = 'user commits'' between end and start of sample period

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when buffering redo entries to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer should waiting be a problem. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

4.34.63 Redo Writes (per second)

This metric represents the number redo write operations per second during this sample period.

The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries can be used for database recovery if necessary.

The log writer processes (LGWR) is responsible for redo log buffer management; that is, writing the redo log buffer to a redo log file on disk.

This test checks the number of writes by LGWR to the redo log files per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Redo write rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Redo write rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaRedoWrites / Seconds where:

- DeltaRedoWrites: difference in 'select value from v$sysstat where name='redo writes'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when redo entries are buffered to the redo log file.

Should waiting be a problem, consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer. Redo log entries contain a record

of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

4.34.64 Redo Writes (per transaction)

This metric represents the number of redo write operations per second during this sample period.

The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries are used for database recovery, if necessary.

The log writer process (LGWR) is responsible for redo log buffer management; that is, writing the redo log buffer to a redo log file on disk.

This test checks the number of writes by LGWR to the redo log files per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Redo write rate is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Redo write rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaRedoWrites /(DeltaCommits+DeltaRollbacks) where:

- DeltaRedoWrites: difference in 'select s.value from v$sysstat s, v$statname n where n.name='redo writes' and n.statistic#=s.statistic#' between sample end and start
- DeltaCommits: difference in 'select s.value from v$sysstat s, v$statname n where n.name='user commits' and n.statistic#=s.statistic#' between sample end and sample start
- DeltaRollbacks: difference in 'select s.value from v$sysstat s, v$statname n where n.name='user commits' and n.statistic#=s.statistic#' between sample end and sample start

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when buffering redo entries to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer should waiting be a problem. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

4.34.65 Rows Processed (per sort)

This metric represents the average number of rows per sort during this sample period.

This test checks the average number of rows per sort during sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Average sort size is %value% rows.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Average sort size is %value% rows.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

(DeltaSortRows / (DeltaDiskSorts + DeltaMemorySorts)) * 100 where:

- DeltaSortRows: difference in 'select value from v$sysstat where name='sorts (rows)'' between sample end and start
- DeltaMemorySorts: difference in 'select value from v$sysstat where name='sorts (memory)'' between sample end and start
- DeltaDiskSorts: difference in 'select value from v$sysstat where name='sorts (disk)'' between sample end and start

User Action

This statistic displays the average number of rows that are being processed per sort. The size provides information about the sort size of the database. This can help you to determine the SORT_AREA_SIZE appropriately. If the rows per sort are high, you should investigate the sessions and SQL performing the most sorts to see if those SQL statements can be tuned to reduce the size of the sort sample set.

The sessions that are performing the most sorts should be identified, such that the SQL they are executing can be further identified. The sort area sizes for the database may be sized correctly and the application SQL may be performing unwanted or excessive sorts. The sessions performing the most sorts are available through the Top Sessions page sorted by Disk Sorts.

Further drilldown into the session performing the most disk sorts with the Current SQL page displays the SQL statement responsible for the disk sorts.

The Top SQL page sorted by Sorts provides a mechanism to quickly display the SQL statements in the cache presented in sorted order by their number of sort operations. This is an alternative to viewing the sort of current sessions. It allows you to view sort activity via SQL statements and contains cumulative statistics for all executions of that statement.

If excessive sorts are taking place on disk and the queries are correct, consider increasing the SORT_AREA_SIZE initialization parameter to increase the size of the sort area. A larger sort area allows the Oracle Server to keep sorts in memory, reducing the number of I/O operations required to do an equivalent amount of work using the current sort area size.

4.34.66 Scans on Long Tables (per second)

This metric represents the number of long table scans per second during sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.

This test checks the long table scans per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Rate of scans on long tables is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Rate of scans on long tables is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaScans / Seconds where:

- DeltaScans: difference in 'select value from v$sysstat where name='table scans (long tables)'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

A table scan means that the entire table is being scanned record by record in order to satisfy the query. For small tables that can easily be read into and kept in the buffer cache this may be advantageous. But for larger tables this will force a lot of physical reads and potentially push other needed buffers out of the cache. SQL statements with large physical read and logical read counts are candidates for table scans. They can be identified either through the Top SQL page sorted by Physical Reads, or through the Top Sessions page sorted by Physical Reads, with a drilldown to the current SQL for a session.

4.34.67 Scans on Long Tables (per transaction)

This metric represents the number of long table scans per transaction during sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the number of long table scans per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Rate of scans on long tables is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Rate of scans on long tables is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaScans / Transactions where:

- DeltaScans: difference in 'select value from v$sysstat where name='table scans (long tables)'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

A table scan means that the entire table is being scanned record by record in order to satisfy the query. For small tables that can easily be read into and kept in the buffer cache this may be advantageous. But for larger tables this will force a lot of physical reads and potentially push other needed buffers out of the cache. SQL statements with large physical read and logical read counts are candidates for table scans. They can be identified either through the Top SQL page sorted by Physical Reads, or through the Top Sessions page sorted by Physical Reads, with a drilldown to the current SQL for a session.

4.34.68 Session Logical Reads (per second)

This metric represents the number of logical reads per second during the sample period. A logical read is a read request for a data block from the SGA. Logical reads may result in a physical read if the requested block does not reside with the buffer cache.

This test checks the logical(db block gets + consistent gets) reads per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Session logical reads are %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Session logical reads are %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

LogicalReads / Seconds where:

- LogicalReads: difference in 'select value from v$sysstat where name='session logical reads'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

Excessive logical reads, even if they do not result in physical reads, can still represent an area that should be considered for performance tuning. Typically large values for this statistic indicate that full table scans are being performed. To identify the SQL that is performing the most logical reads (buffer gets), use the Top SQL page sorted by Buffer Gets. This quickly identifies the SQL responsible for the bulk of the logical reads. You can further investigate these SQL statements via drilldowns. Tuning these SQL statements will reduce your buffer cache access.

4.34.69 Session Logical Reads (per transaction)

This metric represents the number of logical reads per transaction during the sample period.

The value of this statistic is zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding per second metric of the same name will be a better indicator of current performance.

This test checks the logical (db block gets + consistent gets) reads per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Session logical reads are %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Session logical reads are %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaReads / Transactions where:

- DeltaReads: difference in 'select value from v$sysstat where name='session logical reads'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

Excessive logical reads, even if they do not result in physical reads, can still represent an area that should be considered for performance tuning. Typically large values for this statistic indicate that full table scans are being performed. To identify the SQL that is performing the most logical reads (buffer gets) use the Top SQL page sorted by Buffer Gets. This quickly identifies the SQL responsible for the bulk of the logical reads.

4.34.70 Soft Parse (%)

A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.

This metric represents the percentage of parse requests where the cursor was already in the cursor cache compared to the number of total parses. This ratio provides an indication as to how often the application is parsing statements that already reside in the cache as compared to hard parses of statements that are not in the cache.

This test checks the percentage of soft parse requests to total parse requests. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Only %value%% of parses are soft parses.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Only %value%% of parses are soft parses.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Data Source

((DeltaParseCountTotal - DeltaParseCountHard) / DeltaParseCountTotal) * 100 where:

- DeltaParseCountTotal: difference in 'select value from v$sysstat where name='parse count (total)'' between sample end and start
- DeltaParseCountHard: difference in 'select value from v$sysstat where name='parse count (hard)'' between sample end and start

User Action

Soft parses consume less resources than hard parses, so the larger the value for this item, the better. But many soft parses indicate the application is using SQL inefficiently. Reparsing the statement, even if it is a soft parse, requires a network round trip from the application to the database, as well as requiring the processing time to locate the previously compiled statement in the cache. Reducing network round trips and unnecessary processing will improve application performance.

If this metric value is below 80% you should look at the Top Sessions page sorted by Hard Parses. This page lists the sessions that are currently performing the most hard parses. Starting with these sessions and the SQL statements they are executing will indicate which applications and corresponding SQL statements are being used inefficiently.

If the metric is currently showing a high value, the expensive hard parses are not occurring but the application can still be tuned by reducing the amount of soft parses. Visit the Top SQL page sorted by Parses to identify the SQL statements that have been most parsed. This will allow you to quickly identify SQL that is being re-parsed unnecessarily. You should investigate these statements first for possible application logic changes such that cursors are opened once, and executed or fetched from many times.

4.34.71 Sorts to Disk (per second)

This metric represents the number of sorts going to disk per second for this sample period. For best performance, most sorts should occur in memory, because sorts to

disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption.

This test checks the number of sorts performed to disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	The rate of sorts to disk is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	The rate of sorts to disk is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaDiskSorts / Seconds where:

- DeltaDiskSorts: difference in 'select value from v$sysstat where name='sorts (disk)'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

The sessions that are performing the most sorts should be identified, such that the SQL they are executing can be further identified. The sort area sizes for the database may be sized correctly, the application SQL may be performing unwanted or excessive sorts. The sessions performing the most sorts are available through the Top Sessions sorted by Disk Sorts page.

Further drilldown into the session performing the most disk sorts with the Current SQL page will show you the SQL statement responsible for the disk sorts.

The Top SQL page sorted by Sorts provides a mechanism to quickly display the SQL statements in the cache, presented in sorted order by their number sort operations. This is an alternative to viewing sort of current sessions, it allows you to view sort activity via SQL statements, and will contain cumulative statistics for all executions of that statement.

If excessive sorts are taking place on disk, and the query's are correct, consider increasing the SORT_AREA_SIZE initialization parameter to increase the size of the sort area. A larger sort area will allow the Oracle Server to keep sorts in memory, reducing the number of I/O operations required to do an equivalent amount of work using the current sort area size.

4.34.72 Sorts to Disk (per transaction)

This metric represents the number of sorts going to disk per transactions for this sample period. For best performance, most sorts should occur in memory, because sorts to disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the number of sorts performed to disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	The rate of sorts to disk is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	The rate of sorts to disk is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaDiskSorts / Transactions where:

- DeltaDiskSorts: difference in 'select value from v$sysstat where name='sorts (disk)'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

The sessions that are performing the most sorts should be identified, such that the SQL they are executing can be further identified. The sort area sizes for the database may be sized correctly, the application SQL may be performing unwanted or excessive sorts. The sessions performing the most sorts are available through the Top Sessions page sorted by Disk Sorts.

Further drilldown into the session performing the most disk sorts with the Current SQL page will show you the SQL statement responsible for the disk sorts.

The Top SQL page sorted by Sorts provides a mechanism to quickly display the SQL statements in the cache, presented in sorted order by their number sort operations. This is an alternative to viewing sort of current sessions, it allows you to view sort activity via SQL statements, and will contain cumulative statistics for all executions of that statement.

