Oracle® Enterprise Manager

Oracle Collaboration Suite Metric Reference Manual

10*g* Release 2 (10.2)

B25985-01

January 2006

ORACLE®

Oracle Enterprise Manager Oracle Collaboration Suite Metric Reference Manual 10*g* Release 2 (10.2)

B25985-01

Contents

95 Routing Service

96 SMDI Monitor Service

97 Telephony Monitor Service

98 Voicemail and Fax

99 Voicemail and Fax Application

100 Voicemail and Fax Fax Service

101 Voicemail and Fax Service

102 Voicemail and Fax Recording Service

103 Voicemail and Fax Retrieval Service

Preface

This manual is a compilation of the Oracle Collaboration Suite target metrics provided in Oracle Enterprise Manager.

Audience

This document is intended for Oracle Enterprise Manager users interested in Oracle Collaboration Suite target metrics.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, see the following documents in the Oracle Enterprise Manager 10*g* Release 2 documentation set:

- *Oracle Enterprise Manager Framework, Host, and Third-Party Metric Reference Manual*
- *Oracle Enterprise Manager Oracle Database and Database-Related Metric Reference Manual*
- *Oracle Enterprise Manager Oracle Application Server Metric Reference Manual*
- *Oracle Enterprise Manager Concepts*
- *Oracle Enterprise Manager Grid Control Quick Installation Guide*
- *Oracle Enterprise Manager Grid Control Installation and Basic Configuration*
- *Oracle Enterprise Manager Configuration for Oracle Collaboration Suite*
- *Oracle Enterprise Manager Advanced Configuration*
- *Oracle Enterprise Manager Policy Reference Manual*
- *Oracle Enterprise Manager Extensibility*
- *Oracle Enterprise Manager Command Line Interface*
- *Oracle Enterprise Manager SNMP Support Reference Guide*
- *Oracle Enterprise Manager Licensing Information*

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

This preface describes:

Structure of the Metric Reference Manual

This manual contains a chapter for each Enterprise Manager Oracle Collaboration Suite target 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 Collaboration Suite 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
IMAP	Interactive Mail Access Protocol
LDAP	Lightweight Directory Access Protocol
OID	Oracle Internet Directory
OVF	Oracle Voicemail & FAX
POP	Post Office Protocol
SMTP	Simple Mail Transfer Protocol

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.

Part I

Oracle Collaboration Suite Metrics

Part I provides the metrics related to the Oracle Collaboration Suite targets.

Part I contains the following chapters:

1

Calendar Application Redundancy Group

The Calendar Application Redundancy Group target is a grouping of Calendar application agent monitored targets that have identical configuration, characteristics, and functionality. While a single Calendar application instance is vulnerable to the failure of its host or system, a redundant group of Calendar Applications continues to function despite the loss of a Calendar application instance, hiding any such failure from clients, and allowing other Calendar application instances in the group to service the requests.

1.1 Response

The Response category checks and displays whether or not the Calendar applications are available.

1.1.1 Status

This metric displays the status of the Calendar applications. Its status is "up" as long as at least one of the Calendar applications is available.

User Action

If the Status of Calendar Application Redundancy Group is down, then check the status of the individual Calendar applications to identify which particular application is down.

2

Calendar Applications

Lists the metrics for the Oracle Calendar application system processes.

2.1 Calendar Applications DB Size

Monitors the availability of the disk space where the OCAS/sessiondb and OCAS/linkdb exist. The threshold is set if the availabilities are less than 10% and 5%, respectively.

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 2–1 Calendar Applications DB Size Metrics

Metric	Description
% Disk Space Available	Section 2.1.1, "% Disk Space Available"
Filesystem	Name of the filesystem where the Oracle Calendar application system is installed
Mounted on	Mounted drive or directory where the Oracle Calendar application system is located
Total Disk Space (Kb)	Total space in the filesystem where the Oracle Calendar application system is installed
Total Size (Mb)	Total database size of the Oracle Calendar application system, in megabytes
Total Space Free (Kb)	Total available space in the filesystem where the Oracle Calendar application system is installed
Total Space Used (Kb)	Total space used in the filesystem where the Oracle Calendar application system is installed

2.1.1 % Disk Space Available

The percentage of total space used on the file system where the Oracle Calendar application system is installed.

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 2–2 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	<	10	5	1	Not Defined

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "DB Directory" 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 "DB Directory" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

2.2 Calendar Applications Processes Info

This metric will list the following Oracle Calendar application system processes:

1. 1= CPU Time
2. 1= Memory Usage
3. 2= Elapsed time since the start of the process

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 2–3 Calendar Applications Processes Info Metrics

Metric	Description
CPU Time	CPU consumption percentage of the Oracle Calendar application system process. This will be displayed for the ten most active processes collected
Elapsed Time	Elapsed time since the associated Oracle Calendar application system process was started, in the form: [[dd-]hh:]mm:ss where dd is the number of days, hh is the number of hours, mm is the number of minutes and ss is the number of seconds This will be displayed for the ten most active processes collected.
Memory Size (Kb)	See Section 2.2.1, "Memory Size (Kb)"
PID	Decimal value of the Oracle Calendar application system process ID. This will be displayed for the ten most active processes.

2.2.1 Memory Size (Kb)

In kilobytes, the total size of the associated Oracle Calendar application system process in virtual memory. This will be displayed for the ten most active processes collected.

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 2–4 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	>	Not Defined	50000	1	Not Defined

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Calendar Process" 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 "Calendar Process" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

2.3 Response

This metric displays the response time of reaching the Systems web page of the Oracle Calendar application system.

2.3.1 Response Time

The response time, in milliseconds, of reaching the Systems page of the Oracle Calendar application system.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

2.3.2 Status Code

Depending on the response time, the status of the Oracle Calendar application system is set. A threshold is set for this metric if it is not 0.

1. 0= Okay
2. 1= Timed out
3. 2= The service is probably down

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 2–5 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	=	1	2	1	Not Defined

3

Calendar Server

This metric will monitor the ten most active calendar processes sorted in descending order on CPU consumption followed by memory consumption.

3.1 Calendar DB Size

This metric will monitor the disk space where the Oracle Calendar database resides. A threshold is set for the availability of this disk space. If the Oracle Calendar database is mounted on a shared disk, this metric will not reflect just the Oracle Calendar database, but the shared usage of the Oracle Calendar database and all other applications mounted on the disk.

> **Note:** For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 3–1 Calendar DB Size Metrics

Metric	Description
% Disk Space Available	See Section 3.1.1, "% Disk Space Available"
Filesystem	Filesystem type where the Oracle Calendar server is installed
Mounted on	Mounted drive or directory on which the Oracle Calendar server is located
Total Disk Space (MB)	Total disk size of this filesystem, in megabytes
Total Size (MB)	Total size of the Oracle Calendar server database, in megabytes
Total Space Free (MB)	Total disk space available in the filesystem where the Oracle Calendar server is installed
Total Space Used (MB)	Total space used in the filesystem where the Oracle Calendar server is installed

3.1.1 % Disk Space Available

The percent of total space available on the filesystem where the Oracle Calendar server is installed.

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 3–2 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	<	10	5	1	Not Defined

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "DB Directory" 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 "DB Directory" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

3.2 Calendar Server Top Processes

This metric will monitor the ten most active Oracle Calendar server processes, sorted in descending order based on CPU consumption, followed by memory consumption.

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 3–3 Calendar Server Top Processes Metrics

Metric	Description
CPU Time	Will monitor the percentage of CPU consumption used by the ten most active calendar server processes
Elapsed Time	Elapsed time since the associated Oracle Calendar server process was started, in the form: [[dd-]hh:]mm:ss where dd is the number of days, hh is the number of hours, mm is the number of minutes and ss is the number of seconds This will be displayed for the ten most active processes collected.
Memory Size (MB)	Total size, in kilobytes, of the associated Oracle Calendar server process in virtual memory. This will be displayed for the ten most active processes collected.
PID	Decimal value of the Oracle Calendar server process ID. This will be displayed for the ten most active processes collected.

3.3 Connections

This metric collects information about the number of connections made to the calendar server system.

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 3–4 Connections Metrics

Metric	Description
Number of Dedicated Connections	Total number of dedicated connections, including connections made by desktop clients such as Oracle Calendar, Oracle Connector For Outlook, or any calendar SDK based application.
Number of Reserved Connections	See Section 3.3.1, "Number of Reserved Connections".
Number of Shared Connections	Total number of shared connections made by web based applications, such as the Oracle Calendar Web client interface and Oracle Calendar Sync. These applications establish a connection pool to the calendar server that is shared among all connected users.
Total Number of Calendar Connections	Total number of connections made to the calendar server of any type.

3.3.1 Number of Reserved Connections

The total number of reserved connections made by the server internally, usually relating the SNC engine and the CWS. If the calendar server has multiple nodes, then the reserved number of calendar connections should be proportional to the number of node network connections. A threshold is set for this metric if the value is too low.

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	After Every Sample	<	Not Defined	2	1	Not Defined

3.4 Current Requests in CWS Queue

The number of wireless notification/reminder requests currently in the queue. A threshold is set for this metric if it is too high.

3.4.1 Alert Requests

The number of wireless notification/reminder requests currently in the queue. A threshold is set for this metric if the value is too high.

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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	100	1	Not Defined

3.4.2 Mail Requests

The number of node-to-node replication requests currently in the queue. A threshold is set for this metric if the value is too high.

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 3–7 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 5 Minutes	After Every Sample	>	Not Defined	100	1	Not Defined

3.4.3 Replication Requests

The number of node-to-node event replications requests currently in the queue. A threshold is set for this metric if it is too high.

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	After Every Sample	>	Not Defined	100	1	Not Defined

3.4.4 Web Conf. Requests

The number of requests for Web Conference items currently in the queue. A threshold is set for this metric if the value is too high.

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	After Every Sample	>	Not Defined	100	1	Not Defined

3.5 CWS Cumulative Queue Stats

This metric provides information about the cumulative number of requests processed by the CWS.

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 3–10 CWS Cumulative Queue Stats Metrics

Metric	Description
Mail Requests Errors	See Section 3.5.1, "Mail Requests Errors"
Mail Requests Processed	Number of mail notification requests processed successfully, since the last interval, by the CWS
Replication Requests Errors	See Section 3.5.2, "Replication Requests Errors"
Replication Requests Processed	Total number of node-to-node Replication requests successfully processed by the CWS
SSR Requests Errors	See Section 3.5.3, "SSR Requests Errors"
SSR Requests Processed	Total number of Server Side Reminder requests successfully processed by the CWS
Wireless Requests Errors	See Section 3.5.4, "Wireless Requests Errors"
Wireless Requests Processed	Total number of wireless notification requests successfully processed by the CWS

3.5.1 Mail Requests Errors

The number of mail requests processed by the CWS that contain errors.

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 5 Minutes	After Every Sample	>	Not Defined	100	1	Not Defined

3.5.2 Replication Requests Errors

The total number of node-to-node Replication requests processed by the CWS that contain errors.

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 3–12 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 5 Minutes	After Every Sample	>	Not Defined	100	1	Not Defined

3.5.3 SSR Requests Errors

The total number of Server Side Reminder requests processed by the CWS that contain errors.

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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	100	1	Not Defined

3.5.4 Wireless Requests Errors

The number of errors in the processed wireless requests.

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 3–14 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	100	1	Not Defined

3.6 Response

Total transaction time for sending 64Kb of data to the calendar server and receiving a reply back (tests all nodes). This transaction time includes connecting and authenticating to the server.

3.6.1 Status

Displays the status of the calendar server and returns a status of Up, Partially Up or Down

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

3.6.2 Status Code

The status code of the calendar server. Status code 0 indicates a normal calendar server status. Status code 1 indicates the calendar server is running, but partially. Status code 2 indicates the calendar server is either down or running inconsistently.

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 3–15 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
All Versions	Every 5 Minutes	After Every Sample	=	1	2	1	Not Defined

3.7 Response Time (64Kb)

This metric is used to calculate the response time of the calendar server.

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 3–16 Response Time (64 Kb) Metrics

Metric	Description
Time Excluding Authentication OH (ms)	Total transaction time, excluding authentication, for sending 64Kb of data to the calendar server and receiving a reply (tests all nodes
Time Excluding Connection OH (ms)	Total transaction time, excluding connection time, for sending 64Kb of data to the calendar server and receiving a reply (tests all nodes
Total Transaction Time (ms)	See Section 3.7.1, "Total Transaction Time (ms)"

3.7.1 Total Transaction Time (ms)

The total transaction time, including authentication, for sending 64Kb of data to the calendar server and receiving a reply (tests all nodes).

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 5 Minutes	After Every Sample	>	10000	20000	1	Not Defined

4

Calendar Server Redundancy Group

The Calendar Server Redundancy Group target is a grouping of all Calendar server agent monitored targets that have identical configuration, characteristics, and functionality. While a single Calendar server instance is vulnerable to the failure of its host or system, a redundant group of Calendar Servers continues to function despite the loss of a Calendar server instance, hiding any such failure from clients, and allowing other Calendar server instances in the group to service the requests.

4.1 Connections

The Connections category provides information about the number of connections made to the Calendar servers.

> **Note:** For Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 4–1 Connections Metrics

Metric	Description
Number of Reserved Connections	Total number of reserved connections made by the server internally, usually relating the SNC engine and the CWS. The value is the sum of all reserved connections on the Calendar Server agent monitored target
Number of Shared Connections	Total number of shared connections made by Web applications, such as the Oracle Calendar Web client interface and Oracle Calendar Sync. These applications establish a connection pool to the Calendar server that is shared among all connected users. The value is the sum of all shared connections on the Calendar Server agent monitored targets.
Total Number of Calendar Connections	Total number of connections made to the Calendar server of any type. The value is the sum of all the connections on the Calendar Server agent monitored targets
Users-Native Client	Total number of dedicated connections, including connections made by desktop clients such as Oracle Calendar, Oracle Connector For Outlook, or any Calendar SDK based application. The value is the sum of all dedicated connections on the Calendar Server agent monitored targets

4.2 QueueStats

The QueueStats category show the number of wireless notification/reminder requests currently in queue.

Note: For Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 4–2 QueueStats Metrics

Metric	Description
Alert Requests	Number of wireless notification/reminder requests currently in queue. The value is the sum of all alert requests on the Calendar Server agent monitored targets.
Mail Requests	Number of mail requests currently in queue. The value is the sum of all mail requests on the Calendar Server agent monitored targets.
Replication Requests	Number of node-to-node replication requests currently in queue. The value is the sum of all replication requests on the Calendar Server agent monitored targets.
Web Conf. Requests	Number of requests for Web Conference items currently in queue. The value is the sum of all Web Conference requests on the Calendar Server agent monitored targets.

4.3 Response

The Response category captures the response characteristics of the Calendar server as seen by a client application.

4.3.1 Status

This metric displays the status of the Calendar server. The status is "up" as long as at least one of the Calendar server agent monitoring targets is available.

User Action

If the Status of Calendar Server Redundancy Group is down, then check the status of the individual Calendar server agent monitored targets to identify which particular one is down.

5

Calendar Service

The Calendar Service target represents the user functionality provided by Calendar. It includes the Calendar User Access Service, which represents user access to Calendar.

5.1 Connections

The Connections category provides information about the number of connections made to the Calendar servers.

5.1.1 Users - Native client (current)

This metric shows the total number of dedicated connections on the Calendar servers, including connections made by desktop clients such as Oracle Calendar, Oracle Connector For Outlook, or any Calendar SDK based application. The value is the sum of all dedicated connections on the Calendar Server Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

5.2 Response

The Response category checks and displays whether or not the Calendar Services are available.

5.2.1 Status

This metric shows whether or not the Calendar Services are available. The status is "up" only when all the Calendar Services are available.

User Action

If the Status of the Calendar Service is down, then check the results obtained by Root Cause Analysis on the Calendar Service Home Page.

5.3 Response Time

The Response Time category provides information about the time taken by all the Calendar Services to service their transactions.

5.3.1 User Action Total Time (ms)

This metric shows the total time taken by Calendar Services to service their transactions (including login time and connection time). The value is the sum of the time taken by all Calendar Web Applications.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

6

Calendar User Access Service

Calendar User Access Service represents user accessible functions of Calendar. A Calendar User Access service includes the Calendar Web Application Service.

6.1 Connections

The Connections category provides information about the number of connections made to the Calendar server. The following table lists the metrics and their descriptions.

Note: For Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

Table 6–1 Connections Metrics

Metric	Description
Number of Reserved Connections	Total number of reserved connections made by the server internally, usually relating to the SNC engine and the CWS. If the Calendar server has multiple nodes, then the reserved number of Calendar connections should be proportional to the number of node network connections. The value is the sum of all reserved connections on the Calendar Server Redundancy Group.
Number of Shared Connections	Total number of shared connections made by Web applications (e.g. Oracle Calendar Web client interface). These applications establish a connection pool to the Calendar server that is shared among all connected users. The value is the sum of all shared connections on the Calendar Server Redundancy Group.
Total Number of Calendar Connections	Total number of connections made to the Calendar server of any type. The value is the sum of all connections on the Calendar Server Redundancy Group.
Users - Native Client (current)	Total number of dedicated connections, including connections made by desktop clients such as Oracle Calendar, Oracle Connector For Outlook, or any Calendar SDK based application. The value is the sum of all dedicated connections on the Calendar Server Redundancy Group.

6.2 QueueStats

The QueueStats category show the number of wireless notification/reminder requests currently queued. The following table lists the metrics and their descriptions.

Note: For Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

Table 6–2 QueueStats Metrics

Metric	Description
Alert Requests	Number of wireless notification/reminder requests currently queued. The value is the sum of all alert requests on the Calendar Server Redundancy Group.
Mail Requests	Number of mail requests currently queued. The value is the sum of all mail requests on the Calendar Server Redundancy Group.
Replication Requests	Number of node-to-node replication requests currently queued. The value is the sum of all replication requests on the Calendar Server Redundancy Group.
Web Conf. Requests	Number of requests for Web Conference items currently queued. The value is the sum of all Web Conference requests on the Calendar Server Redundancy Group.

6.3 Response

The Response category checks and displays whether or not the Calendar User Access Service (i.e. Calendar Web Application) is available.

6.3.1 Status

This metric displays the status of the Calendar User Access Service. The status is "up" only when the Calendar Web Applications are available.

User Action

If the Status of Calendar User Access Service is down, then check the results obtained by Root Cause Analysis on the Calendar User Access Service Home Page.

6.4 Response Time

The Response Time category provides information about the time taken by the Calendar Web Application to service a transaction.

6.4.1 User Action TotalTime (ms)

This metric shows the total time taken by Calendar Web Applications to service their transactions (including login time and connection time).

Note: For Version 1.0, the evaluation and collection frequency for this metric is every 15 minutes.

7

Collaboration Suite Search Admin Aggregate Service

The Collaboration Suite Search Admin Aggregate Service target is a grouping of the Collaboration Suite Search Admin Service and Collaboration Suite Search Crawler Service.

7.1 Response

The Response category checks and displays whether or not the Collaboration Suite Search Admin Aggregate Services are available.

7.1.1 Status

This metric shows whether or not the Collaboration Suite Search Admin Aggregate Services are available. The status is "up" only when all the Collaboration Suite Search Admin Aggregate Services are available.

User Action

If the Status of the Collaboration Suite Search Admin Aggregate Service is down, then check the results obtained by the Root Cause Analysis on the Collaboration Suite Search Admin Aggregate Service Home Page.

8

Collaboration Suite Search Application Service

The Collaboration Suite Search Application Service target is a grouping of Search Calendar Service, Search Files Service, Search Mail Service, and Search Web Service that are accessed by general users.

8.1 Response

The Response category checks and displays whether or not the Collaboration Suite Search Application Services are available.

8.1.1 Status

This metric shows whether or not the Collaboration Suite Search Application Services are available. The status is "up" only when all the Collaboration Suite Search Application Services are available.

User Action

If the Status of the Collaboration Suite Search Application Service is down, then check the results obtained by the Root Cause Analysis on the Collaboration Suite Search Application Service Home Page.

9

Collaboration Suite Search Service

The Collaboration Suite Search Service target is an aggregate grouping of Collaboration Suite Search Admin Aggregate Service and Search Application Service that are accessed by general users.

9.1 Response

The Response category checks and displays whether or not the Collaboration Suite Search Services are available.

9.1.1 Status

This metric shows whether or not the Collaboration Suite Search Services are available. The status is "up" only when all the Collaboration Suite Search Services are available.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

User Action

If the Status of Collaboration Suite Search Service is down, then check the results obtained by Root Cause Analysis on the Collaboration Suite Search Service Home Page.

9.2 Response Time

The Response Time Category gives you information about total user action time.

9.2.1 User Action Total Time (ms)

This metric shows the total time taken by Collaboration Suite Search Services to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

10

Collaboration Suite Search

Oracle Collaboration Suite Search is an all-in-one search application that provides users with an easy way to find information across different Oracle Collaboration Suite components.

10.1 CollabSuiteSearchStats Metrics

This category contains the metrics used to approximate the responsiveness of search queries as experienced by an end-user.

> **Note:** For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 10–1 CollabSuiteSearchStats Metrics

Metric	Description
Average Search Time (ms)	Approximates the average click-to-render response time, in milliseconds, of searches performed. This is a useful indication of the average response time experienced by end-users.
Average Search Time (seconds)	See Section 10.1.1, "Average Search Time (seconds)"
Current Active Search Requests	Represents the number of search requests that were active (ongoing) at the time of metric collection. This is a good indication of how busy the Search application is.
Host	Hostname on which the Search application resides.
Maximum Search Time (ms)	Approximates the maximum click-to-render response time, in milliseconds, of searches performed. This is a useful indication of the maximum response time experienced by end-users.
Maximum Search Time (seconds)	Approximates the maximum click-to-render response time, in seconds, of searches performed. This is a useful indication of the maximum response time experienced by end-users.
Minimum Search Time (ms)	Approximates the minimum click-to-render response time, in milliseconds, of searches performed. This is a useful indication of the minimum response time experienced by end-users.
Minimum Search Time (seconds)	Approximates the minimum click-to-render response time, in seconds, of searches performed. This is a useful indication of the average response time experienced by end-users.
Name	Name of the Search application

Table 10–1 (Cont.) CollabSuiteSearchStats Metrics

Metric	Description
Process	Process associated with the Search application
Total Search Requests Completed	Total number of searches that have been performed. This metric is cumulative, and resets only when the associated OC4J instance is restarted.

10.1.1 Average Search Time (seconds)

This metric approximates the average click-to-render response time, in seconds, of searches performed. This is a useful indication of the average response time experienced by end-users.

Metric Summary

The following table shows how often the value of the metric is collected and compared against the default thresholds. The 'Consecutive 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 10–2 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	>	50	60	2	%target%, average search response time is unacceptably slow - %value% seconds

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Full 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 "Full Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

10.2 Response

This category contains the metrics used to approximate the availability of the Search application.

10.2.1 UpDown Status

This metric indicates whether or not the associated OC4J instance of the Search application is running. A down status indicates that either the OC4J instance has been shut down, or an error has occurred that is preventing it from starting up.

Metric Summary

The following table shows how often the value of the metric is collected and compared against the default thresholds. The 'Consecutive 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 10–3 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 Minute	After Every Sample	=	Not Defined	0	1	%target%, the associated OC4J instance is down

The OPMN logs should be examined to determine if the associated OC4J instance is failing for a particular reason.

10.3 SearchPerformance Metrics

This category contains the metrics used to approximate the responsiveness of search queries performed by the application searchlets against their respective backend repositories.

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 10–4 SearchPerformance Metrics

Metric	Description
Average Backend Search Time (ms)	Approximates the average backend response time of searches performed. It is a measure of how quickly search results are obtained from the individual searchlets querying their respective backend repositories. Units are in milliseconds.
Average Backend Search Time (seconds)	See Section 10.3.1, "Average Backend Search Time (seconds)".
Current Active Backend Search Requests	Number of active backend search requests that have not yet completed at the time of metric collection. This is a good indication of how busy the Search application is.
Host	Hostname on which the search application resides.
Maximum Backend Search Time (ms)	Approximates the maximum backend response time of searches performed. It is a measure of how quickly search results are obtained from the individual searchlets querying their respective backend repositories. Units are in milliseconds.
Maximum Backend Search Time (seconds)	Approximates the maximum backend response time of searches performed. It is a measure of how quickly search results are obtained from the individual searchlets querying their respective backend repositories. Units are in seconds.
Minimum Backend Search Time (ms)	Approximates the minimum backend response time of searches performed. It is a measure of how quickly search results are obtained from the individual searchlets querying their respective backend repositories. Units are in milliseconds

Table 10–4 (Cont.) SearchPerformance Metrics

Metric	Description
Minimum Backend Search Time (seconds)	Approximates the minimum backend response time of searches performed. It is a measure of how quickly search results are obtained from the individual searchlets querying their respective backend repositories. Units are in seconds.
Name	Name of the Search application
Process	Process associated with the Search application
Total Backend Search Requests Completed	Total number of backend searches that have been performed. This metric is cumulative, and resets only when the associated OC4J instance is restarted

10.3.1 Average Backend Search Time (seconds)

This metric approximates the average backend response time of searches performed. It is a measure of how quickly search results are obtained from the individual searchlets querying their respective backend repositories. Units are in seconds.

Metric Summary

The following table shows how often the value of the metric is collected and compared against the default thresholds. The 'Consecutive 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 10–5 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	>	50	60	2	%target%, average backend search retrieval time is unacceptably slow - %value% seconds

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Full 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 "Full Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

11

Content Services FTP Service

FTP Service is a service that helps general users upload or download files from the file server using FTP.

11.1 FTP Response

The FTP Response category captures the response characteristics of the Oracle Content FTP Service as seen by a client application.

> **Note:** For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 11–1 FTP Response Metrics

Metric	Description
[FTP] Connect Time (ms)	Time taken by the FTP server to accept a network connection from a client. The connection time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total connection time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[FTP] Download Rate (KB/second)	Rate at which the FTP server downloads a file. The download rate is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total download time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[FTP] Download Time (ms)	Time taken by the FTP server to download a file. The download time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total download time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[FTP] Login Time (ms)	Time taken for a connected client to login to the FTP Server. The login time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time consumed for logging into the server. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

Table 11–1 (Cont.) FTP Response Metrics

Metric	Description
[FTP] NOOP Time (ms)	Measures the time taken by the FTP client to connect and receive feedback from the FTP Server by using the NOOP command. The NOOP time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total NOOP time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[FTP] Number of Retries	Total number of retries attempted on the FTP Server.
[FTP] Status	Status of the FTP service. It is the status determined by the Beacon monitoring this service. The Beacon is responsible for executing the perl script to ping the host and determine its status. If the Status of FTP Service is down, then check the results obtained by Root Cause Analysis on the FTP Service Home Page.
[FTP] Status Description	Describes the status of the FTP Test. For example, if the test fails, it describes why it failed.
[FTP] Total Time (ms)	Total time taken to connect (to the FTP Server), login, and download a file. The total time taken is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total processing time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[FTP] Upload Rate (KB/second)	Rate at which the FTP server uploads a file. The upload rate is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total upload time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[FTP] Upload Time (ms)	Time taken by the FTP server to upload a file. The upload time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total upload time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

11.2 Response

The FTP Response category checks and displays whether or not the FTP Service is running.

11.2.1 Status

This metric indicates whether or not clients are able to access files through the FTP Service. The availability of FTP Service depends upon the status determined by the Beacon monitoring this service. The Beacon is responsible for executing the perl script to ping the host and determine its status.

User Action

If the Status of FTP Service is down, then check the results obtained by Root Cause Analysis on the FTP Service Home Page.

11.3 Usage

The Usage category provides information about the usage of FTP Server.

> **Note:** For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 11–2 Usage Metrics

Metric	Description
Average Request Handling Time (seconds)	Average time taken by the FTP Server to handle a request (e.g. request to download a file, upload a file, etc). The average time taken is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the request handling time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
Downloaded Content Size (MB)	Total size of the content downloaded from FTP Server.
Requests Completed	Total number of requests serviced by the FTP Server (e.g. request to download a file, upload a file, etc).
Uploaded Content Size (MB)	Total size of the content uploaded to FTP Server.

12

Content Services Service

Content Services Service target represents the user functionality provided by Content Services. It includes User Access Services like FTP Service, Read Web Application, Send Web Application, and Record Management Web Application.

12.1 Document Statistics

The Document Statistics category provides information about the documents residing on the file servers.

> **Note:** For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 12–1 Document Statistics Metrics

Metric	Description
Average Document Size (bytes)	Average document size for all the documents stored in Content Services
Total Number of Documents	Total number of documents across the entire Content Services service
Total Size of Documents (bytes)	Total size of all the documents across the entire Content Services service

12.2 Response

The Response category checks and displays whether or not the Content Services services are running.

12.2.1 Status

This metric shows whether or not the User Access Content Services are available. Its status depends upon the status of FTP Service, Read Web Application, Send Web Application, and Record Management Web Application. The status is "up" only when only when all of these services are available.

User Action

If the Status of Content Services Service is down, then check the results obtained by Root Cause Analysis on the Content Services Service Home Page.

12.3 Response Time

The Response Time category provides information about the time taken by Content Services to complete Web Application transactions. A transaction could be a request to upload a file, download a file, etc.

12.3.1 User Action Total Time (ms)

This metric shows the total time taken by Content Services to complete Web Application transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

13

Content Services User Access Service

Content Services User Access Service represents user accessible functions of Content Services. The user access services include FTP Service, Read Web Application, Send Web Application, and Record Management Web Application.

13.1 Document Statistics

The Document Statistics category provides information about the documents residing on the file server.

> **Note:** For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 13–1 Document Statistics Metrics

Metric	Description
Average Document Size (bytes)	Average document size for all the documents stored in Content Services
Total Number of Documents	Total number of documents across the entire Content Services service
Total Size of Documents (bytes)	Total size of all the documents across the entire Content Services service

13.2 Response

The Response category checks and displays whether or not Content Services services are running. Content Services services include FTP Service, Read Web Application, Send Web Application, and Record Management Web Application.

13.2.1 Status

This metric shows whether or not the Content Services functionality is available. Its status depends upon the status of FTP Service, Read Web Application, Send Web Application, and Record Management Web Application. The status is "up" only when only when all of these services are available.