If excessive sorts are taking place on disk, and the query's are correct, consider increasing the SORT_AREA_SIZE initialization parameter to increase the size of the sort area. A larger sort area will allow the Oracle Server to keep sorts in memory, reducing the number of I/O operations required to do an equivalent amount of work using the current sort area size.

4.34.73 Total Index Scans (per second)

This metric represents the total number of index scans per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

index scans kdiixs1 / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.74 Total Index Scans (per transaction)

This metric represents the total number of index scans per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

index scans kdiixsl / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.75 Total Parses (per second)

This number reflects the total number of parses per second, both hard and soft. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.

Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor.

This test checks the number of parse calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of

occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Total parse rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Total parse rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaParses / Seconds where:

- DeltaParses: difference in 'select value from v$sysstat where name='parse count (total)'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

If there appears to be excessive time spent parsing, evaluate SQL statements to determine which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The Top Sessions page sorted by Hard Parses will show you which sessions are incurring the most hard parses. Hard parses happen when the server parses a query and cannot find an exact match for the query in the library cache. Hard parses can be avoided by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this page may lead you to the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

4.34.76 Total Parses (per transaction)

This number reflects the total number of parses per transaction, both hard and soft. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.

Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor.

This test checks the number of parse calls per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Total parse rate is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Total parse rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaParses / Transactions where:

- DeltaParses: difference in 'select value from v$sysstat where name='parse count (total)'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

If there appears to be excessive time spent parsing, evaluate SQL statements to determine which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of

the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The Top Sessions page sorted by Hard Parses will show you which sessions are incurring the most hard parses. Hard parses happen when the server parses a query and cannot find an exact match for the query in the library cache. Hard parses can be avoided by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this page may lead you to the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

4.34.77 Total Table Scans (per second)

This metric represents the number of long and short table scans per second during the sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Total table scan rate is %value%/sec.
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Total table scan rate is %value%/sec.
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Data Source

(DeltaLongScans + DeltaShortScans) / Seconds:

- DeltaLongScans: difference in 'select value from v$sysstat where name='table scans (long tables)'' between end and start of sample period
- DeltaShortScans: difference in 'select value from v$sysstat where name='table scans (short tables)'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

A table scan indicates that the entire table is being scanned record-by-record in order to satisfy the query. For small tables that can easily be read into and kept in the buffer cache, this may be advantageous. But larger tables will force many physical reads and potentially push other required buffers out of the cache. SQL statements with large physical read and logical read counts are candidates for table scans. They can be identified through two different methods. The Top Sessions page sorted by Physical Reads displays sessions that are responsible for the current I/O activity. The Top SQL page sorted by Physical Reads lists the SQL statements in the cache by the amount of I/O they have performed. Some of these SQL statements may have high I/O numbers but they may not be attributing to the current I/O load.

4.34.78 Total Table Scans (per transaction)

This metric represents the number of long and short table scans per transaction during the sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Total table scan rate is %value% / transaction.
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Total table scan rate is %value%/ transaction.
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Not Defined

Data Source

(DeltaLongScans + DeltaShortScans) / Transactions:

- DeltaLongScans: difference in 'select value from v$sysstat where name='table scans (long tables)'' between end and start of sample period
- DeltaShortScans: difference in 'select value from v$sysstat where name='table scans (short tables)'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

A table scan indicates that the entire table is being scanned record-by-record in order to satisfy the query. For small tables that can easily be read into and kept in the buffer cache, this may be advantageous. But larger tables will force many physical reads and potentially push other required buffers out of the cache. SQL statements with large physical read and logical read counts are candidates for table scans. They can be identified through two different methods. The Top Sessions page sorted by Physical Reads displays sessions that are responsible for the current I/O activity. The Top SQL page sorted by Physical Reads lists the SQL statements in the cache by the amount of I/O they have performed. Some of these SQL statements may have high I/O numbers but they may not be attributing to the current I/O load.

4.34.79 User Calls (%)

This metric represents the percentage of user calls to recursive calls.

Occasionally, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:

When data dictionary information is not available in the data dictionary cache and must be retrieved from disk.

- In the firing of database triggers
- In the execution of DDL statements

- In the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- In the enforcement of referential integrity constraints

This test checks the percentage of user calls to recursive calls. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	<	Not Defined	Not Defined	2	%value%% of calls are user calls.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	<	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User call rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

(DeltaUserCalls/(DeltaRecursiveCalls + DeltaUserCalls)) * 100 where:

- DeltaRecursiveCalls: difference in 'select value from v$sysstat where name='recursive calls'' between sample end and start
- DeltaUserCalls: difference in 'select value from v$sysstat where name='user calls'' between sample end and start

User Action

A low value for this metric means that the Oracle Server is making a large number of recursive calls. If the Oracle Server appears to be making excessive recursive calls while your application is running, determine what activity is causing these recursive calls. If you determine that the recursive calls are caused by dynamic extension, either reduce the frequency of extension by allocating larger extents or, if you are using Oracle8*i*, considering taking advantage of locally managed tablespaces.

4.34.80 User Calls (per second)

This metric represents the number of logins, parses, or execute calls per second during the sample period.

This test checks the number of logins, parses, or execute calls. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User call rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User call rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaUserCalls / Seconds where:

- DeltaUserCalls: difference in 'select value from v$sysstat where name='user calls'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

This statistic is a reflection of how much activity is going on within the database. Spikes in the total user call rate should be investigated to determine which of the underlying calls is actually increasing. Parse, execute and logon calls each signify different types of user or application actions and should be addressed individually. User Calls is an overall activity level monitor.

4.34.81 User Calls (per transaction)

This metric represents the number of logins, parses, or execute calls per transaction during the sample period.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the number of logins, parses, or execute calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User call rate is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User call rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaUserCalls / Transactions where:

- DeltaUserCalls: difference in 'select value from v$sysstat where name='user calls'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

This statistic is a reflection of how much activity is going on within the database. Spikes in the total user call rate should be investigated to determine which of the underlying calls is actually increasing. Parse, execute and logon calls each signify different types of user or application actions and should be addressed individually. User Calls is an overall activity level monitor.

4.34.82 User Commits (per second)

This metric represents the number of user commits performed, per second during the sample period. When a user commits a transaction, the redo generated that reflects the changes made to database blocks must be written to disk. Commits often represent the closest thing to a user transaction rate.

This test checks the number of user commits per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User commit rate is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User commit rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaCommits / Seconds where:

- DeltaCommits: difference in 'select value from v$sysstat where name='user commits'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

This statistic is an indication of how much work is being accomplished within the database. A spike in the transaction rate may not necessarily be bad. If response times stay close to normal, it means your system can handle the added load. Actually, a drop in transaction rates and an increase in response time may be indicators of problems. Depending upon the application, transaction loads may vary widely across different times of the day.

4.34.83 User Commits (per transaction)

This metric represents the number of user commits performed, per transaction during the sample period. When a user commits a transaction, the redo generated that reflects the changes made to database blocks must be written to disk. Commits often represent the closest thing to a user transaction rate.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the number of user commits per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User commit rate is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User commit rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaCommits / Transactions where:

- DeltaCommits: difference in 'select value from v$sysstat where name='user commits'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

This statistic is an indication of how much work is being accomplished within the database. A spike in the transaction rate may not necessarily be bad. If response times stay close to normal, it means your system can handle the added load. Actually, a drop in transaction rates and an increase in response time may be indicators of problems. Depending upon the application, transaction loads may vary widely across different times of the day.

4.34.84 User Rollback Undo Records Applied (per second)

This metric represents the number of undo records applied to user-requested rollback changes per second.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

(rollback changes - undo records applied) / time

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.85 User Rollback Undo Records Applied (per transaction)

This metric represents the number of undo records applied to user-requested rollback changes per transaction.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

(rollback changes - undo records applied) / transactions

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.34.86 User Rollbacks (per second)

This metric represents the number of times, per second during the sample period, that users manually issue the ROLLBACK statement or an error occurred during a user's transactions.

This test checks the number of rollbacks per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User rollback rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User rollback rate is %value%/sec.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaRollbacks / Seconds where:

- DeltaRollbacks: difference in 'select value from v$sysstat where name='user rollbacks'' between end and start of sample period
- Seconds: number of seconds in sample period

User Action

This value shows how often users are issuing the ROLLBACK statement or encountering errors in their transactions. Further investigation should be made to determine if the rollbacks are part of some faulty application logic or due to errors occurring through database access.

4.34.87 User Rollbacks (per transaction)

This metric represents the number of times, per transaction during the sample period, that users manually issue the ROLLBACK statement or an error occurred during a user's transactions.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" metric of the same name will be a better indicator of current performance.

This test checks the Number of rollbacks per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User rollback rate is %value% / transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User rollback rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Data Source

DeltaRollbacks / Transactions where:

- DeltaRollbacks: difference in 'select value from v$sysstat where name='user rollbacks'' between end and start of sample period
- Transactions: number of transactions in sample period

User Action

This value shows how often users are issuing the ROLLBACK statement or encountering errors in their transactions. Further investigation should be made to determine if the rollbacks are part of some faulty application logic or due to errors occurring through database access.

4.35 User Audit

This metric category contains the metrics used to represent logons to the database by audited users (such as SYS).

4.35.1 Audited User

This metric monitors specified database user connections. For example, an alert is displayed when a particular database user connection, specified by the User name filter argument, has been detected.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 15 Minutes	Not Uploaded	=	SYS	Not Defined	1	User %value% logged on from %machine%.

Metric Summary for Grid Control

The following tables show how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	User rollback rate is %value%/ transaction.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	2	Generated By Database Server

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Username_Machine" object.

If warning or critical threshold values are currently set for any "Username_Machine" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Username_Machine" object, use the Edit Thresholds page.

Data Source

For each metric index:

```
SELECT username
```

User Action

User actions may vary depending on the user connection that is detected.

4.35.2 Audited User Host

This metric represents the host machine from which the audited user's logon originated.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

For each metric index:

```
SELECT machine
```

User Action

Review the access to the database from this client machine.

4.35.3 Audited User Session Count

This metric represents the number of logons the audited user has from a given machine.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
All Versions	Every 15 Minutes

Data Source

For each metric index:

```
SELECT count(username)
```

User Action

No user action is necessary.

4.36 User Block

This metric category contains the metrics that tell to what extent, and how consistently, a given session is blocking multiple other sessions.

4.36.1 Blocking Session Count

This metric signifies that a database user is blocking at least one other user from performing an action, such as updating a table. An alert is generated if the number of consecutive blocking occurrences reaches the specified value.

Note: The catblock.sql script needs to be run on the managed database prior to using the User Blocks test. This script creates some additional tables, view, and public synonyms that are required by the User Blocks test.

Note: Unlike most metrics, which accept thresholds as real numbers, this metric can only accept an integer as a threshold.

Metric Summary for Database Control

For metrics available in Database Control, no data is collected. Only alerts are generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every 5 Minutes	Not Uploaded	>	0	Not Defined	3	Session %sid% blocking %value% other sessions.

Target Version	Server Evaluation Frquency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every Minute	Not Defined	After Every Sample	>	0	Not Defined	15	Generated By Database Server

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Blocking Session ID" object.

If warning or critical threshold values are currently set for any "Blocking Session ID" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Blocking Session ID" object, use the Edit Thresholds page.

Data Source

```
SELECT SUM(num_blocked)
  FROM (SELECT id1, id2, MAX(DECODE(block, 1, sid, 0)) blocking_sid,
```

```
  SUM(DECODE(request, 0, 0, 1)) num_blocked
  FROM v$lock
    WHERE block = 1 OR request>0
    GROUP BY id1, id2)
GROUP BY blocking SID
```

User Action

Either have user who is blocking other users rollback the transaction, or wait until the blocking transaction has been committed.

4.37 User Block Chain

This metric collects information on lock chains, including DB time currently accumulated per chain and the blocked sessions for each chain.

4.37.1 Blocking Session Count

This metric represents the total number of sessions blocked in this chain.

Metric Summary for Database Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes

Data Source

v$lock and v$session

User Action

No user action is required.

4.37.2 Blocking Session DB Time

This metric represents the total DB time currently accumulated in this chain.

Metric Summary for Database Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	Every 15 Minutes	Not Updated	>	Not Defined	Not Defined	1	Total db time %value% seconds is consumed by %count% sessions blocked by session (%blocker_session_info%).

Data Source

v$lock and v$session

User Action

No user action is required.

4.38 User Locks

The metrics in this metric category provide information regarding user locks.

Enterprise Manager will issue the alert when the maximum blocked session count or maximum blocked DB time (seconds) of transactional locks: TM, TX, UL reach the threshold.

4.38.1 Maximum Blocked DB Time (seconds)

This metric represents the maximum time wasted in any given lock chain; not for the total time wasted by everyone in any lock chain.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Key	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	lockType: "TM"	Every 5 Minutes	Not Uploaded	>	Not Defined	Not Defined	1	%value% seconds in DB Time is spent waiting for %lockType% lock.
9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	lockType: "TX"	Every 5 Minutes	Not Uploaded	>	Not Defined	Not Defined	1	%value% seconds in DB Time is spent waiting for %lockType% lock.
9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	lockType: "UL"	Every 5 Minutes	Not Uploaded	>	Not Defined	Not Defined	1	%value% seconds in DB Time is spent waiting for %lockType% lock.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "User Lock Type" object.

If warning or critical threshold values are currently set for any "User Lock Type" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "User Lock Type" object, use the Edit Thresholds page.

Data Source

The data for the metric is retrieved from database view gv$session.

User Action

User can set the threshold for warning alert or critical alert for maximum Blocked DB Time (seconds). When maximum time wasted in any given lock chain reaches the threshold, Enterprise Manager will issue the alert.

4.38.2 Maximum Blocked Session Count

This metric represents the maximum length of any lock chain; not for the total number of people stuck in lock chains.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Target Version	Key	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	lockType: "TM"	Every 5 Minutes	Not Uploaded	>	3	Not Defined	1	%value% sessions are blocked by %lockType% lock.
9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	lockType: "TX"	Every 5 Minutes	Not Uploaded	>	3	Not Defined	1	%value% sessions are blocked by %lockType% lock.
9.0.1.x; 9.2.0.x; 10.1.0.x; 10.2.0.x; 11.1.0.x; 11.2.0.x	lockType: "UL"	Every 5 Minutes	Not Uploaded	>	3	Not Defined	1	%value% sessions are blocked by %lockType% lock.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "User Lock Type" object.

If warning or critical threshold values are currently set for any "User Lock Type" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "User Lock Type" object, use the Edit Thresholds page.

Data Source

The data for the metric is retrieved from database view gv$session.

User Action

User can set the threshold for warning alert or critical alert for "maximum Blocked Session Count". When maximum length of any lock chain reaches the threshold, Enterprise Manager will issue the alert.

4.39 User-Defined SQL Metrics

The UDM metric allows you to execute your own SQL statements. The data returned by these SQL statements can be compared against thresholds and generate severity alerts similar to alerts in predefined metrics.

4.39.1 User-Defined Numeric Metric

Contains a value if the value type is NUMBER. Otherwise, the value is "", if the value is STRING.

Data Source

SQL statement which can be either a Select statement or function that returns a single scalar value (numeric or string).

4.39.2 User-Defined String Metric

Contains a value if the value type is STRING. Otherwise, the value is "", if the value is NUMBER.

Data Source

SQL statement which can be either a Select statement or function that returns a single scalar value (numeric or string).

4.40 Wait Bottlenecks

This metric category contains the metrics that approximate the percentage of time spent waiting by user sessions. This approximation takes system-wide totals and discounts the effects of sessions belonging to background processes.

4.40.1 Active Sessions Using CPU

This metric represents the active sessions using CPU.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute

4.40.2 Active Sessions Waiting: I/O

This metric represents the active sessions waiting for I/O.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute

4.40.3 Active Sessions Waiting: Other

This metric represents all the waits that are neither idle nor user I/O.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute

4.40.4 Average Instance CPU (%)

This metric represents the average instance CPU as a percentage, that is, the instance CPU time divided by the total CPU count, then multipled by 100.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute

4.40.5 Buffer busy waits (%)

This wait happens when a session wants to access a database block in the buffer cache but it cannot because the buffer is busy. Another session is modifying the block and the contents of the block are in flux during the modification. To guarantee that the reader has a coherent image of the block with either all of the changes or none of the changes, the session modifying the block marks the block header with a flag letting other users know a change is taking place and to wait until the complete change is applied.

The two main cases where this wait can occur are:

- Another session is reading the block into the buffer
- Another session holds the buffer in an incompatible mode to our request

While the block is being changed, the block is marked as unreadable by others. The changes that are being made should last under a few hundredths of a second. A disk read should be under 20 milliseconds and a block modification should be under one millisecond. Therefore it will take a lot of buffer busy waits to cause a problem.

However, in a problem situation, there is usually a hot block, such as the first block on the free list of a table, with high concurrent inserts. All users will insert into that block at the same time, until it fills up, then users start inserting into the next free block on the list, and so on.

Another example of a problem is of multiple users running full table scans on the same large table at the same time. One user will actually read the block physically off disk, and the other users will wait on Buffer Busy Wait for the physical I/O to complete.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–1 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'buffer busy waits' event.

Data Source

(DeltaBufferBusyWaitsTime/DeltaServiceTime)*100 where:

- DeltaBufferBusyWaitsTime: difference of 'sum of time waited for sessions of foreground processes on the 'buffer busy waits' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Look at v$waitstat (or the buffer busy drill down page) and determine the block type with the highest waits.

Block Type and Action:

- Undo Header - Use Automatic Undo Management (AUM) or add more RBS segments)
- Undo Block - Use AUM (or increase RBS sizes)
- Data Block - First determine if it is an I/O problem. The Buffer Busy Waits drill-down page should provide this information. Otherwise, sample from v$session_wait

```
SELECT p3, count(*)
  FROM v$session_wait
  WHERE event='buffer busy wait' ;
```

  If p3 is less than 200 then it is an I/O problem. Either improve I/O performance or change application. Applications running concurrent batch jobs that do full table scans on the same large tables run into this problem.

- Free List - Use ASSM (or freelists groups)

4.40.6 CPU Time Delta (sec)

This metric represents the time spent using CPU during the interval, measured in hundredths of a second.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute

Data Source

The difference of sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start.

User Action

No user action is necessary.

4.40.7 DB file scattered read (%)

This is the same type of event as "db file sequential read", except that Oracle will read multiple data blocks. Multi-block reads are typically used on full table scans. The name "scattered read" refers to the fact that multiple blocks are read into database block buffers that are 'scattered' throughout memory.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–2 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	50	Not Defined	5	%value%% of service time is spent waiting on the 'db file scattered read' event.

Data Source

(DeltaDbFileScatteredReadTime/DeltaServiceTime)*100 where:

- DeltaDbFileScatteredReadTime: difference of 'sum of time waited for sessions of foreground processes on the 'db file scattered read' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

If the TIME spent waiting for multiblock reads is significant, then it is helpful to determine against which segments Oracle is performing the reads. The files where the reads are occurring can be found by looking at the V$FILESTAT view where BLKS_READ / READS > 1. (A ratio greater than one indicates there are some multiblock reads occurring).

It is also useful to see which sessions are performing scans and trace them to see if the scans are expected. This statement can be used to see which sessions may be worth tracing:

```
SELECT sid, total_waits, time_waited
  FROM v$session_event
  WHERE event='db file scattered read' and total_waits>0
  ORDER BY 3,2 ;
```

You can also look at:

- Statements with high DISK_READS in the V$SQL view
- Sessions with high table scans blocks gotten in the V$SESSTAT view

4.40.8 DB file sequential read (%)

This event shows a wait for a foreground process while doing a sequential read from the database. The I/O is generally issued as a single I/O request to the OS; the wait blocks until the I/O request completes.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–3 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	50	Not Defined	5	%value%%% of service time is spent waiting on the 'db file sequential read' event.

Data Source

(DeltaDbFileSequentialReadTime/DeltaServiceTime)*100 where:

- DeltaDbFileSequentialReadTime: difference of 'sum of time waited for sessions of foreground processes on the 'db file sequential read' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Because I/O is a normal activity, take notice of unnecessary or slow I/O activity. If the TIME spent waiting for I/Os is significant, then it can be determined for which segments Oracle has to go to disk. See the "Tablespace I/O" and "File I/O" sections of the ESTAT or STATSPACK reports to get information on which tablespaces and files are servicing the most I/O requests, and to get an indication of the speed of the I/O subsystem.

If the TIME spent waiting for reads is significant, then determine against which segments Oracle is performing the reads. The files where the reads are occurring can be found by looking at the V$FILESTAT view.

Also, see which sessions are performing reads and trace them to see if the I/Os are expected. You can use this statement to see which sessions are worth tracing:

```
SELECT sid, total_waits, time_waited
  FROM v$session_event
  WHERE event='db file sequential read' and total_waits>0
  ORDER BY 3,2 ;
```

You can also look at:

- Statements with high DISK_READS in the V$SQL view
- Sessions with high "physical reads" in the V$SESSTAT view

4.40.9 DB file single write (%)

This event is used to wait for the writing of the file headers.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–4 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	50	Not Defined	3	%value%% of service time is spent waiting on the 'db file single write' event.