User Action

If the Status of Content Services User Access Service is down, then check the results obtained by Root Cause Analysis on the Content Services User Access Service Home Page.

13.3 Response Time

The Response Time category provides information about the time taken by Content Services to complete Web Application transactions. A transaction could be a request to upload a file, download a file, etc.

13.3.1 User Action Total Time (ms)

This metric shows the total time taken by Web Applications to service a transaction (including login time and connection time). The total user action time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the file server and determine the total time taken for completing a transaction. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

14

Discussions

Enterprise Manager can be used to view Oracle Discussions metrics. You can use the All Metrics page to view the metrics that have been collected for that target by the Oracle Management Agent.

14.1 Discussions SDK Metrics

This category contains the metrics used to indicate the responsiveness of the application.

The following table lists the metrics and their descriptions.

Table 14–1 Discussion SDK Metrics

Metric	Description
Category - Add To Favorite (msecs)	Average time required to add a Category/Forum to Favorites
Category - Create Board (msecs)	Average time required to create a new Forum
Category - Create Facility (msecs)	Average time required to creating a new Category
Category - Delete (msecs)	Average time required to delete a Category
Category - Delete Board (msecs)	Average time required to delete a Forum
Category - Get Container (msecs)	Average time required to retrieve a Category/Forum by path
Category - Get Container Settings (msecs)	Average time required to retrieve Category/Forum settings
Category - Get Creation Date (msecs)	Average time required to retrieve the creation date of a Category/Forum
Category - Get Creator (msecs)	Average time required to retrieve the creator of a Category/Forum
Category - Get Description (msecs)	Average time required to retrieve the Category/Forum description
Category - Get Display Name (msecs)	Average time required to retrieve the Category/Forum display name
Category - Get Favorite Threads (msecs)	Average time required to retrieve all favorite topics within a Category/Forum
Category - Get Folder (msecs)	Average time required to retrieve a Category/Forum by path

Table 14–1 (Cont.) Discussion SDK Metrics

Metric	Description
Category - Get Last Message Posts (msecs)	Average time required to retrieve the most recent posts for a Category/Forum
Category - Get Last Post (msecs)	Average time required to retrieve the last post for a Category
Category - Get Parent (msecs)	Average time required to retrieve the parent Category
Category - Get Popular Threads (msecs)	Average time required to retrieve the popular topics for a Category/Forum
Category - List Grantee Roles (msecs)	Average time required to list all users with access to a Category/Forum
Category - List With Path (msecs)	Average time required to list all Categories/Forums under a Category by path
Category - List Without Path (msecs)	Average time required to list all Categories/Forums under a Category
Category - Refresh Permissions (msecs)	Average time required to refresh a user's permissions and list of the Categories/Forums they have access to
Category - Remove From Favorites (msecs)	Average time required to remove a Category/Forum from Favorites
Category - Search (msecs)	Average time required to search within a Category/Forum
Category - Set Description (msecs)	Average time required to set a Category/Forum description
Category - Update Container Settings (msecs)	Average time required to update a Category/Forum settings
Category - Update Grantee Roles (msecs)	Average time required to update the list of users with access to a Category/Forum
Favorites - Get All Favorite Threads (msecs)	Average time required to retrieve all Favorite Topics
Favorites - Get Favorite Containers (msecs)	Average time required to retrieve all Favorite Categories/Forums
Favorites - Get Favorite Last Message Posts (msecs)	Average time required to retrieve the most recent messages within Favorite Categories.
Favorites - Get Favorite Popular Threads (msecs)	Average time required to retrieve Popular Topics within Favorite Categories.
Favorites - Get Favorite Thread By Container (msecs)	Average time required to retrieve Favorite Topics within a Category/Forum.
Favorites - Search Favorites (msecs)	Average time required to retrieve within Favorite Categories/Forums.
Forum - Append Message (msecs)	Average time required to post a message to a Forum
Forum - Delete (msecs)	Average time required to delete a Forum
Forum - Edit Message (msecs)	Average time required to retrieve edit a Message
Forum - Erase Messages (msecs)	Average time required to delete a Message

Table 14–1 (Cont.) Discussion SDK Metrics

Metric	Description
Forum - Get Last Post (msecs)	Average time required to retrieve the last post for a Forum
Forum - Get Thread (msecs)	Average time required to retrieve a Topic within a Forum
Forum - Get Threads (msecs)	Average time required to retrieve all Topics within a Forum
Forum - Lock (msecs)	Average time required to lock a Forum
Forum - Mark Public (msecs)	Average time required to lock a Forum
Forum - Unlock (msecs)	Average time required to unlock a Forum
Message - Delete (msecs)	Average time required to Hide a Message
Message - Get Body Plain Text (msecs)	Average time required to retrieve a Message body as plain text
Message - Get Body Rich Text (msecs)	Average time required to retrieve a Message body as rich text.
Message - Get Content (msecs)	Average time required to retrieve a Message's content
Message - Get Number Of Replies (msecs)	Average time required to retrieve the number of replies for a Message
Message - Get Parent (msecs)	Average time required to retrieve the parent of a Message
Message - Undelete (msecs)	Average time required to show a Message
Store - Create Facility (msecs)	Average time required to create a new Category
Store - create_board (msecs)	Average time required to create a new Forum
Store - Get Announcements Board (msecs)	Average time required to retrieve the Announcement Forum instance
Store - Get Container With ID (msecs)	Average time required to retrieve a Category/Forum instance by ID
Store - Get Container With Path (msecs)	Average time required to retrieve a category/Forum instance by path
Store - Get Global Settings (msecs)	Average time required to retrieve the global settings
Store - Get Last Message Posts (msecs)	Average time required to retrieve the most recent messages
Store - Get Last Post (msecs)	Average time required to retrieve the last message
Store - Get My Followups (msecs)	Average time required to retrieve all replies to a user's posts
Store - Get My Posts (msecs)	Average time required to retrieve all of a user's posts
Store - Get Popular Threads (msecs)	Average time required to retrieve the popular topics
Store - Get TD Store (msecs)	Average time required to log into Oracle Discussions
Store - List Globaladmin Users (msecs)	Average time required to list all users who are global administrators

Table 14–1 (Cont.) Discussion SDK Metrics

Metric	Description
Store - List With Path (msecs)	Average time required to list all Categories/Forums
Store - List Without Path (msecs)	Average time required to list all Categories/Forums without using a path
Store - Search (msecs)	Average time required to retrieve search all messages
Store - Update Global Settings (msecs)	Average time required to retrieve update the global settings
Topic - Add To Favorites (msecs)	Average time required to add a Topic to Favorites
Topic - Get Message (msecs)	Average time required to retrieve a Message within a Topic
Topic - Get Messages (msecs)	Average time required to retrieve all Messages within a Topic
Topic - Lock (msecs)	Average time required to lock a Topic
Topic - Move (msecs)	Average time required to move a Topic from one Forum to another
Topic - Remove From Favorites (msecs)	Average time required to remove a Topic from Favorites
Topic - Unlock (msecs)	Average time required to unlock a Topic

14.2 Response

This category contains the metrics used to indicate the status of the application.

14.2.1 UpDown Status

Indicates if the application is up and running. This metric is based on the status of the OC4J_OCSClient container in which the application is deployed.

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 14–2 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 Minute	After Every Sample	=	Not Defined	0	1	The associated OC4J instance is down

15

Discussions Redundancy Group

Discussions Redundancy Group target is a grouping of all Discussions agent monitored targets.

15.1 Response

The Response category checks and displays whether or not the Discussions agent monitored targets are available.

15.1.1 Status

This metric shows the status of Discussions redundancy group. Its status is up even if only one of the Discussions agent monitored targets is available.

User Action

If the Status of Discussions Redundancy Group is down, then check the status of the individual Discussions agent monitored targets to identify which particular Discussions target is down.

15.2 Usage

The Usage category provides information about the usage of Discussions agent monitored targets.

15.2.1 Number of Requests Completed

This metric shows the number of requests serviced by the Discussions agent monitored targets. The value is the sum of all completed requests of all Discussions agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

15.2.2 Resolve Context Completed

This metric shows the number of contexts resolved by the Discussions agent monitored targets. The value is the sum of all completed contexts of all Discussions agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

16

Discussions Service

The Discussions Service target is a grouping of the Discussions User Access Services. The User Access Service is made up of the News Feed and Web Application services, which are accessed by general users.

16.1 Response

The Response category checks and displays whether or not the Discussions Services are available.

16.1.1 Status

This metric shows whether or not the Discussions Services are available. The status is "up" only when all the Discussions Services are available.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

User Action

If the Status of Discussion Service is down, then check the results obtained by Root Cause Analysis on the Discussions Service Home Page.

16.2 Response Time

The Response Time Category gives you information about total user action time.

16.2.1 User Action Total Time (ms)

This metric shows the total time taken by Discussions Services to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

16.3 Usage

The Usage Category gives you information about number of requests completed and the resolve contexts completed.

16.3.1 Number of Requests Completed

This metric displays the number of requests completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

16.3.2 Resolve Context Completed

This metric displays the number of contexts resolved.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

17

Discussions User Access Service

The Discussions User Access Service target is a grouping of Discussions News Feed Service and Discussions Web Applications Service that are accessed by general users.

17.1 Response

The Response category checks and displays whether or not the Discussions User Access Services are available.

17.1.1 Status

This metric shows whether or not the Discussions User Access Services are available. The status is "up" only when all the Discussions User Access Services are available.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

User Action

If the Status of Discussions User Access Service is down, then check the results obtained by Root Cause Analysis on the Discussions User Access Service Home Page.

17.2 Response Time

The Response Time Category gives you information about total user action :if expand("%") == "" | browse confirm w | else | confirm w | endif time.

17.2.1 User Action Total Time (ms)

This metric shows the total time taken by Discussions User Access Services to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

17.3 Usage

The Usage Category gives you information about number of requests completed and the resolve contexts completed.

17.3.1 Number of Requests Completed

This metric displays the number of requests completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

17.3.2 Resolve Context Completed

This metric displays the number of contexts resolved.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

18

E-Mail POP Server

The POP (Post Office Protocol) Server provides email access for Internet Standards Based mail clients. POP is intended to permit a client to access a mail drop. POP is not intended to provide extensive manipulation operations of mail on the server. Normally, mail is downloaded and then deleted from the mail drop.

18.1 AUTH Details

This category contains metrics that provide information about AUTH commands that all clients are sending to the POP Server. A POP client uses the AUTH command to indicate an authentication mechanism to the server, perform an authentication protocol exchange, and (optionally) negotiate a protection mechanism for subsequent protocol interactions. The authentication and protection mechanisms used by the POP3 AUTH command are those used by IMAP4.

Note: For all target versions, the collection frequency for each metric is every 10 minutes.

The following table lists the metrics and their descriptions.

Table 18–1 AUTH Details Metrics

Metric	Description
AUTH Average Time (milliseconds)	Measures the average number of milliseconds the POP Server requires to process AUTH commands.
AUTH Failure Rate (Failures/minute)	See Section 18.1.1, "AUTH Failure Rate (Failures/minute)"
AUTH Rate (Requests/minute)	Measures the number of AUTH commands sent to the POP Server each minute.

18.1.1 AUTH Failure Rate (Failures/minute)

This informational metric measures the number of failed AUTH commands sent to the POP Server each minute.

User Action

Root causes can include:

1. Mandatory password changes. Failures can increase if multiple e-mail users change their password at the same time. The problem will go away after users

have changed their password. Over time, a site should expect the password policy to even out and not cause thresholds to be crossed.

2. Oracle directory server is temporarily unavailable. Authentications are not cached. If the Oracle directory server service is not available, people will not be able to log in.
3. The POP Server and the Oracle directory server cannot communicate over the network. Note this could be caused by changes in DNS, routers, or firewalls.
4. Insufficient connection pools for Oracle directory server lookups. Oracle Email protocol servers share connection pools for all client connections into Oracle directory server. If the authentication rate is high and the number of maximum connections into Oracle directory server is small, this could cause contention issues.
5. Check that the Oracle Collaboration Suite Database mail host is up and running and that the POP Server can connect to it. Also, check that the listener for Oracle Collaboration Suite Database (mailstore) is up and running.

18.2 Network

This section contains metrics that provide information on network resources used by the POP Server. This includes the amount of data transferred to and from this server and the number of client connections to this server.

Note: For all target versions, the collection frequency for each metric is every 10 minutes.

The following table lists the metrics and their descriptions.

Table 18–2 Network Metrics

Metric	Description
Client Connection Rate (Connections/minute)	Number of new POP client sessions created per minute.
Current Client Connections	Number of client sessions currently open on the POP Server.
Data Reception Rate (Kb/minute)	Amount of data the POP Server is receiving per minute from POP clients.
Data Transmission Rate (Kb/minute)	Amount of data sent to clients per minute by the POP Server. It includes traffic due to mail and POP responses related data.

18.3 PASS Details

This category contains metrics that provide information about PASS commands received by the POP Server. When a POP client issues the PASS command, the POP Server uses the argument pair from the USER and PASS commands to determine if the client should be given access to the user's mail drop.

Note: For all target versions, the collection frequency for each metric is every 10 minutes.

The following table lists the metrics and their descriptions.

Table 18–3 PASS Details Metrics

Metric	Description
PASS Average Time (milliseconds)	Average number of milliseconds the POP Server requires to process PASS commands
PASS Failure Rate (Failures/minute)	See Section 18.3.1, "PASS Failure Rate (Failures/minute)"
PASS Rate (Requests/minute)	Number of PASS commands sent to the POP Server each minute

18.3.1 PASS Failure Rate (Failures/minute)

This metric measures the rate of failed PASS commands (login failures) sent to the POP Server each minute. It is an aggregate value that includes login failures for bad user names or passwords, account validation failures against an Oracle directory server, or failures to access an Oracle Collaboration Suite Database (mailstore) after successful validation of the account.

To successfully process a POP PASS command, the server first communicates with the Oracle directory server to authenticate the user. A successful authentication with the Oracle directory server returns an Oracle Collaboration Suite Database (mailstore) to which the user will need a connection. If the POP Server is not able to communicate with the default mailstore, the login could return a failure.

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 18–4 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 10 Minutes	After Every Sample	>	300	500	1	The login failure rate is %value%

User Action

An increase in login failures could be due to a problem with one of the mail systems or to a large number of invalid user account and password pairs attempting to log in. You can test for these conditions on a test account for each Oracle Collaboration Suite Database (mailstore). If you are able to log into the POP Server successfully with a test account and you still notice a large number of failures, this could indicate that someone is attempting to break into your POP Server. Perform the following checks:

1. Check the log files. Client IP addresses are logged in the log files when the log level is set to the Notification level or higher. Use esd_logscan.pl to scan the POP server log files.
2. An attack on your POP Servers will result in a load on your Oracle directory server. Check the log files for sufficient client resources to the Oracle directory server. Use esd_logscan.pl to scan the POP server log files.

If the test account fails to login, check to see if the POP Server has connectivity to the Oracle directory server and the Oracle Collaboration Suite Database (mailstore).