Data Source

(DeltaDbFileSingleWriteTime/DeltaServiceTime)*100 where:

- DeltaDbFileSingleWriteTime: difference of 'sum of time waited for sessions of foreground processes on the 'db file single write' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

No user action is necessary.

4.40.10 Direct path read (%)

The session is waiting for a direct read to complete. A direct read is a physical I/O from a data file that bypasses the buffer cache and reads the data block directly into process-private memory.

If asynchronous I/O is supported (and in use), then Oracle can submit I/O requests and continue processing. Oracle can then pick up the results of the I/O request later and wait on "direct path read" until the required I/O completes.

If asynchronous I/O is not being used, then the I/O requests block until completed but these do **not** show as waits at the time the I/O is issued. The session returns later to pick up the completed I/O data but can then show a wait on "direct path read" even though this wait will return immediately.

Hence this wait event is very misleading because:

- The total number of waits does not reflect the number of I/O requests
- The total time spent in "direct path read" does not always reflect the true wait time.

This style of read request is typically used for:

- Sort I/O (when a sort does not fit in memory)
- Parallel Query slaves
- Read ahead (where a process may issue an I/O request for a block it expects to need in the near future)

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–5 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	50	Not Defined	3	%value%% of service time is spent waiting on the 'direct path read' event.

Data Source

(DeltaDirectPathReadTime/DeltaServiceTime)*100 where:

- DeltaDirectPathReadTime: difference of 'sum of time waited for sessions of foreground processes on the 'direct path read' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

In DSS type systems, or during heavy batch periods, waits on "direct path read" are normal. However, if the waits are significant on an OLTP style system, there may be a problem.

You can:

- Examine the V$SESSION_EVENT view to identify sessions with high numbers of waits
- Examine the V$SESSTAT view to identify sessions with high "physical reads direct" (statistic only present in newer Oracle releases)
- Examine the V$FILESTAT view to see where the I/O is occurring
- Examine the V$SQLAREA view for statements with SORTS and high DISK_ READS (which may or may not be due to direct reads)
- Determine whether the file indicates a temporary tablespace check for unexpected disk sort operations.
- Ensure that the DISK_ASYNCH_IO parameter is set to TRUE. This is unlikely to reduce wait times from the wait event timings but may reduce sessions elapsed times (as synchronous direct I/O is not accounted for in wait event timings).
- Ensure the OS asynchronous I/O is configured correctly.
- Check for I/O heavy sessions and SQL and see if the amount of I/O can be reduced.
- Ensure no disks are I/O bound.

4.40.11 Direct path read (lob) (%)

The session is waiting for a direct read of a large object (lob) to complete. A direct read is a physical I/O from a data file that bypasses the buffer cache and reads the data block directly into process-private memory.

If asynchronous I/O is supported (and in use), then Oracle can submit I/O requests and continue processing. Oracle can then pick up the results of the I/O request later and wait on "direct path read" until the required I/O completes.

If asynchronous I/O is not being used, then the I/O requests block until completed but these do **not** show as waits at the time the I/O is issued. The session returns later to pick up the completed I/O data but can then show a wait on "direct path read" even though this wait will return immediately.

Hence this wait event is very misleading because:

- The total number of waits does not reflect the number of I/O requests
- The total time spent in "direct path read" does not always reflect the true wait time.

This style of read request is typically used for:

- Sort I/O (when a sort does not fit in memory)
- Parallel Query slaves
- Read ahead (where a process may issue an I/O request for a block it expects to need in the near future)

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–6 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	50	Not Defined	3	%value%% of service time is spent waiting on the 'direct path read (lob)' event.

Data Source

(DeltaDirectPathReadLobTime/DeltaServiceTime)*100 where:

- DeltaDirectPathReadLobTime: difference of 'sum of time waited for sessions of foreground processes on the 'direct path read (lob)' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

For noncached lob segments, it is helpful to place the data files where the LOB SEGMENTS reside on a buffered disk, for example, on a File system disk. This placement allows the direct reads to benefit from a cache not on Oracle for data read operations.

4.40.12 Direct path write (%)

Session is waiting for a direct write to complete.

Direct path writes allow a session to queue an I/O write request and continue processing while the OS handles the I/O. If the session needs to know if an outstanding write is complete, then it waits for this wait event. This can happen because the session is either out of free slots and needs an empty buffer (it waits on the oldest I/O) or it needs to ensure all writes are flushed.

If asynchronous I/O is not being used, then the I/O write request blocks until it is completed but this does not show as a wait at the time the I/O is issued. The session returns later to pick up the completed I/O data but can then show a wait on "direct path write" even though this wait will return immediately.

Hence this wait event is misleading because:

- The total number of waits does not reflect the number of I/O requests
- The total time spent in "direct path write" does not always reflect the true wait time.

This style of read request is typically used for:

- Sort I/O (when a sort does not fit in memory)
- Parallel DML are issued to create and populate objects
- Direct load operations, for example, Create Table as Select (CTAS)

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–7 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	50	Not Defined	3	%value%% of service time is spent waiting on the 'direct path write' event.

Data Source

(DeltaDirectPathWriteTime/DeltaServiceTime)*100 where:

- DeltaDirectPathWriteTime: difference of 'sum of time waited for sessions of foreground processes on the 'direct path write' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

It is unusual to see lots of waits on "direct path write" except for specific jobs. If the figure is a large proportion of the overall wait time it is best to identify where the writes are coming from.

You can:

- Examine the V$SESSION_EVENT view to identify sessions with high numbers of waits.
- Examine the V$SESSTAT view to identify sessions with high "physical writes direct" (statistic only present in newer Oracle releases).
- Examine the V$FILESTAT view to see where the I/O is occurring.
- Determine whether the file indicates a temporary tablespace check for unexpected disk sort operations.
- Ensure the DISK_ASYNCH_IO parameter is set to TRUE. This is unlikely to reduce wait times from the wait event timings but may reduce sessions elapsed times because synchronous direct I/O is not accounted for in wait event timings.
- Ensure the OS asynchronous I/O is configured correctly.
- Ensure no disks are I/O bound.

- For parallel DML, check the I/O distribution across disks and make sure that the I/O subsystem is adequately sized for the degree of parallelism.

4.40.13 Direct path write (lob) (%)

Direct path write to a large object (LOB). The session is waiting on the operating system to complete the write operation.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–8 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	50	Not Defined	3	%value%% of service time is spent waiting on the 'direct path write (lob)' event.

Data Source

(DeltaDirectPathWriteLobTime/DeltaServiceTime)*100 where:

- DeltaDirectPathWriteLobTime: difference of 'sum of time waited for sessions of foreground processes on the 'direct path write (lob)' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

It is unusual to see lots of waits on "direct path write (lob)" except for specific jobs. If the figure is a large proportion of the overall wait time it is best to identify where the writes are coming from.

You can:

- Examine the V$SESSION_EVENT view to identify sessions with high numbers of waits.
- Examine the V$SESSTAT view to identify sessions with high "physical writes direct" (statistic only present in newer Oracle releases).
- Examine the V$FILESTAT view to see where the I/O is occurring.
- Determine whether the file indicates a temporary tablespace check for unexpected disk sort operations.
- Ensure the DISK_ASYNCH_IO parameter is set to TRUE. This is unlikely to reduce wait times from the wait event timings but may reduce sessions elapsed times because synchronous direct I/O is not accounted for in wait event timings.

- Ensure the OS asynchronous I/O is configured correctly.
- Ensure no disks are I/O bound.
- For parallel DML, check the I/O distribution across disks and make sure that the I/O subsystem is adequately sized for the degree of parallelism.

4.40.14 Enqueue - other (%)

Enqueues are local locks that serialize access to various resources. This wait event indicates a wait for a lock that is held by another session (or sessions) in an incompatible mode to the requested mode.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–9 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'enqueue' event.

Data Source

(DeltaEnqueueTime/DeltaServiceTime)*100 where:

- DeltaEnqueueTime: difference of 'sum of time waited for sessions of foreground processes on the 'enqueue' event, or any other 'enqueue:' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

The action to take depends on the lock type which is causing the most problems. The most common lock waits are generally for:

- TX: Transaction Lock -- Generally due to application or table setup issues, for example row level locking conflicts and ITL allocation
- TM: DML enqueue -- Generally due to application issues, particularly if foreign key constraints have not been indexed.
- ST: Space management enqueue -- Usually caused by too much space management occurring (for example, small extent sizes, lots of sorting, and so on)
- HW: High Water Mark -- Concurrent users trying to extend a segment's high-water mark for space allocated.

In Oracle9*i* and earlier releases, all enqueue wait times are included in this alert.

To determine which enqueues are causing the most waits systemwide:

- In Oracle9*i* and later, examine the V$ENQUEUE_STAT view thus:

```
SELECT eq_type "Lock", total_req# "Gets", total_wait# "Waits", cum_wait_time
  FROM V$enqueue_stat
  WHERE Total_wait# > 0 ;
```

- In Oracle8*i* and earlier, examine the X$KSQST view thus:

```
SELECT ksqsttyp "Lock", ksqstget "Gets", ksqstwat "Waits"
  FROM X$KSQST
  where KSQSTWAT>0 ;
```

The above give the systemwide number of waits for each lock type. Remember that it only takes one long wait to distort the average wait time figures.

You can also examine:

- Sessions with high numbers of "enqueue waits" in the V$SESSTAT view
- Sampling of the V$LOCK view to find waiting / blocking sessions

4.40.15 Enqueue: DML - contention (%)

TM Per table locks are acquired during the execution of a transaction when referencing a table with a DML statement so that the object is not dropped or altered during the execution of the transaction, if and only if the dml_locks parameter is non-zero.

TM Locks are held for base table/partition operations under the following conditions:

- Enabling of referential constraints
- Changing constraints from DIASABLE NOVALIDATE to DISABLE VALIDATE
- Rebuild of an IOT
- Create View or Alter View operations
- Analyze table compute statistics or validate structure
- Parallel DML operations

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–10 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'enqueue: DML - contention' event.

Data Source

(DeltaEnqueueDMLTime/DeltaServiceTime)*100 where:

- DeltaEnqueueDMLTime: difference of 'sum of time waited for sessions of foreground processes on the 'enqueue: DML - contention' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Examine the database locks page and determine the user who is blocking another user and why, then decide the appropriate action.

4.40.16 Enqueue: HW, Segment High Water Mark - contention (%)

The HW enqueue is used to serialize the allocation of space above the high-water mark in an object.