1. Check whether a process on the target is able to connect and log into the Oracle directory server.
2. Check that the Oracle Collaboration Suite Database (mailstore) is up and running, the listener for the Oracle Collaboration Suite Database is up and running, and the connect string is registered properly in the infrastructure Oracle directory server.

18.4 Resource Usage

This category measures the usage of resources like databases connections and server threads. The POP Server maintains a pool of connections to database(s).

Note: For all target versions, the collection frequency for each metric is every 10 minutes.

The following table lists the metrics and their descriptions.

Table 18–5 Resource Usage Metrics

Metric	Description
Database Connection Failure Rate (Failures/minute)	This is the number of times per minute that the POP Server failed to get a database connection from the pool of database connections. This value should ideally be zero, because anytime the POP Server fails to get a connection, the end user will see an error. Database connection failures can occur if more than the allowed number of user requests come in within a short span of time. This scenario is likely after the Oracle Collaboration Suite Database (mailstore) comes back online after being offline for sometime and all the users try to reconnect to it. In this case, the pool should stabilize within a few minutes on its own. To prevent a connection overload to the Oracle Collaboration Suite Database (mailstore), increase the maximum number of connections allowed to the Oracle Collaboration Suite Database (mailstore) database if needed.
Database Connections In Use	Number of database connections currently in use by the POP Server. This is not the total number of connections in the connection pool, but a subset consisting of database connections in the pool that are currently in use. A growing trend for this metric may indicate an increase in POP workload or a slowdown in database response time. Use standard database monitoring tools to resolve these problems.
Protocol Threads In Use	This metric shows the number of server threads busy in the POP Server. Each busy thread represents one currently active request on a POP session. A growing trend may indicate an increase in POP workload or a slowdown in database response time. Use standard database monitoring tools to resolve these problems.

18.5 Response

This category contains metrics that provide information about the Up/Down status of the POP Server.

18.5.1 Status

This metric provides information about the Up/Down status of the POP Server and alerts you when the status is down. The POP Server shows a status of Down when all POP processes on the target are down.

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 18–6 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	=	0	Not Defined	1	The POP server is down

User Action

You can start the POP Server by selecting the target and clicking the Start button on the Email Application home page in the Enterprise Manager. If the POP Server does not start, a probable cause is that the server cannot connect to at least one of the Oracle Collaboration Suite Databases (mailstores) or it cannot connect to the Oracle directory server. Check the following:

1. Verify that a process on the target host is able to connect to and log into the system's Oracle directory server.
2. Verify that the Oracle Collaboration Suite Database (mailstore) is up and running and the connect string is correctly and accurately registered in the Oracle directory server.

18.6 RETR Details

This category contains metrics that chart information about RETR commands received by the POP Server. A POP client issues the RETR command to retrieve a message.

> **Note:** For all target versions, the collection frequency for each metric is every 10 minutes.

The following table lists the metrics and their descriptions.

Table 18–7 RETR Details Metrics

Metric	Description
RETR Average Time (milliseconds)	Measures the average number of milliseconds the POP Server requires to process RETR commands
RETR Failure Rate (Failures/minute)	See Section 18.6.1, "RETR Failure Rate (Failures/minute)"
RETR Rate (Requests/minute)	Measures the number of RETR commands sent to the POP Server each minute

18.6.1 RETR Failure Rate (Failures/minute)

This informational metric measures the number of failed RETR commands sent to the POP Server each minute.

User Action

RETR command failures are often a result of the POP Server not being able to connect to one or more of the mailstores. Root causes could include:

1. A mailstore is down. If the information store database or the listener for the information store is not running, then the POP Server will not be able to communicate with it.
2. Insufficient connection pool maximum for a mailstore. Oracle Email protocol servers share connection pools for all client connections to the mailstore. This leverages the resources required to get folder and message information. A large number of mail client connections will share a much smaller number of connections without contention issues. While the multiplier for connection pools will vary widely based upon how a company uses their mail system, the maximum connect pool value is typically in the 10's to support a concurrent user base in the low thousands. If there is capacity, consider adding another POP instance on this host or increasing the maximum connection pool size per POP instance.

18.7 Security

This category contains metrics that provide information about POP Server security.

18.7.1 Flood Connections Refusal Rate (Connections/minute)

This represents the rate of new connection requests rejected by the POP Server per minute. A connection refusal occurs when a server detects that too many new connection requests are coming in a short period of time from any one IP address or there are too many concurrent connections from a given IP address. You can change the number of connections allowed or the time window in which the POP Server counts new connection requests.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 10 Minutes

User Action

Check the POP Server log files to find out the IP address from which 'flooding' is detected. Ensure that only a reasonable number of mail clients are running on this machine. If the machine is running several mail clients for the same (or different) users, the POP Server may detect a 'flooding'. If required, either increase the number of connections allowed or decrease the amount of time in which flooding is detected to the values appropriate for your site and type of mail clients used. Use esd_logscan.pl to scan the POP server log files.

18.8 STAT Details

This category contains metrics that provide information about STAT commands received by the POP Server. POP clients use the STAT command to query the POP Server for the number of e-mail messages in the user's mail drop.

Note: For all target versions, the collection frequency for each metric is every 10 minutes.

The following table lists the metrics and their descriptions.

Table 18–8 STAT Details Metrics

Metric	Description
STAT Average Time (milliseconds)	Measures the average number of milliseconds the POP Server requires to process STAT commands
STAT Failure Rate (Failures/minute)	Measures the number of failed STAT commands sent to the POP Server each minute
STAT Rate (Requests/Minute)	Measures the number of STAT commands sent to the POP Server each minute

18.9 TOP Details

This category contains metrics that provide information about TOP commands received by the POP Server. A POP client issues the TOP command to retrieve the headers and opening lines of a message.

Note: For all target versions, the collection frequency for each metric is every 10 minutes.

The following table lists the metrics and their descriptions.

Table 18–9 TOP Details Metrics

Metric	Description
TOP Average Time (milliseconds)	Measures the average number of milliseconds the POP Server required to process TOP commands
TOP Failure Rate (Failures/minute)	See Section 18.9.1, "TOP Failure Rate (Failures/minute)"
TOP Rate (Requests/minute)	Measures the number of TOP commands sent to the POP Server each minute

18.9.1 TOP Failure Rate (Failures/minute)

This informational metric measures the number of failed TOP commands sent to the POP Server each minute.

User Action

TOP command failures are often a result of the POP Server not being able to connect to one or more of the mailstores. Root causes could include:

1. A mailstore is down. If the information store database or the listener for the information store is not running, then the POP Server will not be able to communicate with it.
2. Insufficient connection pool maximum for a mailstore. Oracle Email protocol servers share connection pools for all client connections to the mailstore. This leverages the resources required to get folder and message information. A large number of mail client connections will share a much smaller number of connections without contention issues. While the multiplier for connection pools will vary widely based upon how a company uses their mail system, the maximum connect pool value is typically in the 10's to support a concurrent user base in the low thousands. If there is capacity, consider adding another POP instance on this host or increasing the maximum connection pool size per POP instance.

19

E-Mail POP Service

The E-Mail POP Service target allows you to monitor the Oracle Email System at the service level. This target is monitored by periodically performing client-like protocol operations to monitor whether the POP Service is available and responding in a reasonable time. This target must be configured manually to refer to the host name and port number that are used to connect to the Oracle Email POP Service address. The POP service can run from a single host or, in large installations, behind a network load balancer or network address translator.

19.1 Response

This category of metrics captures the response characteristics of the Oracle Email POP service as seen by a client application.

19.1.1 Connect Time (ms)

This metric shows the time taken for the POP server to accept a network connection from a client. This metric also indicates the performance of the Oracle Net Services Listener.

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 19–1 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	>	100	2000	2	Time to connect to POP service is %value% (ms).

User Action

None. This is for informational purposes only. This metric is aggregated into the Total Time Metric.

19.1.2 Login Time (ms)

This metric shows the time taken for a connected client to log in to the POP Server. This metric also indicates the Oracle directory server response time, because clients are authenticated against the Oracle directory server.

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 19–2 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	>	2000	5000	2	Login Time is %value% (ms).

User Action

None. This is for informational purposes only. This metric is aggregated into the Total Time Metric.

19.1.3 Status

This metric shows whether clients are able to access e-mail through the POP Service. At least one IMAP service and Oracle Net Services Listener must be running in order for the IMAP Service to be available.

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 19–3 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	=	Not Defined	0	1	Failed to connect to POP service

User Action

The IMAP Service logically consists of the Oracle Email POP Server and an associated Oracle Net Services Listener which listens for POP network connection requests. If this service is down, check to see if at least one IMAP server process is running. Also check to see if the Oracle Net Services Listener configured for the Oracle Email system is running.

19.1.4 Time to Read E-Mail (ms)

This metric shows the time taken to retrieve a message from the Oracle Collaboration Suite Database (mailstore) through the POP server. This metric also indicates database performance.

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 19–4 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	>	2000	5000	2	Time taken to read an e-mail time is %value% (ms).

User Action

None. This is for informational purposes only. This metric is aggregated into the Total Time Metric.

19.1.5 Total Time (ms)

This metric shows the total time taken to complete one simulated POP session. This metric is directly dependent on the performance characteristics of the POP Server target.

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 19–5 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	>	5000	10000	2	Total Time to read an e-mail is %value% (ms).

User Action

To reduce the total response time, tune the POP servers after observing their performance levels. You can also identify which operations in a client session are slower by looking at the other columns in this metric.

20

Identity Management Service

The Identity Management Service target is a grouping of Identity Management User Access Services that are accessed by general users.

20.1 LDAP Statistics

The LDAP Statistics category checks and displays whether or not the Identity Management Service is available.

20.1.1 Total LDAP Logon Sessions

This metrics displays the total number of LDAP logon sessions across all the LDAP servers of the Identity Management service.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

20.2 Response

The Response category checks and displays whether or not the Identity Management Service is available. Its status depends on the status of all Identity Management Services. The Identity Management Service is available only when all these services are available.

20.2.1 Status

This metric shows the status of the Identity Management Service.

User Action

If the Status of Identity Management Service is down, then check the results obtained by Root Cause Analysis on the Identity Management Service Home Page.

20.3 Response Time

The Response Time category provides information about the time taken by all the Identity Management services to service their transactions.

20.3.1 Average Base Search Time (ms)

This metric shows the average time taken to search the Oracle Internet Directory.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

20.4 SSO Login

The SSO Login category provides information about the login attempts made to the Single Sign-On servers of the Identity Management service.

20.4.1 Number of Successful Login Attempts

The total number of successful login attempts over the last hour across all the Single Sign-On servers of the Identity Management service

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

21

Identity Management User Access Service

The Identity Management User Access Service target is a grouping of the Internet Directory Service and Single Sign-on Service that are accessed by general users.

21.1 LDAP Statistics

The LDAP Statistics Category gives you information about active database sessions, directory operations and the total LDAP logon sessions.

Note: For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 21–1 LDAP Statistics Metrics

Metric	Description
Active Data Base Sessions	Number of sessions currently running on the LDAP servers and Single Sign-On servers. The value is the sum of all active database sessions on all LDAP and Single Sign-On agent monitored targets.
Directory Operations (last 15 min.)	Total number of the LDAP directory operations across all the LDAP servers of the Identity Management service. This metric shows the total number of directory operations performed on the LDAP servers and Single Sign-On servers. The value is the sum of all open TCP connections, all completed "add" operations, and all completed "bind" operations performed on all LDAP and Single Sign-On agent monitored targets.
Total LDAP Logon Sessions	Total number of LDAP logon sessions across the LDAP servers and Single Sign-On servers.

21.2 Response

The Response category checks and displays whether or not the Identity Management Services are available. Its status depends upon the status of all LDAP servers and Single Sign-On servers. The Identity Management User Access Services is available only when all these services are available.

21.2.1 Status

If the Status of Identity Management User Access Service is down, then check the results obtained by Root Cause Analysis on the Identity Management Service Home Page.

21.3 Response Time

The Response Time category gives you information about the time taken by LDAP and Single Sign-on servers to perform a search.

21.3.1 Average Base Search Time (ms)

This metric shows the average time taken by LDAP and Single Sign-on servers to perform a base search.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

21.4 SSO Login

The SSO Login category provides information about the login attempts made to the LDAP and Single Sign-On servers.

21.4.1 Number of Successful Login Attempts

This metric displays the total number of successful login attempts over the last hour across all LDAP and Single Sign-on servers.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

21.4.2 Number of Unsuccessful Login Attempts

This metric displays the total number of unsuccessful login attempts over the last hour across all LDAP and Single Sign-on servers.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

22

Internet Directory Redundancy Group

The Internet Directory Redundancy Group target is a grouping of all LDAP agent monitored targets.

22.1 LDAP Statistics

The LDAP Statistics category provides information about the usage of the LDAP server.

> **Note:** For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 22–1 LDAP Statistics Metrics

Metric	Description
Active Data Base Sessions	Number of sessions currently running on the LDAP Server. The value is the sum of all active database sessions on the LDAP agent monitored targets.
Directory Operations	Total number of directory operations performed on the LDAP Server. The value is the sum of all open TCP connections, all completed "add" operations, and all completed "bind" operations performed on the LDAP agent monitored targets.
Server Load	Amount of load on the LDAP Server. The value is the average of total load on all LDAP agent monitored targets.
Total LDAP Logon Sessions	Total number of connections on the LDAP Server. The value is the sum of all open TCP connections on the LDAP agent monitored targets.

22.2 Response

The Response category checks and displays whether or not the LDAP Servers are available.

22.2.1 Status

This metric displays the status of the LDAP Servers Redundancy Group. Its status is "up" even if only one of the LDAP agent monitored targets is available.

User Action

If the Status of Internet Directory Redundancy Group is down, then check the status of the individual LDAP server agent monitored targets to identify which particular LDAP server is down.

23

Internet Directory Service

The Internet Directory Service monitors the availability, performance, and usage of the Identity Management Service.

23.1 LDAP Response

The LDAP Response Category gives you information about address search time, base search time, compare time, connect time, message search time, status and status message.

> **Note:** For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 23–1 LDAP Response Metrics

Metric	Description
[LDAP] Address Search Time (ms)	Time taken to search an address in the LDAP server. The search time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total address search time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[LDAP Base Search Time (ms)	Time taken to perform a base search. The search time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total base search time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[LDAP] Compare Time (ms)	Time taken to compare two files. The search time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total compare time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[LDAP] Connect Time (ms)	Time taken to connect to the LDAP server.

Table 23–1 (Cont.) LDAP Response Metrics

Metric	Description
[LDAP] Message Search Time (ms)	Time taken to search a message in the LDAP server. The search time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total message search time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[LDAP] Status	Shows whether or not the Internet Directory Services are available
[LDAP] Status Message	Describes the status. If the status is "down", this metric describes why the LDAP server down.

23.2 LDAP Statistics

The LDAP Statistics Category gives you information about active data base sessions, directory operations, server load and the total LDAP logon sessions.

Note: For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 23–2 LDAP Statistics Metrics

Metric	Description
Active Data Base Sessions	Number of sessions currently running on the LDAP Server. The value is the sum of all active database sessions on the LDAP agent monitored targets.
Directory Operations (last 15 min.)	Total number of directory operations performed on the LDAP Server. The value is the sum of all open TCP connections, all completed "add" operations, and all completed "bind" operations performed on all LDAP servers.
Server Load	Amount of load on the LDAP Server. The value is the average of total load on all LDAP servers.
Total LDAP Logon Sessions	Total number of connections on the LDAP Server. The value is the sum of all open TCP connections on all LDAP servers.

23.3 Response

The Response category checks and displays whether or not the Internet Directory Service is available.

23.3.1 Status

This metric displays the status of the LDAP Servers.

Metric Summary

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

Target Version	Collection Frequency
Version 1.0	Every 15 minutes

User Action

If the Status of Internet Directory Services is down, then check the results obtained by Root Cause Analysis on the Internet Directory Service Home Page.

23.4 Response Time

The Response Time category gives you information about LDAP average base search time.

23.4.1 LDAP Average Base Search Time (ms)

This metric shows the average time taken to perform a base search.

Metric Summary

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

Target Version	Collection Frequency
Version 1.0	Every 15 minutes

24

Mobile Collaboration Access Service

The Mobile Collaboration Access Service target is a grouping of all Mobile Collaboration Access Services that are accessed by general users. The Mobile Collaboration Access Services include the Address Book Service, Calendar Service, Content Services Service, Directory Service, Fax Service, Mail Service, and Short Msg Service.

24.1 Response

The Response category checks and displays whether or not the Mobile Collaboration Access Services are available. The Mobile Collaboration Access Services include the Address Book Service, Calendar Service, Cnotent Services Service, Directory Service, Fax Service, Mail Service, and Short Msg Service.

24.1.1 Status

This metric shows whether or not the Mobile Collaboration Access Services are available. The status is "up" only when all the Mobile Collaboration Access Services are available.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

User Action

If the Status of Mobile Collaboration Access Service is down, then check the results obtained by the Root Cause Analysis on the Mobile Collaboration Access Service Home Page.

24.2 Response Time

The Response Time Category gives you information about total user action time.

24.2.1 User Action Total Time (ms)

This metric shows the total time taken by Mobile Collaboration User Access Services to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

24.3 Statistics

The Statistics Category gives you information about total number of active sessions, total number of services invoked over the last five minutes, and total number of users.

Note: For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 24–1 Statistics Metrics

Metric	Description
Total Number of Active Sessions	Total number of active sessions on the Mobile Collaboration Access Services
Total Number of Services Invoked Over Last 5 min	Total number of services invoked on the Mobile Collaboration Access Service for the past five minutes
Total Number of Users	Total number of active users on the Mobile Collaboration Access Service

25

Mobile Collaboration Device Management Service

The Mobile Collaboration Device Management Service target is an aggregate grouping of all Mobile Collaboration Device Management Services that are accessed by general users.

25.1 Response

The Response category checks and displays whether or not the Mobile Collaboration Device Management Services are available.

25.1.1 Status

This metric shows whether or not the Mobile Collaboration Device Management Services are available. The status is "up" only when all the Mobile Collaboration Device Management Services are available.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

User Action

If the Status of Mobile Collaboration Device Management Service is down, then check the results obtained by Root Cause Analysis on the Mobile Collaboration Device Management Service Home Page.

25.2 Response Time

The Response Time Category gives you information about user action total time.

25.2.1 User Action Total Time (ms)

This metric shows the total time taken by Mobile Collaboration Device Management Services to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

26

Mobile Collaboration Push Mail Service

The Mobile Collaboration Push Mail Service target is a grouping of all Mobile Collaboration Push Mail services that are accessed by general users.

26.1 Response

The Response category checks and displays whether or not the Mobile Collaboration Push Mail Services are available.

26.1.1 Status

This metric shows whether or not the Mobile Collaboration Push Mail Services are available. The status is "up" only when all the Mobile Collaboration Push Mail Services are available.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

User Action

If the Status of Mobile Collaboration Push Mail Service is down, then check the results obtained by Root Cause Analysis on the Mobile Collaboration Push Mail Service Home Page.

26.2 Response Time

The Response Time Category gives you information about total user action time.

26.2.1 User Action Total Time (ms)

This metric shows the total time taken by Mobile Collaboration Push Mail Management Services to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

27

Mobile Collaboration Redundancy Group

Mobile Collaboration Redundancy Group target is a grouping of all Wireless (Mobile) agent monitored targets.

27.1 Response

The Response category checks and displays whether or not the Mobile agent monitored targets are available.

27.1.1 Status

This metric displays the status of the Mobile Collaboration Redundancy Group. Its status is "up" even if only one of the Mobile agent monitored targets is available.

User Action

If the Status of Mobile Collaboration Redundancy Group is down, then check the status of the individual Mobile agent monitored targets to identify which particular agent monitored target is down.

27.2 Statistics

The Statistics category provides information about the usage of Mobile agent monitored targets.

Note: For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 27–1 Statistics Metrics

Metric	Description
Total Number of Active Sessions	Total number of sessions currently running on the Mobile Collaboration agent monitored target. The value is the sum of all active sessions of all Mobile Collaboration agent monitored targets.
Total Number of Services Invoked Over Last 5 Minutes	Total number of services invoked on the Mobile Collaboration agent monitored target for the past five minutes. The value is the sum of all services invoked over the past five minutes on all Mobile Collaboration agent monitored targets.

Table 27–1 (Cont.) Statistics Metrics

Metric	Description
Total Number of Users	Total number of users on the Mobile Collaboration agent monitored target. The value is the sum of all users on all Mobile Collaboration agent monitored targets.

28

Mobile Collaboration Service

The Mobile Collaboration Service target is a grouping of Mobile Collaboration Access Service, Mobile Collaboration Device Management Service, and Mobile Collaboration Push Mail Service.

28.1 Response

The Response category checks and displays whether or not the Mobile Collaboration Services are available.

28.1.1 Status

This metric shows whether or not the Mobile Collaboration Services are available. The status is "up" only when all the Mobile Collaboration Services are available.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

User Action

If the Status of Mobile Collaboration Service is down, then check the results obtained by Root Cause Analysis on the Mobile Collaboration Service Home Page.

28.2 Response Time

The Response Time Category gives you information about total user action time.

28.2.1 User Action Total Time (ms)

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

28.3 Statistics

The Statistics Category gives you information about total number of active sessions, total number of services invoked over the last five minutes, and total number of users.

Note: For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 28–1 Statistics Metrics

Metric	Description
Total Number of Active Sessions	Total number of active sessions on the Mobile Collaboration Services
Total Number of Services Invoked Over Last 5 Minutes	Total number of services invoked on the Mobile Collaboration Services for the last 5 minutes
Total Number of Users	Total number of active users on the Mobile Collaboration Services

29

OID Client

These are the metrics monitored by the OID (Oracle Internet Directory) client.

29.1 Response

This metric category provides the response metrics.

29.1.1 Addressing Search Time (ms)

This metric represents the time (in milliseconds) it consumed to perform an e-mail addressing search against an LDAP (Lightweight Directory Access Protocol) Server.

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 29–1 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	>	2000	4000	2	OID Addressing ing search time is %value% (ms).

29.1.2 Base Search Time (ms)

This metric represents the time (in milliseconds) it consumed to perform a base search against an LDAP (Lightweight Directory Access Protocol) Server.

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 29–2 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	>	2000	4000	2	OID Base search time is %value% (ms).

29.1.3 Compare Time (ms)

This metric represents the time (in milliseconds) it consumed to perform a compare operation against an LDAP (Lightweight Directory Access Protocol) Server. This simulates logging in LDAP activity.

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 29–3 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	>	2000	4000	2	OID Compare op time is %value% (ms).

29.1.4 Messaging Search Time (ms)

This metric represents the time (in milliseconds) it consumed to perform an e-mail message search against an LDAP (Lightweight Directory Access Protocol) Server.

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 29–4 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	>	125	4000	2	OID Messaging search time is %value% (ms).

29.1.5 Status

Displays the present status of the OID client.

- Up (value of 1): OID client is running

- Down (value of 0): OID client is not running

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 29–5 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	=	Not Defined	0	1	Failed to connect to LDAP server

30

Oracle Collaboration Suite Search Client Redundancy Group

The Oracle Collaboration Suite Search Client Redundancy Group target is a grouping of Oracle Collaboration Suite Client monitored targets that have identical configuration, characteristics, and functionality. While a single Oracle Collaboration Suite Client instance is vulnerable to the failure of its host or system, a redundant group of Oracle Collaboration Suite Clients continues to function despite the loss of an instance, hiding any such failure, and allowing other instances in the group to service the requests.

30.1 Response

The Response category captures the response characteristics of the Oracle Collaboration Suite Search Clients as seen by other applications.

30.1.1 Status

This metric indicates whether or not the Oracle Collaboration Suite Search Client Redundancy Group is up or down. The availability of the Oracle Collaboration Suite Search Client Redundancy Group depends upon the status of all the Oracle Collaboration Suite Search Client targets. The status is "up" as long as at least one of the agent monitored targets is available.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

User Action

If the Status of Oracle Collaboration Suite Search Client Redundancy Group is down, then check the status of the individual targets to identify which particular one is down.

30.2 Statistics

The Statistics Category gives you information about current and completed search requests.

Note: For target Version 1.0, the evaluation and collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 30–1 Statistics Metrics

Metric	Description
Current Active Backend Search Requests	Statistics of the active backend search requests made
Current Active Search Requests	Statistics of the current active search requests made
Total Backend Search Requests Completed	Statistics of the total backend search requests completed
Total Search Requests Completed	Statistics of the total search requests completed

31

Oracle Collaboration Suite Service

The Oracle Collaboration Suite Service (OCS Service) is an aggregate service that includes one or more Collaboration Suite component services (subservices). The availability, performance, and usage of the Collaboration Suite service depend on the availability, performance, and usage of the individual component services comprising the Collaboration Suite service.

31.1 Response

The Response category checks and displays whether or not all the services configured under the Oracle Collaboration Suite Services are running.

31.1.1 Status

This metric indicates whether or not all the services configured under the Oracle Collaboration Suite Services are available. Its status is "up" only when all of the Oracle Collaboration Suite Services are available.

User Action

If the Status of Oracle Collaboration Suite Service is down, then check the results obtained by Root Cause Analysis on the Oracle Collaboration Suite Service Home Page.

32

Oracle Content Services

An Oracle Content Services target is comprised of all Oracle Content Services processes in a given domain. These Oracle Content Services processes run protocol servers, agents, or servlets.

You can use Oracle Enterprise Manager to monitor and manage these processes.

32.1 All Sessions

The *All Sessions* category provides summarized session information for the target Oracle Content Services domain. It reports the total session count across all Oracle Content Services node processes and all Oracle Content Services server types.

32.1.1 Sessions

This metric reports the total session count of the target Oracle Content Services domain across all Oracle Content Services node processes and all Oracle Content Services server types.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

32.2 Documents

The *Documents* category provides basic document statistics for documents in the target Oracle Content Services repository. It reports the total document count, the total document content size, and the average document content size.

> **Note:** For all target versions, the collection frequency for each metric is every 60 minutes.

The following table lists the metrics and their descriptions.

Table 32–1 Documents Metrics

Metric	Description
Average Content Size (KB)	Average content size (in KB) of the documents in the target Oracle Content Services repository
Total Content Size (GB)	Total content size (in GB) of the documents in the target Oracle Content Services repository
Total Number	Total number of documents in the target Oracle Content Services repository

32.3 Documents By MIME Type

The *Documents By MIME Type* category provides document statistics grouped by MIME type, for documents in the target Oracle Content Services repository. It reports the number of documents, the total content size, and the average content size for each MIME type.

Note: For all target versions, the collection frequency for each metric is every 60 minutes.

The following table lists the metrics and their descriptions.

Table 32–2 Documents By MIME Type Metrics

Metric	Description
Average Size (KB)	Average content size (in KB) of all the documents belonging to a given MIME type
Documents	Total number of documents for a given MIME type
Total Size (MB)	Total content size (in MB) of all the documents belonging to a given MIME type

32.4 Domain Response

The *Domain Response* category provides status information about the entire Oracle Content Services domain, which includes all the Oracle Content Services processes on all the middle tiers that belong to this domain.

32.4.1 Status

This metric reports the overall status of the Oracle Content Services domain. The possible values are:

- 0 (Down) - All of the processes in the domain are down.
- 1 (Up) - One or more of the processes in the domain are up.

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 32–3 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 12 Samples	=	Not Defined	0	1	The domain of %target% is down

32.4.2 Status Message

This metric provides detailed status messages about the Oracle Content Services domain. For example, it displays all the Oracle Content Services processes that are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

32.5 FTP Servers

The *FTP Servers* category provides basic runtime performance data for the FTP servers running on Oracle Content Services node processes for a given middle tier. This category reports the following data for each FTP server, calculated since the server's node process was started:

- Total number of completed requests
- Average request handling time (in seconds)
- Total size of all downloaded content (in MB)
- Total size of all uploaded content (in MB)

The following table lists the metrics and their descriptions.

Table 32–4 FTP Servers Metrics

Metric	Description
Average Request Handling Time (seconds)	Average request handling time (in seconds) for the given FTP server, calculated since the server's node process was started
Downloaded Content Size (MB)	Total size of all downloaded content (in MB) for the given FTP server, calculated since the server's node process was started
Requests Completed	Total number of completed requests for the given FTP server, calculated since the server's node process was started
Uploaded Content Size (MB)	Total size of all uploaded content (in MB) for the given FTP server, calculated since the server's node process was started

32.6 Libraries By Site

The *Libraries By Site* category provides basic Library statistics grouped by Site for all Oracle Content Services Libraries, including Personal Libraries and Shared Libraries. It reports the following for each Site:

- Total number of Libraries
- Total number of Personal Libraries
- Total number of Shared Libraries
- Total quota allocated to all Libraries (in GB)
- Total quota consumed by all Libraries (in GB)
- Percentage of quota consumed by all Libraries
- Total quota allocated to Personal Libraries (in GB)
- Total quota consumed by Personal Libraries (in GB)
- Percentage of quota consumed by Personal Libraries
- Total quota allocated to Shared Libraries (in GB)
- Total quota consumed by Shared Libraries (in GB)
- Percentage of quota consumed by Shared Libraries

Note: For all target versions, the collection frequency for each metric is every 60 minutes.

The following table lists the metrics and their descriptions.

Table 32–5 Libraries By Site Metrics

Metric	Description
All Libraries	Total number of Libraries in a given Site
Allocated Quota For Personal Libraries (GB)	Total amount of quota (in GB) allocated to all the Personal Libraries in a given Site
Allocated Quota For Shared Libraries (GB)	Total amount of quota (in GB) allocated to all the Shared Libraries in a given Site
Consumed (%)	toTal quota consumed as a percentage of the total quota allocated for all the Libraries in a given Site
Consumed By Personal Libraries (%)	Total quota consumed as a percentage of the total quota allocated for all the Personal Libraries in a given Site
Consumed By Shared Libraries (%)	Total quota consumed as a percentage of the total quota allocated for all the Shared Libraries in a given Site
Consumed Quota By Personal Libraries (GB)	Amount of quota (in GB) consumed by all the Personal Libraries in a given Site
Consumed Quota By Shared Libraries (GB)	Total amount of quota (in GB) consumed by all the Shared Libraries in a given Site
Personal Libraries	Total number of Personal Libraries in a given Site
Shared Libraries	Total number of Shared Libraries in a given Site
Total Allocated Quota (GB)	Total amount of quota (in GB) allocated to all the Libraries in a given Site
Total Consumed Quota (GB)	Total amount of quota (in GB) consumed by all the Libraries in a given Site

32.7 Load Balanced RM Application URL Timing

The *Load Balanced RM Application URL Timing* category provides responsiveness information for the load balanced URL of the Oracle Records Management application. It reports the availability and the response time of the load balanced URL.