This lock is acquired when a segment's high-water mark is moved, which typically is the case during heavy inserts.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–11 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'enqueue: HW, Segment High Water Mark - contention' event.

Data Source

(DeltaEnqueueHWTime/DeltaServiceTime)*100 where:

- DeltaEnqueueHWTime: difference of 'sum of time waited for sessions of foreground processes on the 'enqueue: Segment High Water Mark - contention' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Use Locally Managed Tablespaces.

For version dictionary managed tablespaces:

- Recreate the objects and preallocate extents with the following: ALTER TABLE...ALLOCATE EXTENT statements.
- Increasing the number of free lists may help, as well as moving the high-water mark. This depends on the number of freelists.

4.40.17 Enqueue: ST, Space Transaction - contention (%)

When Oracle needs to perform a space management operation (such as allocating temporary segments for a sort) the user session acquires a special enqueue called the 'ST' enqueue.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–12 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'enqueue: ST, Space Transaction - contention' event.

Data Source

(DeltaEnqueueSTTime/DeltaServiceTime)*100 where:

- DeltaEnqueueSTTime: difference of 'sum of time waited for sessions of foreground processes on the 'enqueue: Space Transaction - contention' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Ensure that temporary tablespaces are proper temporary tablespaces of type "temporary".

4.40.18 Enqueue: TM, TX, Transaction - row lock contention (%)

Two users are attempting to change the same row.

These locks are of type TX.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–13 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'enqueue: TM,TX, Transaction - row lock contention' event.

Data Source

(DeltaEnqueueRowLockTime/DeltaServiceTime)*100 where:

- DeltaEnqueueRowLockTime: difference of 'sum of time waited for sessions of foreground processes on the 'enqueue: Transaction - row lock contention' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Examine the database locks page and determine the user who is blocking another user and why, then decide the appropriate action.

4.40.19 Enqueue: TX mode 4, Transaction - allocate ITL entry (%)

Oracle keeps note of which rows are locked by which transaction in an area at the top of each data block known as the 'interested transaction list'. The number of ITL slots in any block in an object is controlled by the INITRANS and MAXTRANS attributes. INITRANS is the number of slots initially created in a block when it is first used, while MAXTRANS places an upper bound on the number of entries allowed. Each transaction which wants to modify a block requires a slot in this 'ITL' list in the block.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–14 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'enqueue: TX mode 4, Transaction - allocate ITL entry' event.

Data Source

(DeltaEnqueueAllocITLTime/DeltaServiceTime)*100 where:

- DeltaEnqueueAllocITLTime: difference of 'sum of time waited for sessions of foreground processes on the 'enqueue: TX mode 4, Transaction - allocate ITL entry' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

To increase the number of ITL slots, recreate the table and increase the INITRANS parameter for the object with the contention. An alter table statement can be run to increase the ITL slots by increasing the value for INITRANS, but this will only take effect for new blocks.

4.40.20 Enqueue: UL: User-defined - contention (%)

Caused by the application explicitly running commands of the nature "lock table".

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–15 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'enqueue: UL: User-defined - contention' event.

Data Source

(DeltaEnqueueUserDefTime/DeltaServiceTime)*100 where:

- DeltaEnqueueUserDefTime: difference of 'sum of time waited for sessions of foreground processes on the 'enqueue: User-defined - contention' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

This is an application issue. Determine where the application code is locking objects and why. Make relevant application changes if necessary.

Use the Blocking Sessions page to find lock holds and waits.

4.40.21 Free buffer waits (%)

This event occurs mainly when a server process is trying to read a new buffer into the buffer cache but too many buffers are either pinned or dirty and thus unavailable for reuse. The session posts to DBWR then waits for DBWR to create free buffers by writing out dirty buffers to disk.

DBWR may not be keeping up with writing dirty buffers in the following situations:

- The I/O system is slow.
- There are resources it is waiting for, such as latches.
- The buffer cache is so small that DBWR spends most of it's time cleaning out buffers for server processes.
- The buffer cache is so big that one DBWR process is not enough to free enough buffers in the cache to satisfy requests.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–16 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'free buffer waits' event.

Data Source

(DeltaFreeBufferWaitsTime/DeltaServiceTime)*100 where:

- DeltaFreeBufferWaitsTime: difference of 'sum of time waited for sessions of foreground processes on the 'free buffer waits' event' between sample end and start

- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Sometimes the easy solution is to increase the buffer cache to allow for more free blocks. This works in many cases, but if the application is generating a sustained amount of dirty blocks then increasing the buffer cache may only help or delay the problem but not solve it.

If this event occurs frequently, examine the session waits for DBWR to see whether there is anything delaying DBWR.

Run this query to see if the I/O is evenly distributed.

```
SELECT name, phyrds, phywrts
  FROM v$filestat a, v$datafile b
  WHERE a.file# = b.file#
```

Also look for files having full table scans, using this query:

```
SELECT name, phyrds, phyblkrd, phywrts
  FROM v$filestat a, v$datafile b
  WHERE a.file# = b.file#
    AND phyrds != phyblkrd
```

4.40.22 Host CPU Utilization (%)

This metric represents the percentage of CPU being used on the host.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected.

Target Version	Collection Frequency
10.1.0.x	Every 15 Minutes

4.40.23 Latch free - other (%)

A latch is a low-level internal lock used by Oracle to protect memory structures. Latches are similar to short duration locks that protect critical bits of code. This wait indicates that the process is waiting for a latch that is currently busy (held by another process).

The latch free event is updated when a server process attempts to get a latch, and the latch is unavailable on the first attempt.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–17 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'latch free' event.

Data Source

(DeltaLatchFreeTime/DeltaServiceTime)*100 where:

- DeltaLatchFreeTime: difference of 'sum of time waited for sessions of foreground processes on the 'latch free' event, or any other 'latch:' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Determine which latch is causing the highest amount of contention.

To find the problem latches since database startup, run the following query:

```
SELECT n.name, l.sleeps
  FROM v$latch l, v$latchname n
  WHERE n.latch#=l.latch# and l.sleeps > 0 order by l.sleeps ;
```

To see latches that are currently a problem on the database run:

```
SELECT n.name, SUM(w.p3) Sleeps
  FROM V$SESSION_WAIT w, V$LATCHNAME n
  WHERE w.event = `latch free'
    AND w.p2 = n.latch#
  GROUP BY n.name;
```

Take action based on the latch with the highest number of sleeps.

4.40.24 Latch: cache buffer chains (%)

The cache buffers chains latches are used to protect a buffer list in the buffer cache. These latches are used when searching for, adding, or removing a buffer from the buffer cache.

Blocks in the buffer cache are placed on linked lists (cache buffer chains) which hang off a hash table. The hash chain that a block is placed on is based on the DBA and CLASS of the block. Each hash chain is protected by a single child latch. Processes need to get the relevant latch to allow them to scan a hash chain for a buffer so that the linked list does not change underneath them.

Contention on this latch usually means that there is a block that is in great contention (known as a hot block).

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–18 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%%% of service time is spent waiting on the 'latch: cache buffer chains' event.

Data Source

(DeltaLatchCacheBufferChainsTime/DeltaServiceTime)*100 where:

- DeltaLatchCacheBufferChainsTime: difference of 'sum of time waited for sessions of foreground processes on the 'latch: cache buffer chains' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

To identify the heavily accessed buffer chain, and hence the contended for block, look at latch statistics for the cache buffers chains latches using the V$LATCH_CHILDREN view. If there is a specific cache buffers chains child latch that has many more GETS, MISSES, and SLEEPS when compared with the other child latches, then this is the contended for child latch.

This latch has a memory address, identified by the ADDR column.

```
SELECT addr, sleeps
  FROM v$latch_children c, v$latchname n
  WHERE n.name='cache buffers chains'
    and c.latch#=n.latch# and sleeps > 100
  ORDER BY sleeps /
```

Use the value in the ADDR column joined with the V$BH view to identify the blocks protected by this latch. For example, given the address (V$LATCH_CHILDREN.ADDR) of a heavily contended latch, this queries the file and block numbers:

```
SELECT file#, dbablk, class, state, TCH
  FROM X$BH WHERE HLADDR='address of latch';
```

X$BH.TCH is a touch count for the buffer. A high value for X$BH.TCH indicates a hot block.

Many blocks are protected by each latch. One of these buffers will probably be the hot block. Any block with a high TCH value is a potential hot block. Perform this query a number of times, and identify the block that consistently appears in the output.

After you have identified the hot block, query DBA_EXTENTS using the file number and block number to identify the segment.

4.40.25 Latch: library cache (%)

There are multiple library cache latches. Each one protects a range of 'hash buckets' and the latch covers all heaps.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–19 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'latch: library cache' event.

Data Source

(DeltaLatchLibraryCacheTime/DeltaServiceTime)*100 where:

- DeltaLatchLibraryCacheTime: difference of 'sum of time waited for sessions of foreground processes on the 'latch: library cache' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Contention for the library cache latches can be caused by excessive parsing of literal SQL. It is advisable to use sharable SQL wherever possible.

4.40.26 Latch: redo copy (%)

When a sessions redo buffer is larger than *Parameter: log_small_entry_max_size* the kernel first allocates a redo copy buffer, protected by a redo copy latch.

The buffer will not be used until space is allocated on the log buffer and some header has been set. However, the redo copy latch is acquired to reduce the code inside the allocation latch holding and to prevent further contention.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–20 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'latch: redo copy' event.

Data Source

(DeltaLatchRedoCopyTime/DeltaServiceTime)*100 where:

- DeltaLatchRedoCopyTime: difference of 'sum of time waited for sessions of foreground processes on the 'latch: redo copy' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

The number of redo copy latches is controlled by the init.ora *Parameter:log_simultaneous_copies*. If the parameter is not set, it defaults to the number of CPUs.

For log generating processes, the latch get is made in an immediate mode, then it will be convenient to have enough redo copy latches to reduce contention of foreground processes.

Before flushing out the log buffer, the LGWR will acquire all redo copy latches in a willing-to-wait mode. Thus an excessive number of copy latches will cause contention in the log buffer flushing process.

The number of LWGR redo copy latch allocations is redo writes * No.redo copy latches.

4.40.27 Latch: shared pool (%)

This latch protects the allocation of memory from the shared pool.

If there is contention on this latch, it is often an indication that the shared pool is fragmented.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–21 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'latch: shared pool' event.

Data Source

(DeltaLatchSharedPoolTime/DeltaServiceTime)*100 where:

- DeltaLatchSharedPoolTime: difference of 'sum of time waited for sessions of foreground processes on the 'latch: shared pool' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Shared pool latch contention is often an indication of high hard parsing usually caused by the use of literal values in SQL statements. These statements could otherwise be shared if bind variables were used.