32.7.1 Load Balanced RM Application URL Response Time (seconds)

This metric provides the response time of the load balanced URL for the Oracle Records Management application. In particular, it returns the total elapsed time (in seconds) that it took to download the contents of that URL. The URL's contents include both the base page source and any frames or images in the page.

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 32–6 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 12 Samples	>	2.0	3.0	2	The response time for the load balanced RM application is slow - %value% seconds

32.7.2 Load Balanced RM Application URL Status

This metric reports the availability of the load balanced URL for the Oracle Records Management application:

- 0 - The URL is not available.
- 1 - The URL is available.

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 32–7 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 5 Minutes	After Every 12 Samples	=	Not Defined	0	1	The load balancer or the RM application is down

32.8 Load Balanced Web Application URL Timing

The *Load Balanced Web Application URL Timing* category provides responsiveness information for the load balanced URL of the Oracle Content Services Web application. It reports the availability and the response time of the load balanced URL.

32.8.1 Load Balanced Web Application URL Response Time (seconds)

This metric provides the response time of the load balanced URL for the Oracle Content Services Web application. In particular, it returns the total elapsed time (in seconds) that it took to download the contents of that URL. The URL's contents include both the base page source and any frames or images in the page.

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 32–8 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	After Every 12 Samples	>	2.0	3.0	2	The response time for the load balanced web application is slow - %value% seconds

32.8.2 Load Balanced Web Application URL Status

This metric reports the availability of the load balanced URL for the Oracle Content Services Web application:

- 0 - The URL is not available.
- 1 - The URL is available.

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 32–9 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	After Every 12 Samples	=	Not Defined	0	1	The load balancer or the web application is down

32.9 Nodes

The *Nodes* category provides basic statistics on all the node processes of the target Oracle Files domain. It reports the following for each node process:

- Session count
- Java VM thread count
- Java VM total memory (in MB)
- Java VM free memory (in MB)
- Java VM used memory (in MB)
- Java VM free memory percentage

> **Note:** For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 32–10 Nodes Metrics

Metric	Description
JVM Free Memory (%)	See Section 32.9.1, "JVM Free Memory (%)"
JVM Free Memory (MB)	Java VM free memory (in MB) for a given Oracle Content Services node process
JVM Threads	Java VM thread count for a given Oracle Content Services node process
JVM Total Memory (MB)	Java VM total memory (in MB) for a given Oracle Content Services node process
JVM Used Memory (MB)	Java VM used memory (in MB) for a given Oracle Content Services node process
Sessions	Session count for a given Oracle Content Services node process

32.9.1 JVM Free Memory (%)

This metric reports the percentage of the Java VM free memory over the total memory for a given Oracle Content Services node process.

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 32–11 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 5 Minutes	After Every 12 Samples	<	15.0	10.0	2	The Java VM free memory in %NodeName% on %MiddleTier% is low - %value%%

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each unique combination of "Node Name", "Middle Tier", and "Host Name and IP" objects.

If warning or critical threshold values are currently set for any unique combination of "Node Name", "Middle Tier", and "Host Name and IP" 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 "Node Name", "Middle Tier", and "Host Name and IP" objects, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

32.10 Processes

The *Processes* category provides the CPU usage, the memory usage, and the up/down status for each Oracle Content Services process on a given middle tier. It reports the following for each process:

- CPU usage percentage
- CPU idle percentage
- Physical memory usage (in MB)
- Physical memory usage percentage
- Free physical memory (in MB)
- Free physical memory percentage
- Total physical memory (in MB)
- Start time (in milliseconds since epoch)
- Up time (in milliseconds)
- Status

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 32–12 Processes Metrics

Metric	Description
Free Memory (%)	Free physical memory percentage on the local host
Free Memory (MB)	Free physical memory (in MB) on the local host
Idle CPU Time (%)	CPU idle percentage for the local host
Process CPU Usage (%)	See Section 32.10.1, "Process CPU Usage (%)"
Process Memory Usage (%)	See Section 32.10.2, "Process Memory Usage (%)"
Process Memory Usage (MB)	Physical memory usage (in MB) for the given Oracle Content Services process
Start Time (ms since epoch)	Time the given Oracle Content Services process was started. The value is given in the number of milliseconds between the last start time and midnight of January 1, 1970 UTC

Table 32–12 (Cont.) Processes Metrics

Metric	Description
Status	This metric reports the status of the given Oracle Content Services process. The possible values are: ■ 0 (Down) - The process is down. ■ 1 (Up) - The process is up.
Total Memory (MB)	Total physical memory (in MB) on the local host
Up Time (ms)	Length of time (in milliseconds) since the given Oracle Content Services process was started

32.10.1 Process CPU Usage (%)

This metric reports the CPU usage percentage for the given Oracle Content Services process.

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 32–13 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
All Versions	Every 5 Minutes	After Every 12 Samples	>	Not Defined	Not Defined	2	CPU utilization for %Process% is high - %value%%%

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process" 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 "Process" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

32.10.2 Process Memory Usage (%)

This metric reports the physical memory usage percentage for the given Oracle Content Services process.

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 32–14 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
All Versions	Every 5 Minutes	After Every 12 Samples	>	80	90	2	Memory utilization for %Process% is high - %value%%

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process" 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 "Process" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

32.11 Resource Usage

The *Resource Usage* category provides the CPU usage and the memory usage for all Oracle Content Services processes for a given middle tier. It reports the following:

- CPU usage percentage
- CPU usage percentage of other processes
- CPU idle percentage
- Physical memory usage (in MB)
- Physical memory usage percentage
- Physical memory usage percentage of other processes
- Free physical memory (in MB)

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 32–15 Resource Usage Metrics

Metric	Description
CPU Idle Time (%)	CPU idle percentage for the local host
CPU Usage (%)	See Section 32.11.1, "CPU Usage (%)"
Free Memory (MB)	Free physical memory (in MB) on the local host
Memory Usage (%)	See Section 32.11.2, "Memory Usage (%)"
Memory Usage (MB)	Physical memory usage (in MB) for all Oracle Files processes for a given middle tier
Other CPU Usage (%)	CPU usage percentage for all processes other than the Oracle Content Services processes

Table 32–15 (Cont.) Resource Usage Metrics

Metric	Description
Other Memory Usage (MB)	Physical memory usage (in MB) for all processes other than the Oracle Content Services processes

32.11.1 CPU Usage (%)

This metric reports the CPU usage percentage for all Oracle Content Services processes for a given middle tier.

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 32–16 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
All Versions	Every 5 Minutes	After Every 12 Samples	>	Not Defined	Not Defined	2	CPU utilization is high - %value%%%

32.11.2 Memory Usage (%)

This metric reports the physical memory usage percentage for all Oracle Content Services processes for a given middle tier.

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 32–17 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 5 Minutes	After Every 12 Samples	>	80	90	2	Memory utilization is high - %value%%%

32.12 Response

The *Response* category provides the overall status of all Oracle Content Services processes for a given middle tier.

32.12.1 Status

This metric reports the overall status of all Oracle Content Services processes for a given middle tier. The possible values are:

- 0 (Down) - All of the local processes are down.

- 1 (Up) - One or more of the local processes are up.

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 32–18 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 5 Minutes	After Every 12 Samples	=	Not Defined	0	1	%target% is down

32.13 RM Application URL Timing

The *RM Application URL Timing* category provides responsiveness information for the URL of the Oracle Records Management application running on a given middle tier. It reports the availability and the response time of the URL.

32.13.1 RM Application URL Response Time (seconds)

This metric provides the response time of the URL for the Oracle Records Management application running on a given middle tier. In particular, it returns the total elapsed time (in seconds) that it took to download the contents of that URL. The URL's contents include both the base page source and any frames or images in the page.

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 32–19 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
All Versions	Every 5 Minutes	After Every 12 Samples	>	2.0	3.0	2	The response time for the RM application is slow - %value% seconds

32.13.2 RM Application URL Status

This metric reports the availability of the URL for the Oracle Records Management application running on a given middle tier:

- 0 - The URL is not available.
- 1 - The URL is available.

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 32–20 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
All Versions	Every 5 Minutes	After Every 12 Samples	=	Not Defined	0	1	The RM application is down

32.14 Servers

The *Servers* category provides basic performance data for all servers, including protocol servers and agents, running on Oracle Content Services node processes for a given middle tier. This category reports the following data for each server, calculated since the server's node process was started:

- Status (running, stopped, and so on)
- Last time the server was started
- Last time the server was stopped
- Total number of completed activation periods
- Last time the server began its activation period
- Last time the server completed its activation period
- Total number of completed event processing periods
- Average activation period time (in seconds)
- Average event processing period time (in seconds)

The following table lists the metrics and their descriptions.

Table 32–21 Servers Metrics

Metric	Description
Activations Completed	Total number of completed activation periods for the given server, calculated since the server's node process was started. This metric only applies to agents, since protocol servers do not have activation periods
Average Activation Handling Time (seconds)	Average activation period time (in seconds) for the given server, calculated since the server's node process was started. This metric only applies to agents, since protocol servers do not have activation periods.
Average Event Processing Time (seconds)	Average event processing period time (in seconds) for the given server, calculated since the server's node process was started
Event Processing Completed	Total number of completed event processing periods for the given server, calculated since the server's node process was started

Table 32–21 (Cont.) Servers Metrics

Metric	Description
Last Activation Start Time	Last time the given server started an activation period, calculated since the server's node process was started. This metric only applies to agents, since protocol servers do not have activation periods. The possible values are: ■ The number of milliseconds between the last activation period start time and midnight of January 1, 1970 UTC. ■ -1, if the server has not started an activation period since the node was started.
Last Activation Stop Time	Last time the given server completed an activation period, calculated since the server's node process was started. This metric only applies to agents, since protocol servers do not have activation periods. The possible values are: ■ The number of milliseconds between the last activation period stop time and midnight of January 1, 1970 UTC. ■ -1, if the server has not completed an activation period since the node was started.
Last Start Time	Last time the given server was started, calculated since the server's node process was started. The possible values are: ■ The number of milliseconds between the last start time and midnight of January 1, 1970 UTC. ■ -1, if the server has not been started since the node process was started.
Last Stop Time	Last time the given server was stopped, calculated since the server's node process was started. The possible values are: ■ The number of milliseconds between the last stop time and midnight of January 1, 1970 UTC. ■ -1, if the server has not been stopped since the node process was started.
Status	Current status of the given server. The possible values are: ■ 0 - unknown ■ 1 - stopped ■ 2 - running ■ 3 - stopping ■ 4 - starting ■ 5 - suspended ■ 6 - disposed

32.15 Sessions By Server (Domain)

The *Sessions By Server (Domain)* category provides basic session information for the target Oracle Files domain. It reports the session count grouped by Oracle Content Services server type.

32.15.1 Sessions

This metric reports the session count across all the Oracle Content Services node processes in the domain for a given Oracle Content Services server type.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

32.16 Sessions By Server (Node)

The *Sessions By Server (Node)* category provides basic session information for each Oracle Content Services node in the target domain. For each node, it reports the session count grouped by Oracle Content Services server type.

32.16.1 Sessions

This metric reports the session count for a given Oracle Content Services node process and a given Oracle Content Services server type.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

32.17 Users

The *Users* category reports the total number of Oracle Content Services users across all the Sites in the target Oracle Content Services repository.

32.17.1 All Named Users

This metric reports the total number of users in Oracle Content Services.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 60 Minutes

32.18 Users By Site

The *Users By Site* category reports the total number of Oracle Content Services users for each Site in the target Oracle Content Services repository.

32.18.1 Users

This metric reports the total number of users for a given Site in Oracle Content Services.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 60 Minutes

32.19 Web Application URL Timing

The *Web Application URL Timing* category provides responsiveness information for the URL of the Oracle Content Services Web application running on a given middle tier. It reports the availability and the response time of the URL.

32.19.1 Web Application URL Response Time (seconds)

This metric provides the response time of the URL for the Oracle Content Services Web application running on a given middle tier. In particular, it returns the total elapsed time (in seconds) that it took to download the contents of that URL. The URL's contents include both the base page source and any frames or images in the page.

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 32–22 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
All Versions	Every 5 Minutes	After Every 12 Samples	>	2.0	3.0	2	The response time for the web application is slow - %value% seconds

32.19.2 Web Application URL Status

This metric reports the availability of the URL for the Oracle Content Services Web application running on a given middle tier:

- 0 - The URL is not available.
- 1 - The URL is available.

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 32–23 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
All Versions	Every 5 Minutes	After Every 12 Samples	=	Not Defined	0	1	The web application is down

32.20 WebDAV Servers

The *WebDAV Servers* category provides basic runtime performance data for the WebDAV servers running on Oracle Content Services node processes for a given

middle tier. This category reports the following data for each WebDAV server, calculated since the server's node process was started:

- Total number of completed requests
- Average request handling time (in seconds)
- Total size of all downloaded content (in MB)
- Total size of all uploaded content (in MB)

The following table lists the metrics and their descriptions.

Table 32–24 WebDAV Servers Metrics

Metric	Description
Average Request Handling Time (seconds)	Average request handling time (in seconds) for the given WebDAV server, calculated since the server's node process was started
Downloaded Content Size (MB)	Total size of all downloaded content (in MB) for the given WebDAV server, calculated since the server's node process was started
Requests Completed	Total number of completed requests for the given WebDAV server, calculated since the server's node process was started
Uploaded Content Size (MB)	Total size of all uploaded content (in MB) for the given WebDAV server, calculated since the server's node process was started

33

Real-Time Collaboration

You can use Enterprise Manager to view the metrics for a Real-Time Collaboration target.

33.1 Conference Server Meeting Usage

This category contains metrics about conference server meeting usage.

33.1.1 Active Clients

Number of users currently running web conferencing.

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 33–1 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 Message	Clear Message
All Versions	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Number of Active Clients is %value% and has exceeded warning/ critical threshold %threshold%	Number of Active Clients is %value% and has fallen below warning/ critical threshold %threshold%

33.1.2 Memory Used KB

Memory currently being used, in kilobytes.

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 33–2 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 Message	Clear Message
All Versions	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Memory used is %value%, and has exceeded warning/ critical threshold %threshold%	Memory used is %value%, and has fallen below warning/ critical threshold %threshold%

33.1.3 Total Number of Meeting Minutes (last calendar week)

The total number of meeting minutes for the past calendar week (Sunday 12:00am to Saturday 11:59pm).

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 33–3 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 Message	Clear Message
All Versions	Every 24 hours	After Every Sample	>	Not Defined	Not Defined	1	Number of Meeting Minutes is %value% and has exceeded warning/ critical threshold %threshold%	Number of Meeting Minutes is %value% and has fallen below warning /critical threshold %threshold%

33.2 Conference Server Usage

This category contains metrics about the number of conferences occurring and the number of users participating in all conferences.

33.2.1 Active Sessions

The number of conferences currently taking place.

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 33–4 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 Message	Clear Message
All Versions	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Number of Active Sessions is %value% and has exceeded warning/ critical threshold %threshold%	Number of Active Sessions is %value% and has fallen below warning/ critical threshold %threshold%

33.3 Presence Server Usage

This category contains metrics about the number of users using Oracle Messenger, and the number of messages sent.

33.3.1 Chat Conferences

Total number of chat conferences that are currently 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 33–5 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 Message	Clear Message
All Versions	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Number of Chat Conferences is %value% and has exceeded warning/ critical threshold %threshold%	Number of Chat Conferences is %value% and has fallen below warning/ critical threshold %threshold%

33.3.2 Number of Messages Sent Last 5 Mins

The number of messages sent with Oracle Messenger within the last 5 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 33–6 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 Message	Clear Message
All Versions	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Number of Messages Sent Last 5 Mins is %value% and has exceeded warning/ critical threshold %threshold%	Number of Messages Sent Last 5 Mins is %value% and has fallen below warning/ critical threshold %threshold%

33.3.3 Number of New Logins Last 5 Mins

The number of users who have logged into Oracle Messenger within the last 5 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 33–7 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 Message	Clear Message
All Versions	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Number of New Logins Last 5 Mins is %value% and has exceeded warning/ critical threshold %threshold%	Number of New Logins Last 5 Mins is %value% and has fallen below warning/critical threshold %threshold%

33.3.4 Total Online Users

The number of persons currently online (available) on Oracle Messenger.

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 33–8 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 Message	Clear Message
All Versions	Every 15 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Number of Total Online Users is %value% and has exceeded warning/ critical threshold %threshold%	Number of Total Online Users is %value% and has fallen below warning/ critical threshold %threshold%

33.4 Process Information

This category contains CPU and memory utilization metrics for all the Real-Time Collaboration processes.

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 33–9 Process Information Metrics

Metric	Description
CPU Idle (%)	Percentage of CPU time spent doing nothing
CPU Other (%)	Percentage of CPU time used by all the other processes
CPU Usage (%)	See Section 33.4.1, "CPU Usage (%)"
Free Physical Memory (MB)	Amount of free memory, in megabytes
Page Size (Bytes)	Size of the page, in bytes
Physical Memory Percentage	Percentage of physical memory used by this process
Physical Memory Usage (MB)	Memory used by this process, in megabytes
Resident Memory Utilization (%)	Percentage of resident memory utilization
Resident Memory Utilization (KB)	Resident memory utilization, in kilobytes
Total Physical Memory Usage (MB)	Total memory used, in megabytes
Virtual Memory Utilization (KB)	Virtual memory usage, in kilobytes

33.4.1 CPU Usage (%)

Percentage of the CPU used by this process.

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 33–10 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 Message	Clear Message
All Versions	Every 5 Minutes	After Every 12 Samples	>	Not Defined	Not Defined	1	CPU used is %value% and has exceeded warning/ critical threshold %threshold%	CPU used is %value% and has fallen below warning/ critical threshold %threshold%

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

33.5 Response

This category contains metrics about a Real-Time Collaboration system.

33.5.1 Status

Reports the overall status of the Real-Time Collaboration system. A value of 1 indicates the application is up. A value of 0 indicates the application is down.

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 33–11 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 Message	Clear Message
All Versions	Every 15 Minutes	After Every Sample	=	Not Defined	0	1	Failed to run imtctl.	Succeeded in running imtctl.

34

Real-Time Collaboration Redundancy Group

The Real-Time Collaboration Redundancy Group target is a grouping of all Real-Time Collaboration agent monitored targets.

34.1 Response

The Response category checks and displays whether or not the Real-Time Collaboration agent monitored targets are available.

34.1.1 Status

This metric shows the status of Real-Time Collaboration Redundancy Group. Its status is "up" even if only one of the Real-Time Collaboration agent monitored targets is available.

User Action

If the Status of Real-Time Collaboration Redundancy Group is down, then check the status of the individual Real-Time Collaboration agent monitored targets to identify which particular target is down.

34.2 Statistics

The Statistics category provides information about the usage of Real-Time Collaboration agent monitored targets.

Note: For target Version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 34–1 Statistics Metrics

Metric	Description
Active Clients	Total number of clients currently logged on to all the Web Conferencing servers in the selected redundancy group
Active Sessions	Total number of open connections on all the Web Conferencing servers in the selected redundancy group
Conference Minutes	Total duration (in minutes) of the last web conference
Used Memory	Total amount of space used for a conference by all the Web Conferencing servers in the selected redundancy group

35

Real-Time Collaboration Service

The Real-Time Collaboration Service target is a grouping of the Real-Time Collaboration User Access Services that is accessed by general users.

35.1 Midtier Statistics

The Midtier Statistics Category gives you information about conference minutes, current users, and web conferences.

> **Note:** For target Version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 35–1 Midtier Statistics Metrics

Metric	Description
Conference Minutes (last cal week)	Total duration (in minutes) of the last web conference
Users (current)	Total number of users currently using web conferencing functionality
Web Conferences (current)	Total number of conferences currently active

35.2 Response

The Response category checks and displays whether or not the Real-Time Collaboration Services are available.

35.2.1 Status

This metric shows whether or not the Real-Time Collaboration Services are available. The status is "up" only when all the Real-Time Collaboration Services are available.

User Action

If the Status of Real-Time Collaboration Service is down, then check the results obtained by Root Cause Analysis on the Real-Time Collaboration Service Home Page.

35.3 Response Time

The Response Time Category gives you information about total user action time.

35.3.1 User Action Total Time (ms)

This metric shows the total time taken by Real Time Collaboration services to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

36

Real-Time Collaboration User Access Service

The Real-Time Collaboration User Access Service target is a grouping of Real-Time Collaboration Web Conferencing Service and Real-Time Collaboration Web Presence Service that are accessed by general users.

36.1 Midtier Statistics

The Midtier Statistics Category gives you information about conference minutes, the current users, and web conferences.

> **Note:** For target Version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 36–1 Midtier Statistics Metrics

Metric	Description
Conference Minutes (last cal week)	Total number of web conference minutes in the last calendar week
Users (current)	Total number of users currently running web Conferencing
Web Conferences (current)	Total number of conferences currently taking place

36.2 Response

The Response category checks and displays whether or not the Real-Time Collaboration User Access Services are available.

36.2.1 Status

This metric shows whether or not the Real-Time Collaboration User Access Services are available. The status is "up" only when all the Real-Time Collaboration User Access Services are available.

User Action

If the Status of Real-Time Collaboration User Access Service is down, then check the results obtained by the Root Cause Analysis on the Real-Time Collaboration User Access Service Home Page.

36.3 Response Time

The Response Time Category gives you information about total user action time.

36.3.1 User Action Total Time (ms)

This metric shows the total time taken by Real Time Collaboration services to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 Minutes

37

Single Sign-On Redundancy Group

Single Sign-On Redundancy Group target is a logical grouping of all Single Sign-On server agent monitored targets.

37.1 Response

The Response category checks and displays whether or not the Single Sign-On servers are available.

37.1.1 Status

This metric displays the status of the Single Sign-On servers Redundancy Group. Its status is "up" even if only one of the Single Sign-On server agent monitored targets is available.

User Action

If the Status of Single Sign-on Redundancy Group is down, then check the status of the individual Single Sign-On server agent monitored targets to identify which particular agent monitored target is down.

37.2 SSO Login

The SSO Login category provides information about the login attempts made to the Single Sign-On servers.

37.2.1 Number of Successful Login Attempts

This metric shows the number of successful login attempts on the Single Sign-On servers. The value is the sum of all login attempts that were successful on all Single Sign-On servers.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

37.2.2 Number of Unsuccessful Login Attempts

This metric shows the number of unsuccessful login attempts on the Single Sign-On servers. The value is the sum of all login attempts that were unsuccessful on all Single Sign-On servers.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

38

Web Access Client Service

The Web Access Client Service target is a grouping of the Web Access Client Address Book Service, Web Access Client Directory Service, Web Access Client Messaging Service, and Web Access Client Scheduling Service that are accessed by general users.

38.1 Response

The Response category checks and displays whether or not the Web Access Client Service is available. Its status depends upon the status of all Web Access Client Services. The Web Access Client Service is available only when all these services are available.

38.1.1 Status

This metric shows whether or not the Web Access Client Service is available.

User Action

If the Status of Web Access Client Service is down, then check the results obtained by Root Cause Analysis on the Web Access Client Service Home Page.

38.2 Response Time

The Response Time Category gives you information about total user action time.

38.2.1 User Action Total Time (ms)

This metric shows the total time taken by Web Access Client Service to service their transactions (including login time and connection time).

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

38.3 Statistics

The Statistics Category gives you information about current active search requests, current active sessions and current directory cache usage.

Note: For target Version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 38–1 Statistics Metrics

Metric	Description
Current Active Search Requests	Number of search requests that are active (ongoing). This is a good indication of how busy the Search application is
Current Active Sessions	Number of active sessions. Active sessions is an indication of the number of users connected to the Web Access client application. So, this is a good representation of the load on the Web Access client application
Current Directory Cache Usage	Number of directory caches currently in use. This is a good indication of the concurrent and current user access of the Web Access Client service application

39

Web Access Client Web Access Redundancy Group

Web Access Client Web Access Redundancy Group is a logical grouping of all Web Access Client Collaboration Suite Search (Web Access OCS Client) agent monitored targets.

39.1 Response

The Response category checks and displays whether or not the Web Access OCS Client agent monitoring targets are available.

39.1.1 Status

This metrics shows the status of Web Access OCS Client Redundancy Group.

User Action

If the Status of Web Access OCS Client Redundancy Group is down, then check the status of the individual Web Access OCS Client agent monitoring targets to identify which particular target is down.

39.2 Statistics

The Statistics category provides information about the usage of the Web Access OCS Client agent monitored targets.

Note: For target Version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 39–1 Statistics Metrics

Metric	Description
Current Active Sessions	Number of connections currently open on the Web Access OCS Client agent monitored targets
Current Directory Cache Usage	Amount of directory cache currently used by the Web Access OCS Client agent monitored targets
directoryFind.maxActive	Number of searches performed by the Web Access OCS Client agent monitored targets

Table 39–1 (Cont.) Statistics Metrics

Metric	Description
getPersonalMessageFolders .active	Number of personal message folders available on the Web Access OCS Client agent monitored targets
getSharedMessageFolders. maxActive	Number of message folders shared on the Web Access OCS Client agent monitored targets
ICMessageSent.maxActive	Number of messages sent by the Web Access OCS Client agent monitored targets

40

Workspaces

Enterprise Manager can be used to view Oracle Workspaces metrics. You can use the All Metrics page to view the metrics that have been collected for that target by the Oracle Management Agent.

40.1 Response

This category contains the metrics used to indicate the status of the application.

40.1.1 UpDown Status

Indicates if the application is up and running. This metric is based on the status of the OC4J_OCSClient container in which the application is deployed.

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 40–1 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 Minute	After Every Sample	=	Not Defined	0	1	The associated OC4J instance is down

40.2 Workspaces Web UI Metrics

This category contains the metrics used to indicate the responsiveness of the application.

The following table lists the metrics and their descriptions.

Table 40–2 Workspaces Web UI Metrics

Metric	Description
All Other Requests, msecs	Average time taken for all other requests in the Workspaces application
Announcements: Create Announcement, msecs	Average time taken to create an announcement in a Workspace

Table 40–2 (Cont.) Workspaces Web UI Metrics

Metric	Description
Announcements: List Announcements, msecs	Average time taken to list announcements in a workspace
Discussions: Create a Forum, msecs	Average time taken to create a forum in a Workspace
Discussions: Delete Forums, msecs	Average time taken to delete a forum in a Workspace
Discussions: Get a Forum by Id, msecs	Average time taken to get a specific forum in a Workspace, given the ID of the forum
Discussions: List Discussion Messages in a Topic, msecs	Average time taken to list the messages in a specific discussion topic in a Workspace
Discussions: List Discussion Topics, msecs	Average time taken to list the discussion topics in a specific forum in a Workspace
Discussions: List Forums, msecs	Average time taken to list the forums in a Workspace
Discussions: Post a Discussion Message, msecs	Average time taken to post a message to a discussion topic in a Workspace
Library: File Download, msecs	Average time taken to download the contents of a file in the Workspace library.
Library: File Upload, msecs	Average time taken to upload a file to the Workspace library
Library: List Library Contents, msecs	Average time taken to list the contents of the library in a Workspace
Meetings: Create a Calendar Meeting, msecs	Average time taken to create a calendar Meeting in a workspace
Meetings: List Calendar Meetings, msecs	Average time taken to list calendar meetings in a Workspace
Meetings: Show Meetings Day View, msecs	Average time taken to show calendar meetings in a Workspace in the Day View
Meetings: Show Meetings Week View, msecs	Average time taken to show calendar meetings in a Workspace in the Week View
Tasks: Create a Task, msecs	Average time taken to create a task in a Workspace
Tasks: List Tasks By Range, msecs	Average time taken to list tasks in a Workspace in a specified time range
Tasks: List Tasks, msecs	Average time taken to list tasks in a Workspace
Workspace Overview: Show Workspace home Page, msecs	Average time taken to display the home page of a specific Workspace
Workspaces Home: Create a New Workspace, msecs	Average time taken to create a new Workspace
Workspaces Home: List All My Workspaces, msecs	Average time taken to list all Workspaces for a user
Workspaces Home: List of My Favorite Workspaces, msecs	Average time taken to list the favorite Workspaces for a user

41

Workspaces Redundancy Group

The Workspaces Redundancy Group gives information about the Operation, Response and Web UI Metrics.

41.1 Responses

The Response category checks and displays whether or not the Workspaces Redundancy Group is available. Its status depends upon the status of all Workspaces Redundancy Groups.

41.1.1 Status

This metric shows whether or not the Workspaces Redundancy Group is available.

User Action

If the Status of Workspaces Redundancy Group is down, then check the results obtained by Root Cause Analysis on the Workspaces Redundancy Group Page.

41.2 Operation

The Response Time Category gives you information about number of objects completed and requests completed.

41.2.1 Number of Objects Completed

This metric shows the number of objects completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

41.2.2 Requests Completed

The Requests Completed Category gives you information about the requests completed.

41.3 Web UI Metrics

This category gives information about the number of objects completed and requests completed.

41.3.1 Number of Objects Completed

This metric displays the number of objects completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

41.3.2 Requests Completed

This metric displays the number of requests.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

42

Workspaces Service

The Workspaces Service target is a grouping of Workspaces User Access Service and the Workspaces Web Service that are accessed by general users.

42.1 Operation

The Operation Category gives you information about the number of objects completed and the requests completed..

42.1.1 Number of Objects Completed

This metric shows information about the number of objects completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

42.1.2 Requests Completed

This metrics gives you information about the number of requests completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

42.2 Response

The Response category checks and displays whether or not the Workspaces Service is available. Its status depends upon the status of all Workspaces Services.

42.2.1 Status

This metric shows whether or not the Workspaces Service is available.

User Action

If the Status of Workspaces Service is down, then check the results obtained by Root Cause Analysis on the Workspaces Service Page.