Prior to Oracle Server release 8.1.6, shared pool fragmentation could be acerbated by a shared pool that was too large. Reducing the size of the shared pool would reduce the contention for this latch.

For Oracle Server release 8.1.6 and later, there should be very little shared pool latch contention. If there is, it is probably a symptom of an application using literals. One possible solution is to use the init.ora parameter*cursor_sharing=FORCE*.

4.40.28 Library cache load lock (%)

Oracle tries to find the load lock for the database object so that it can load the object. The load lock is always gotten in Exclusive mode, so that no other process can load the same object. If the load lock is busy the session will wait on this event until the lock becomes available.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–22 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%%% of service time is spent waiting on the 'library cache load lock' event.

Data Source

(DeltaLibraryCacheLoadLockTime/DeltaServiceTime)*100 where:

- DeltaLibraryCacheLoadLockTime: difference of 'sum of time waited for sessions of foreground processes on the 'library cache load lock' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

To be waiting for a load lock means that there is a blocker with a higher or incompatible mode. This event in itself is not affected by the parallel server. However, you must have acquired the 'library cache lock' before you get to this point. The 'cache lock' is a DFS lock.

4.40.29 Library cache lock (%)

The library cache lock controls the concurrency between clients of the library cache by acquiring a lock on the object handle so that one client can prevent other clients from accessing the same object or the client can maintain a dependency for a long time (no other client can change the object). This lock is also gotten to locate an object in the library cache.

Blocking situations can occur when two sessions compile the same PL/SQL package, or one session is recreating an index while another session is trying to execute a SQL statement that depends on that index.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–23 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'library cache lock' event.

Data Source

(DeltaLibraryCacheLockTime/DeltaServiceTime)*100 where:

- DeltaLibraryCacheLockTime: difference of 'sum of time waited for sessions of foreground processes on the 'library cache lock' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Waiting for a load lock indicates that there is a blocker with a higher or incompatible mode. Locks map to Instance Locks.

The following query will list waiters and the holder of the resource along with the event the resource holder is waiting for.

```
column h_wait format A20
SELECT s.sid,
  waiter.p1raw w_p1r,
  waiter.p2raw w_p2r,
  holder.event h_wait,
  holder.p1raw h_p1r,
  holder.p2raw h_p2r,
  count(s.sid) users_blocked,
  sql.hash_value
FROM
  v$sql sql,
  v$session s,
  x$kgllk l,
  v$session_wait waiter,
  v$session_wait holder
WHERE
  s.sql_hash_value = sql.hash_value and
  l.KGLLKADR=waiter.p2raw and
  s.saddr=l.kgllkuse and
  waiter.event like 'library cache lock' and
  holder.sid=s.sid
GROUP BY
  s.sid,
  waiter.p1raw ,
  waiter.p2raw ,
  holder.event ,
  holder.p1raw ,
  holder.p2raw , s
```

```
ql.hash_value ;
```

4.40.30 Library cache pin (%)

Library cache pins are used to manage library cache concurrency. Pinning an object causes the heaps to be loaded into memory (if not already loaded). PINS can be acquired in NULL, SHARE or EXCLUSIVE modes and can be considered like a special form of lock. A wait for a "library cache pin" implies some other session holds that PIN in an incompatible mode.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–24 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%%% of service time is spent waiting on the 'library cache pin' event.

Data Source

(DeltaLibraryCachePinTime/DeltaServiceTime)*100 where:

- DeltaLibraryCachePinTime: difference of 'sum of time waited for sessions of foreground processes on the 'library cache pin' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

What to do to reduce these waits depends heavily on what blocking scenario is occurring. A common problem scenario is the use of DYNAMIC SQL from within a PL/SQL procedure where the PL/SQL code is recompiled and the DYNAMIC SQL calls something which depends on the calling procedure.

- If there is general widespread waiting then the shared pool may need tuning.
- If there is a blocking scenario, collect evidence as described in the following query and contact Oracle support.

The following query will list the waiters and the session holding the pin, along with the wait event the holder is waiting for.

```
column h_wait format A20
SELECT s.sid,
  waiter.p1raw w_p1r,
  holder.event h_wait,
  holder.p1raw h_p1r,
```

```
  holder.p2raw h_p2r,
  holder.p3raw h_p2r,
  count(s.sid) users_blocked,
  sql.hash_value
FROM
  v$sql sql,
  v$session s,
  x$kglpn p,
  v$session_wait waiter,
  v$session_wait holder
WHERE
  s.sql_hash_value = sql.hash_value and
  p.kglpnhdl=waiter.p1raw and
  s.saddr=p.kglpnuse and
  waiter.event like 'library cache pin' and
  holder.sid=s.sid
GROUP BY
  s.sid,
  waiter.p1raw ,
  holder.event ,
  holder.p1raw ,
  holder.p2raw ,
  holder.p3raw ,
  sql.hash_value ;
```

4.40.31 Local write wait (%)

The wait event can be caused by truncate operations. Truncate operations cause the DBWR to be posted to flush out the space header.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–25 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'local write wait' event.

Data Source

(DeltaLocalWriteWaitTime/DeltaServiceTime)*100 where:

- DeltaLocalWriteWaitTime: difference of 'sum of time waited for sessions of foreground processes on the 'local write wait' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

Wait time: Up to one second, then loop back and check that buffer is clean.

Parameters:

P1: Absolute file number

P2: Block number

See the Idle Events section in this chapter.

User Action

No user action is necessary.

4.40.32 Log buffer space (%)

The system is waiting for space in the log buffer because data is being written into the log buffer faster than LGWR can write it out.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–26 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'log buffer space' event.

Data Source

(DeltaLogBufferSpaceTime/DeltaServiceTime)*100 where:

- DeltaLogBufferSpaceTime: difference of 'sum of time waited for sessions of foreground processes on the 'log buffer space' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Consider making the log buffer bigger if it is small, or moving the log files to faster disks such as striped disks.

4.40.33 Log file switch (archiving needed) (%)

The system is waiting for a log switch because the log being switched into has not been archived yet.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–27 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	1	5	1	%value%% of service time is spent waiting on the 'log file switch (archiving needed)' event.

Data Source

(DeltaLogFileSwitchArchTime/DeltaServiceTime)*100 where:

- DeltaLogFileSwitchArchTime: difference of 'sum of time waited for sessions of foreground processes on the 'log file switch (archiving needed)' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Check the alert file to make sure that archiving has not stopped due to a failed archive write. To speed up archiving consider adding more archive processes or putting the archive files on striped disks.

If the archiver is slow, then it might be prudent to prevent I/O contention between the archiver process and LGWR by ensuring that archiver reads and LGWR writes are separated. This is achieved by placing logs on alternating drives.

4.40.34 Log file switch (checkpoint complete) (%)

Waiting for a log switch because the system cannot wrap into the next log because the checkpoint for that log has not completed.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–28 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	5	50	1	%value%% of service time is spent waiting on the 'log file switch (checkpoint complete) event.

Data Source

(DeltaLogFileSwitchCkptTime/DeltaServiceTime)*100 where:

- DeltaLogFileSwitchCkptTime: difference of 'sum of time waited for sessions of foreground processes on the 'log file switch (checkpoint complete)' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Increase the redo log sizes.

To speed up checkpoint, consider making the buffer cache smaller, or increasing *Parameter:DB_BLOCK_CHECKPOINT_BATCH*, or adding more DBWR processes. You can also enable the checkpoint process by setting the init.ora *Parameter:CHECKPOINT_PROCESS* = TRUE.

4.40.35 Log file switch completion (%)

Waiting for log switch because current log is full and LGWR needs to complete writing to current log and open the new log or some other request to switch log files.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–29 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'log file switch completion' event.

Data Source

(DeltaLogFileSwitchCompleteTime/DeltaServiceTime)*100 where:

- DeltaLogFileSwitchCompleteTime: difference of 'sum of time waited for sessions of foreground processes on the 'log file switch completion' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

For the log file switch (checkpoint incomplete) event:

- Check if there are too few, or too small redo logs. If there are a few redo logs or small redo logs, and the system produces enough redo to cycle through all the logs before DBWR has been able to complete the checkpoint, then increase the size or number of redo logs. This is often the easiest solution but may increase time to recovery.
- Check if DBWR is slow, possibly due to an overloaded or slow I/O system. Check the DBWR write times, check the I/O system, and distribute I/O if necessary.

4.40.36 Log file sync (%)

When a user session COMMITs (or rolls back), the sessions redo information needs to be flushed to the redo log file. The user session will post the LGWR to write all redo required from the log buffer to the redo log file. When the LGWR has finished it will post the user session. The user session waits on this wait event while waiting for LGWR to post it back to confirm all redo changes are safely on disk.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–30 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	30	Not Defined	5	%value%% of service time is spent waiting on the 'log file sync' event.

Data Source

(DeltaLogFileSyncTime/DeltaServiceTime)*100 where:

- DeltaLogFileSyncTime: difference of 'sum of time waited for sessions of foreground processes on the 'log file sync' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

There are 3 main things you can do to help reduce waits on "log file sync":

- Tune LGWR to get good throughput to disk.
  - Do not put redo logs on RAID 5.
  - Place log files on dedicated disks.
  - Consider putting log files on striped disks.
- If there are lots of short duration transactions, see if it is possible to BATCH transactions together so there are fewer distinct COMMIT operations. Each commit has to have it confirmed that the relevant REDO is on disk. Although

commits can be piggybacked by Oracle, reducing the overall number of commits by batching transactions can have a very beneficial effect.

- Determine whether any activity can safely be done with NOLOGGING / UNRECOVERABLE options.

4.40.37 Log switch/archive (%)

Used as part of the 'alter system archive log change *scn*' command. Oracle is basically waiting for the current log from an open thread other than our own to be archived.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–31 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	5	Not Defined	3	%value%% of service time is spent waiting on the 'log switch/archive' event.

Data Source

(DeltaLogSwitchArchTime/DeltaServiceTime)*100 where:

- DeltaLogSwitchArchTime: difference of 'sum of time waited for sessions of foreground processes on the 'log switch/archive' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

No user action is necessary.

4.40.38 Pipe put (%)

The session is waiting for the pipe send timer to expire or for space to be made available in the pipe.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–32 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'pipe put' event.

Data Source

(DeltaPipePutTime/DeltaServiceTime)*100 where:

- DeltaPipePutTime: difference of 'sum of time waited for sessions of foreground processes on the 'pipe put' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

You are dependent on space being freed up on the pipe, so you are not actually dependent on any one session. You can query X$KGLOB to find the pipe name. There is virtually no way of finding the pipe name other than via SQL, as there are no useful addresses.

4.40.39 Row cache lock (%)

This metric is used to wait for a lock on a data dictionary cache specified by "cache id". If one is running in shared mode (Parallel Server), the LCK0 is signaled to get the row cache lock for the foreground waiting on this event. The LCK0 process will get the lock asynchronously. In exclusive mode, the foreground process will try to get the lock.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–33 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'row cache lock' event.

Data Source

(DeltaRowCacheLockTime/DeltaServiceTime)*100 where:

- DeltaRowCacheLockTime: difference of 'sum of time waited for sessions of foreground processes on the 'row cache lock' event' between sample end and start

- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

If this event shows up a lot, consider increasing the shared pool so that more data dictionary can be cached.

4.40.40 SQL*Net break/reset to client (%)

The server is sending a break or reset message to the client. The session running on the server is waiting for a reply from the client.

These waits are caused by an application attempting to:

- Select from a closed cursor
- Select on a cursor after the last row has already been fetched and no data has been returned
- Select on a non-existent table
- Insert a duplicate row into a uniquely indexed table
- Issuing a query with invalid syntax

If the value, v$session_wait.p2, for this parameter equals 0, it means a reset was sent to the client. A non-zero value means that the break was sent to the client.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–34 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'SQL*Net break/reset to client' event.

Data Source

(DeltaNetResetToClientTime/DeltaServiceTime)*100 where:

- DeltaNetResetToClientTime: difference of 'sum of time waited for sessions of foreground processes on the 'SQL*Net break/reset to client' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

Wait time: Up to one second, then loop back and check that buffer is clean.

Parameters:

P1: Absolute file number

P2: Block number

See the Idle Events section in this chapter.

User Action

If these waits are significant, track down the application logic producing these errors to reduce these waits. If you are using Oracle9*i* or higher, check in v$sysstat "parse count (failures)" to see that statements have been parsed where columns or tables are unknown. The statistic "parse count (failures)" does not increase if you send SQL with invalid syntax.

The clearest method to track down the root cause of the error is to run tracing on the users experiencing the wait. Their trace files will contain the SQL statements failing and generating the break/reset wait.

4.40.41 SQL*Net break/reset to dblink (%)

The server is sending a break or reset message to the client. The session running on the server is waiting for a reply from the client.

These waits are caused by an application attempting to:

- Select from a closed cursor
- Select on a cursor after the last row has already been fetched and no data has been returned
- Select on a non-existent table
- Insert a duplicate row into a uniquely indexed table
- Issuing a query with invalid syntax

If the value, v$session_wait.p2, for this parameter equals 0, it means a reset was sent to the client. A non-zero value means that the break was sent to the client.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–35 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'SQL*Net break/reset to dblink' event.

Data Source

(DeltaNetResetToDblinkTime/DeltaServiceTime)*100 where:

- DeltaNetResetToDblinkTime: difference of 'sum of time waited for sessions of foreground processes on the 'SQL*Net break/reset to dblink' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

If these waits are significant, track down the application logic producing these errors to reduce these waits. If you are using Oracle9*i* or higher, check in v$sysstat "parse count (failures)" to see that statements have been parsed where columns or tables are unknown. The statistic "parse count (failures)" does not increase if you send SQL with invalid syntax.

4.40.42 SQL*Net message to client (%)

The shadow process is waiting for confirmation of a send to the client process.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–36 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'SQL*Net message to client' event.

Data Source

(DeltaNetMsgToClientTime/DeltaServiceTime)*100 where:

- DeltaNetMsgToClientTime: difference of 'sum of time waited for sessions of foreground processes on the 'SQL*Net message to client' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

This event could indicate network latency problems.

4.40.43 SQL*Net message to dblink (%)

The shadow process is waiting for confirmation of a send to the client process.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–37 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'SQL*Net message to dblink' event.

Data Source

(DeltaNetMsgToDblinkTime/DeltaServiceTime)*100 where:

- DeltaNetMsgToDblinkTime: difference of 'sum of time waited for sessions of foreground processes on the 'SQL*Net message to dblink' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

This event could indicate network latency problems.

4.40.44 SQL*Net more data from client (%)

The shadow process has received part of a call from the client process (for example, SQL*Plus, Pro*C, and JDBC) in the first network package and is waiting for more data for the call to be complete. Examples are large SQL or PL/SQL block and insert statements with large amounts of data.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–38 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'SQL*Net more data from client' event.

Data Source

(DeltaNetMoreFromClientTime/DeltaServiceTime)*100 where:

- DeltaNetMoreFromClientTime: difference of 'sum of time waited for sessions of foreground processes on the 'SQL*Net more data from client' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

This event could indicate:

- Network latency problems
- tcp_no_delay configuration issues
- Large array insert
- Soft parsing, shipping SQL and PL/SQL text. Using stored procedures and packages will help alleviate this problem.

4.40.45 SQL*Net more data from dblink (%)

The shadow process has received part of a call from the client process (for example, SQL*Plus, Pro*C, and JDBC) in the first network package and is waiting for more data for the call to be complete. Examples are large SQL or PL/SQL block and insert statements with large amounts of data.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–39 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'SQL*Net more data from dblink' event.

Data Source

(DeltaNetMoreFromDblinkTime/DeltaServiceTime)*100 where:

- DeltaNetMoreFromDblinkTime: difference of 'sum of time waited for sessions of foreground processes on the 'SQL*Net more data from dblink' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

This event could indicate:

- Network latency problems
- tcp_no_delay configuration issues
- Large array insert
- Large number of columns or wide column data

4.40.46 SQL*Net more data to client (%)

The shadow process has completed a database call and is returning data to the client process (for example SQL*Plus). The amount of data being sent requires more than one send to the client. The shadow process waits for the client to receive the last send. This happens, for example, in a SQL statement that returns a large amount of data.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–40 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'SQL*Net more data to client' event.

Data Source

(DeltaNetMoreToClientTime/DeltaServiceTime)*100 where:

- DeltaNetMoreToClientTime: difference of 'sum of time waited for sessions of foreground processes on the 'SQL*Net more data to client' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

This event could indicate:

- Network latency problems
- tcp_no_delay configuration issues
- Large array insert
- Large number of columns or wide column data

4.40.47 SQL*Net more data to dblink (%)

The shadow process has completed a database call and is returning data to the client process (for example SQL*Plus). The amount of data being sent requires more than one send to the client. The shadow process waits for the client to receive the last send. This happens, for example, in a SQL statement that returns a large amount of data.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–41 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'SQL*Net more data to dblink' event.

Data Source

(DeltaNetMoreToDblinkTime/DeltaServiceTime)*100 where:

- DeltaNetMoreToDblinkTime: difference of 'sum of time waited for sessions of foreground processes on the 'SQL*Net more data to dblink' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

This event could indicate:

- Network latency problems
- tcp_no_delay configuration issues
- Large array insert
- Large number of columns or wide column data

4.40.48 Wait Time (%)

This metric represents the percentage of time spent waiting, instance-wide, for resources or objects during this sample period.

This test checks the percentage time spent waiting, instance-wide, for resources or objects during this sample period. If the % Wait Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–42 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	Not Defined	Not Defined	3	%value%% of database service time is spent waiting.

Table 4–43 Metric Summary Table

Target Version	Server Evaluation Frequency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	Every Minute	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	3	Generated By Database Server

Data Source

DeltaTotalWait / (DeltaTotalWait + DeltaCpuTime) where:

- DeltaTotalWait: difference of 'sum of time waited for all wait events in v$system_event' between sample end and start
- DeltaCpuTime: difference of 'select value from v$sysstat where name='CPU used by this session' between sample end and start

User Action

Investigate further into which specific wait events are responsible for the bulk of the wait time. Individual wait events may identify unique problems within the database. Diagnosis will be tailored where appropriate through drilldowns specific to individual wait events.

4.40.49 Write complete waits (%)

The session is waiting for a buffer to be written. The write is caused by normal aging or a cross instance call.

A user wants to modify a block that is part of DBWRs current write batch. When DBWR grabs buffers to write, it marks them as 'being written'. All the collected buffers are then written to disk. The wait 'write complete waits' implies we wanted a buffer while this flag was set. The flags are cleared as each buffer is written.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–44 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	20	Not Defined	3	%value%% of service time is spent waiting on the 'write complete waits' event.

Data Source

(DeltaWriteCompleteWaitsTime/DeltaServiceTime)*100 where:

- DeltaWriteCompleteWaitsTime: difference of 'sum of time waited for sessions of foreground processes on the 'write complete waits' event' between sample end and start
- DeltaServiceTime: difference of 'sum of time waited for sessions of foreground processes on events not in IdleEvents + sum of 'CPU used when call started' for sessions of foreground processes' between sample end and start

See the Idle Events section in this chapter.

User Action

Multiple DBWRs, ASYNC_IO and/or increasing the size of the buffer cache may help reduce waits.

4.41 Wait by Session Count

This metric category contains the metrics that represent the number of sessions waiting on each non-idle wait event. High waiting levels are caused by excessive contention.

4.41.1 Session Waiting for Event Count

This metric represents the number of sessions waiting on a given wait event at the sample time.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–45 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
8.1.7.4; 9.0.1.x; 9.2.0.x	Every Minute	After Every Sample	>	Not Defined	Not Defined	3	%value% sessions are waiting for event %event%.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Wait Event" object.

If warning or critical threshold values are currently set for any "Wait Event" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Wait Event" object, use the Edit Thresholds page.

Data Source

For each metric index:

```
select count (1)
```

User Action

Evaluate the various types of wait activity using the real-time and historical performance monitoring capabilities of Enterprise Manager.

4.42 Waits by Wait Class

This metric category contains the waits by wait class metrics.

4.42.1 Average Users Waiting Count

This metric represents the average number of users that have made a call to the database and that are waiting for an event, such as an I/O or a lock request, to complete. If the number of users waiting on events increases, it indicates that either more users are running, increasing workload, or that waits are taking longer, for example when maximum I/O capacity is reached and I/O times increase.

Metric Summary for Database Control and Grid Control

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding

Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–46 Metric Summary Table

Target Version	Key	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	class: "Administrative"	Every 15 Minutes	After Every Sample	>	10	Not Defined	1	Not Defined
10.1.0.x	class: "Application"	Every 15 Minutes	After Every Sample	>	10	Not Defined	1	Not Defined
10.1.0.x	class: "Cluster"	Every 15 Minutes	After Every Sample	>	30	Not Defined	1	Not Defined
10.1.0.x	class: "Commit"	Every 15 Minutes	After Every Sample	>	30	Not Defined	1	Not Defined
10.1.0.x	class: "Concurrency"	Every 15 Minutes	After Every Sample	>	10	Not Defined	1	Not Defined
10.1.0.x	class: "Configuration"	Every 15 Minutes	After Every Sample	>	10	Not Defined	1	Not Defined
10.1.0.x	class: "Network"	Every 15 Minutes	After Every Sample	>	10	Not Defined	1	Not Defined
10.1.0.x	class: "Other"	Every 15 Minutes	After Every Sample	>	10	Not Defined	1	Not Defined
10.1.0.x	class: "Scheduler"	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Not Defined
10.1.0.x	class: "System I/O"	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Not Defined
10.1.0.x	class: "User I/O"	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Not Defined

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Wait Class" object.

If warning or critical threshold values are currently set for any "Wait Class" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Wait Class" object, use the Edit Thresholds page.

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page.

4.42.2 Database Time Spent Waiting (%)

This metric represents the percentage of time that database calls spent waiting for an event. Although there is no correct value for this metric, it can be used to detect a change in the operation of a system, for example, an increase in Database Time Spent

Waiting from 50% to 75%. ('No correct value' means that there is no single value that can be applied to any database. The value is a characteristic of the system and the applications running on the system.)

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 4–47 Metric Summary Table

Target Version	Key	Server Evaluation Frequency	Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
10.1.0.x	class: "Administrative"	Every Minute	Every 15 Minutes	After Every Sample	>	30	Not Defined	1	Generated By Database Server
10.1.0.x	class: "Application"	Every Minute	Every 15 Minutes	After Every Sample	>	30	Not Defined	1	Generated By Database Server
10.1.0.x	class: "Cluster"	Every Minute	Every 15 Minutes	After Every Sample	>	50	Not Defined	1	Generated By Database Server
10.1.0.x	class: "Commit"	Every Minute	Every 15 Minutes	After Every Sample	>	50	Not Defined	1	Generated By Database Server
10.1.0.x	class: "Concurrency"	Every Minute	Every 15 Minutes	After Every Sample	>	30	Not Defined	1	Generated By Database Server
10.1.0.x	class: "Configuration"	Every Minute	Every 15 Minutes	After Every Sample	>	30	Not Defined	1	Generated By Database Server
10.1.0.x	class: "Network"	Every Minute	Every 15 Minutes	After Every Sample	>	30	Not Defined	1	Generated By Database Server
10.1.0.x	class: "Other"	Every Minute	Every 15 Minutes	After Every Sample	>	30	Not Defined	1	Generated By Database Server
10.1.0.x	class: "Scheduler"	Every Minute	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Generated By Database Server
10.1.0.x	class: "System I/O"	Every Minute	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Generated By Database Server
10.1.0.x	class: "User I/O"	Every Minute	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Generated By Database Server

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Wait Class" object.

If warning or critical threshold values are currently set for any "Wait Class" object, those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Wait Class" object, use the Edit Thresholds page.

User Action

View the latest Automatic Database Diagnostic Monitor (ADDM) report. For a more detailed analysis, run ADDM from the Advisor Central link on the Database Home page. ADDM will highlight the source of increased time spent in wait events.

5 Listener

You can use Enterprise Manager to manage Oracle Listener targets. From the Enterprise Manager Listener home page, you can monitor key metrics that can help determine the performance and availability of the listener and help you troubleshoot potential performance problems.

5.1 General Status

This metric is a container for a set of metrics that provide general information about the listener target. For more information, see the section on Listener Administration in the *Oracle Database Net Services Administrator's Guide 10g Release 2 (10.2)*.

The following table lists the metrics, their descriptions, and data sources.

Table 5–1 General Status Metrics

Metric	Description	Data Source
Alias	Alternative name for the listener. On the Metric Detail page, you can see the value of this metric only when you select one of the Real Time refresh options. The alias also appears on the Listener home page.	Derived from the STATUS command of the Listener Control Utility
Security	Shows whether or not a password is required to run specific commands with the Listener Control Utility	Derived from the STATUS command of the Listener Control Utility
SID List	Lists the System Identifiers (SIDs) for the services monitored by the listener	List of SIDs for the listener is stored in the `listener.ora` configuration file
SNMP Status	Indicates whether or not the listener can respond to queries from an SNMP-based network management system	Derived from the `STATUS` command of the Listener Control Utility
Start Date	Represents the day and time when the listener was last started. On the Metric Detail page, you can see the value of this metric only when you select one of the Real Time refresh options. This metric also appears on the Enterprise Manager Listener home page.	Derived from the `STATUS` command of the Listener Control Utility
TNS Address	Displays the protocol, host, and port information for the listener. On the Metric Detail page, you can see the value of this metric only when you select one of the Real Time refresh options. The TNS address also appears on the Listener home page.	TNS address of the Listener is defined in the `listener.ora` configuration file

Table 5–1 (Cont.) General Status Metrics

Metric	Description	Data Source
Trace Level	Represents the level of tracing currently enabled for the listener. Tracing can be used to troubleshoot problems with the listener by saving additional information to the trace file. For more information about the trace levels you can set for the listener, see the information about the Listener Control Utility in the *Oracle Database Net Services Reference Guide 10g Release 2 (10.2)*. On the Metric Detail page, you can see the value of this metric only when you select one of the Real Time refresh options.	Derived from the `STATUS` command of the Listener Control Utility
Version	Version of the listener software. On the Metric Detail page, you can see the value of this metric only when you select one of the Real Time refresh options. This metric also appears on the Enterprise Manager Listener home page.	Derived from the `STATUS` command of the Listener Control Utility

5.2 Load

This metric is a container for a set of metrics that provide you with information about the number of connections supported by the Listener over a period of time. For more information, see the section on Listener Administration in the *Oracle Database Net Services Administrator's Guide 10g Release 2 (10.2)*.

The following table lists the metrics, their descriptions, data sources, and user actions.

Table 5–2 Load Metrics

Metric	Description	Data Source	User Action
Connections Established	Number of connections established since the listener was last started	Derived from the `SERVICES` command of the Listener Control Utility	If you are noticing experiencing performance issues with the database or other services supported by the listener, review the historical values of this metric to determine whether or not the performance problems are caused by excessive load on the listener or host.
Connections Established (per min)	Average number of connections per minute that were established with the listener	Derived from the Listener Control Utility	If you are noticing experiencing performance issues with the database or other services supported by the listener, review the historical values of this metric to determine whether or not the performance problems are caused by excessive load on the listener or host.
Connections Refused	Number of connections to the listener that were refused. A connection can be refused for a variety of reasons, including situations where the database or other listener service is down, or if the connection timed out.	Derived from the `SERVICES` command of the Listener Control Utility	If Enterprise Manager reports a high number of refused connections, check the availability and performance of the database or other services supported by the listener.

Table 5–2 (Cont.) Load Metrics

Metric	Description	Data Source	User Action
Connections Refused (per min)	Average number of connections that were refused per minute	Derived from the Listener Control Utility	If Enterprise Manager reports a high number of refused connections, check the availability and performance of the database or other services supported by the listener.

5.3 Response

This metric is a container for the Response and Status metrics that provide you with performance information about the Listener.

5.3.1 Response Time (msec)

This metric represents the time (in milliseconds) that it takes for the Listener to respond to a network request (ping).

By default, this metric has a critical threshold of 100 and a warning threshold of 80. A critical alert is generated when the metric value exceeds the critical threshold value 1 time. A warning alert is generated when the metric value exceeds the warning threshold value 1 time. You can edit the value for a threshold as required.

By default, Enterprise Manager tests the value of this metric every 24 hours.

When an alert is generated, the alert text is:

```
Listener response to a TNS ping is %value% msecs
```

Data Source

The value of this metric is derived using the `TNSPING` command. For more information about the `TNSPING` command, see the *Oracle Database Net Services Administrator's Guide 10g Release 2 (10.2)*.

User Action

If the Listener response time consistently exceeds the threshold, users are likely experiencing performance issues while accessing the database or other services on this host. Use the Enterprise Manager Central Console to review other performance indicators, such as the overall health of your database and the response time of your hosts and Web Applications.

5.3.2 Status

This metric returns a value of "1" if the Listener is up and running; it returns a 0 if the Listener is unavailable.

By default, this metric has a critical threshold of 0. A critical alert is generated when the metric value equals the critical threshold value 1 time. You can edit the value for a threshold as required.

By default, Enterprise Manager tests the value of this metric every 24 hours.

When an alert is generated, the alert text is:

```
The listener is down: %oraerr%.
```

Data Source

This metric is derived from the `STATUS` command in the Listener Control Utility. For more information, see the *Oracle Database Net Services Administrator's Guide 10g Release 2 (10.2)*.

User Action

When the listener is down, users cannot access the database or other services on this host. Review the troubleshooting information in *Oracle Database Net Services Administrator's Guide 10g Release 2 (10.2*).

6

Ultra Search

This represents an Oracle Ultra Search database repository.

6.1 Response

This represents the Oracle Ultra Search repository up/down status.

6.1.1 Status

This represents the Oracle Ultra Search repository up/down status.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 6–1 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 5 Minutes	After Every Sample	=	Not Defined	0	1	Ultra Search is down

6.2 Ultra Search Crawler Status

This represents schedule status. The following table lists the metrics and their descriptions.

Note: For all target versions, the collection frequency for each metric is every 15 minutes.

Table 6–2 Ultra Search Crawler Status Metrics

Metric	Description
Instance Name	Ultra Search instance name
Schedule Finish Time	Means that the time schedule is finished
Schedule Frequency	Represents how often the crawler will be invoked to collect data

Table 6–2 (Cont.) Ultra Search Crawler Status Metrics

Metric	Description
Schedule Name	Schedule name
Schedule State	See Section 6.2.1, "Schedule State"

6.2.1 Schedule State

This represents schedule status.

Metric Summary

The following table shows how often the metric's value is collected and compared against the default thresholds. The 'Consecutive Number of Occurrences Preceding Notification' column indicates the consecutive number of times the comparison against thresholds should hold TRUE before an alert is generated.

Table 6–3 Metric Summary Table

Target Version	Evaluation and Collection Frequency	Upload Frequency	Operator	Default Warning Threshold	Default Critical Threshold	Consecutive Number of Occurrences Preceding Notification	Alert Text
All Versions	Every 15 Minutes	After Every Sample	CONTAINS	FINISHED	FAILED	1	Crawler status is %value%

Multiple Thresholds

For this metric, you can set different warning and critical threshold values for each "Schedule ID" object.

If warning or critical threshold values are currently set for any "Schedule ID" object, then those thresholds can be viewed on the Metric Detail page for this metric.

To specify or change warning or critical threshold values for each "Schedule ID" object, use the Edit Thresholds page.