42.3 Response Time

The Response Time Category gives you information about the transaction time.

42.3.1 Transaction Time

This metric shows information about the transaction time.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

42.4 Web UI Metrics

This category gives information about the number of objects completed and requests completed.

42.4.1 Number of Objects Completed

This metric displays the information about the number of objects completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

42.4.2 Requests Completed

This metric displays information about the number of requests completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

43

Workspaces User Access Service

The Workspaces User Access Service target is a grouping of the Workspaces Web Service that is accessed by general users.

43.1 Operation

The Operation Category gives you information about the number of objects completed and the requests completed.

43.1.1 Number of Objects Completed

This metric shows information about the number of objects completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

43.1.2 Requests Completed

This metrics gives you information about the number of requests completed.

43.2 Responses

The Response category checks and displays whether or not the Workspaces User Access Service is available. Its status depends upon the status of all Workspaces User Access Services.

43.2.1 Status

This metric shows whether or not the Workspaces User Access Service is available.

User Action

If the Status of Workspaces User Access Service is down, then check the results obtained by Root Cause Analysis on the Workspaces User Access Service Page.

43.3 Response Time

The Response Time Category gives you information about the transaction time.

43.3.1 Transaction Time

This metric shows information about the transaction time.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

43.4 Web UI Metrics

This category gives information about the number of objects completed and requests completed.

43.4.1 Number of Objects Completed

This metric displays the number of objects completed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

43.4.2 Requests Completed

This metric displays the number of requests.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

Part II

E-Mail Metrics

Part II provides the metrics related to the Oracle Collaboration Suite E-Mail targets.

Part II contains the following chapters:

44

Collaboration Suite Database

An Oracle Collaboration Suite Database (mailstore) target contains message and mail queue management information. The Oracle Collaboration Suite Database contains a single copy of an e-mail message with multiple instance records of that message, depending upon the number of recipients and the number of times it was copied into different folders.

44.1 Message Queue

The Message Queue category contains metrics about mail messages in a mail store that are queued to be processed by a mail server. Mail servers which process queued messages are the SMTP Outbound, List, and NNTP Outbound servers.

The following diagnostic scripts can be used to get more details about the status of queues:

1. esd_mail_queue.sql: Use this script to examine the contents of a queue or all queues. Important information, such as sender of the message, sent date, and subject, about each message in a queue is listed.
2. esd_queue_examine.sql: Use this script to list the top 5 most frequently found subjects, senders, and recipients of messages in the submit queue.
3. See Appendix D, "Oracle Mail Command-Line Reference" in Oracle Mail Adminstrator's Guide for more information these scripts.

44.1.1 Length of Archive Queue

This metric is a gauge that measures the number of messages captured by all SMTP and list server processes for this Oracle Collaboration Suite Database (mailstore) that need to have archive message copies built and sent.

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 44–1 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 10 Minutes	After Every Sample	>	750	1000	1	The length of archive queue is %value%

User Action

A relatively low and constant number is desirable for this metric. If the number is trending up, then there is probably not enough SMTP Outbound processing resoures applied to **Archive Queue Processing**. A spike in the queue could indicate an unusual burst of archivable traffic but, if the spike does not start to return, one of the target archive repositories might not be available.

If SMTP Outbound processes are running and the queue is still growing, check the following:

1. Consider creating a separate and dedicated SMTP Outbound instance to processing the archive queue.
2. Check the resources available to the Oracle Collaboration Suite Database host to ensure that host has sufficient memory and CPU.
3. Check the resources available to the Oracle Collaboration Suite host running the SMTP Outbound process(es) to ensure that host has sufficient memory and CPU.
4. Consider increasing the concurrency of the SMTP Outbound process(es) that process the archive queue.
5. Check the archive policy e-mail addresses or relay hosts and port numbers to ensure they are not rejecting connections and are capable of receiving messages.

44.1.2 Length of Collection Queue

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 44–2 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 10 Minutes	After Every Sample	>	750	1000	1	The length of collection queue is %value%

44.1.3 Length of List Queue

This metric is a gauge that measures the number of messages that are in the list server queue. The messages in this queue are sent to mailing lists and have to be processed by the list server.

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 44–3 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 10 Minutes	After Every Sample	>	750	1000	1	The length of list queue is %value%

44.1.4 Length of Local Queue

This metric is a gauge that measures the number of messages that are in the local delivery queue. The messages in this queue have to be processed by SMTP Outbound or list server.

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 44–4 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 10 Minutes	After Every Sample	>	750	1000	1	The length of local queue is %value%

44.1.5 Length of NNTP Queue

This metric is a gauge that measures the number of messages that are in the NNTP Outbound queue. The messages in this queue have to be fed to other news servers and have to be processed by the NNTP Outbound server.

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 44–5 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 10 Minutes	After Every Sample	>	750	1000	1	The length of NNTP queue is %value%

44.1.6 Length of Prune Queue

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 44–6 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 10 Minutes	After Every Sample	>	750	1000	1	The length of prune queue is %value%

44.1.7 Length of Relay Queue

This metric is a gauge that measures the number of messages that are in the relay queue. The messages in this queue have to be processed by the SMTP Outbound or list server.

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 44–7 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 10 Minutes	After Every Sample	>	750	1000	1	The length of relay queue is %value%

44.1.8 Length of Submit Queue

This metric is a gauge that measures the number of messages that are in the submit queue. The messages in this queue have to be processed by the SMTP Outbound server.

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 44–8 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 10 Minutes	After Every Sample	>	750	1000	1	The length of submit queue is %value%

44.1.9 Messages Being Processed

This metric is a gauge that measures the number of messages which are currently being processed by the various Oracle Mail servers, including SMTP Outbound, list server, and NNTP Outbound.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

44.1.10 Messages Queued for Reattempting Local Delivery

This metric is a gauge that measures the number of messages that are in the local delivery queue but could not be delivered due to the mailbox being full or some other reason. The messages in this queue will be retried for delivery by the SMTP Outbound server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

44.1.11 Messages Queued for Reattempting Relay Delivery

This metric is a gauge that measures the number of messages that are in the relay queue but could not be delivered due to the relay SMTP server being unavailable or some other reason. The messages in this queue will be retried for delivery by the SMTP Outbound server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

44.2 Response

The Mailstore Response category contains metrics that provide information about the Up/Down status of an instance of the Oracle Collaboration Suite Database (mailstore).

44.2.1 Status

The Response Status metric indicates whether or not the Oracle Collaboration Suite Database is available to use as a mail store. A value of one (1) means the Oracle Collaboration Suite Database is up and running along with the database listener (the Oracle Listener). A value of zero means it is not available.

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 44–9 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 10 Minutes	After Every Sample	=	Not Defiend	0	1	Failed to connect to the database

45

E-Mail Housekeeper

The Housekeeper target is a background process which works on the Oracle Collaboration Suite Database to prune and expunge deleted or expired messages. An Oracle Collaboration Suite Database contains a single copy of an e-mail message with multiple instance records of that message, depending upon the number of recipients and the number of times it was copied into different folders. Managing and updating the records in an Oracle Collaboration Suite Database is a multi-step process handled by housekeepers.

45.1 Message Pruning and Collection

The message pruning and collection category contains metrics regarding the rate at which the housekeeper processes are working.

45.1.1 Message Collection Rate (Messages/minute)

This metric measures the rate of messages collected each minute by the housekeeper.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 60 minutes

45.1.2 Message Prune Rate (Messages/minute)

This metric measures the rate of message instance records deleted each minute by the housekeeper.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 60 minutes

45.2 Response

The Housekeeper Response category checks and displays whether or not the Housekeeper Server processes are running within this ORACLE_HOME.

45.2.1 Status

Status is checked by looking for one or more housekeeper processes on the target.

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 45–1 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	=	0	Not Defined	1	Housekeeper not running

User Action

If the Housekeeper processes should be up but are not, then this indicates that they were unable to initialize successfully. Probable causes are an inability to contact or connect to either one of the Oracle Collaboration Suite Databases or the system's Oracle directory server. Perform the following checks.

1. Check that a process on the target is able to connect to and log into the Oracle directory server for the installation. The Oracle directory server could be down, or the network between this host and the Oracle directory server could be broken.
2. Make sure the Oracle Collaboration Suite Database is up and running and the connect string is correctly and accurately registered in the infrastructure Oracle directory server.

46

E-Mail IMAP Server

The Internet Message Access Protocol (IMAP) target provides session-oriented access for Internet Standards Based mail clients. The metric categories provide statistical information on these IMAP servers.

46.1 APPEND Details

This category contains metrics that provide information about the APPEND command. Mail clients use the IMAP APPEND command to copy messages into an Oracle Collaboration Suite Database from an external source. Mail clients commonly use this command to place a copy of sent messages into folders on the Oracle Collaboration Suite Database. Less frequently, a particular client that has two user accounts on two different Oracle Collaboration Suite Databases might use the APPEND command to copy messages across Oracle Collaboration Suite Databases.

46.1.1 APPEND Average Time (milliseconds)

The APPEND Average Time metric measures the latency, in milliseconds, involved from the time a message starts to be copied into a folder on the IMAP Server until its completion. Latencies will vary and are a function of the size of the message.

Trending increases in APPEND Average Time typically mean that the IMAP writes to the Oracle Collaboration Suite Database (mailstore) cannot keep up with the amount of traffic. An increase in APPEND latency is often accompanied by an increase in the latencies of the SMTP_IN process for that Oracle Collaboration Suite Database.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Review the Enterprise Manager metrics for the Oracle Collaboration Suite Database instance. Common reasons for increased latency include:

1. Insufficient processor or memory or inefficient use of memory for the Oracle Collaboration Suite Database. Try applying more resources to the Oracle Collaboration Suite Database or tune the Oracle Collaboration Suite Database. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about

tuning a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.

2. Too many connections configured for the mail protocol servers. All mail protocol servers have a minimum, maximum, and increment value. The minimum number of connections is an aggregate of all server instance minimums. The maximum is an aggregate of all instance maximums. The servers grow and shrink their pools dynamically. A sustained jump in latency during peak loads followed by a return to normal could be caused by insufficient RAM on the database to process the number of connection requests. Increase the RAM or tune the number of instances and connection pool parameters. (For more information, see *Oracle Email Administrator's Guide Release 2 (9.0.4.1)*).
3. Datasets have become too large. Consider partitioning the Oracle Collaboration Suite Database.

46.1.2 APPEND Failure Rate (Failures/minute)

This metric measures the rate of APPEND failures per minute. APPEND failures occur when sufficient resources are not available to create a new message in the user's Oracle Collaboration Suite Database.

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 46–1 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 10 Minutes	After Every Sample	>	300	500	1	The number of failed APPENDs are %value%

User Action

Root causes of APPEND command failures could include:

1. Disk capacity. A failure will occur when an Oracle Collaboration Suite Database runs out of disk space or is unable to extend tablespaces.
2. Insufficient connection pool maximum for the Oracle Collaboration Suite Database. Oracle Email protocol servers share connection pools for all client connections into the Oracle Collaboration Suite Database, enabling a large number of mail client connections to share a smaller number of connections without contention issues. While the multiplier for connection pools varies based upon how the mail system is used, the maximum connect pool value is typically in the 10's to support a concurrent user base in the low thousands. If there is disk capacity, consider adding another IMAP instance on this host or increasing the maximum connection pool size.

46.1.3 APPEND Rate (Requests/minute)

This informational metric represents the rate of APPEND commands that occurred per minute during the period since the last capture of this information.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Use this value to better understand user email usage patterns. Use this information as a factor when deciding to alter the critical alert and warning alert thresholds to better suit system requirements.

46.2 AUTHENTICATE Details

IMAP Servers are session oriented. All mail clients must authenticate themselves with the IMAP Server at the start of the session before they are allowed to execute any other IMAP commands.

The LOGIN command and the AUTHENTICATE command are used by a client to start a session and have access to more capabilities. The LOGIN command supports basic username and password authentication. AUTHENTICATE supports basic username and password authentication as well as more sophisticated and complex authentication algorithms up to and including Simple Authentication and Security Layer (SASL: RFC 2222) support.

46.2.1 AUTHENTICATE Average Time (milliseconds)

This metric is the latency period involved in logging into the IMAP Server (in tenths of a second). Each IMAP authentication requires the server to access the Oracle directory server as the "source of truth" for authentication. If your Oracle directory server configuration chains authentication to yet another Oracle directory server, the AUTHENTICATE Average Time includes the time to communicate with and receive information from that second Oracle directory server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

The root cause for an unusually long time to authenticate is typically found in the network between the IMAP Server and the Oracle directory server or in resources for the Oracle directory server:

1. Network latency increases between servers. Check network latencies between your mail protocol servers (middle tier installations) and the instance of the Oracle directory server, which supports those servers. This includes any transit times through routers and firewalls.

2. Insufficient processor or memory or inefficient use of memory for the Oracle directory server database. For default installations, the Oracle directory server database is shared with the "infrastructure" database instance. If the database or host do not have enough memory allocated to support the transaction load against the database, apply more resources to Oracle directory server or tune the Oracle directory server. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about tuning a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.

46.2.2 AUTHENTICATE Failure Rate (Failures/minute)

This metric graphs a rate of AUTHENTICATE command failures. It is an aggregate value, counting failures for invalid user names or passwords and failures to validate an account against the Oracle directory server.

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 46–2 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 10 Minutes	After Every Sample	>	300	500	1	The number of failed authentications are %value%

User Action

Root causes of an increasing AUTHENTICATE Failure Rate can include:

1. Mandatory password changes. The AUTHENTICATE Failure Rate can increase if password policies require the users to change their password after a given length of time. If multiple people enter this state at the same time, sudden increases in authentication failures can occur.
2. The Oracle directory server is temporarily unavailable. If the Oracle directory server service is not available, authentications are not cached, preventing logins.
3. The IMAP Server and the Oracle directory server cannot communicate over the network. This could be caused by changes in DNS, routers, or firewalls.
4. Insufficient connection pools for Oracle directory server lookups. Oracle Email protocol servers share connection pools for all client connections into the Oracle directory server. If the authentication rate is high and the number of maximum connections into the Oracle directory server is small, contention issues could arise.
5. Check that the Oracle Collaboration Suite Database mail host is up and running and that the IMAP Server can connect to it. Also, check that the listener for Oracle Collaboration Suite Database (mailstore) is up and running.

46.2.3 AUTHENTICATE Rate (Requests/minute)

This informational metric graphs the per minute rate at which sessions were instantiated since the last check was performed. This is not equivalent to the number of concurrent users, because:

1. Mail clients often open multiple sessions to their IMAP Server per mail client session
2. Mail clients often use the more basic LOGIN command
3. The number of concurrent users is a count and it does not take into account closed sessions

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.3 COPY Details

The COPY command is used by mail clients to copy (not move) a message into another mail folder.

46.3.1 COPY Average Time (milliseconds)

This metric measures the average time it took the IMAP Server to respond to a COPY command. The latency includes the time it took the IMAP Server to communicate with an Oracle Collaboration Suite Database and the time required to update information in an Oracle Collaboration Suite Database.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Increases in the response times to the COPY command may indicate problems in your network or your Oracle Collaboration Suite Databases. When an increase in the latency of a command is detected, check the latency of commands to other mail protocol servers (POP and SMTP) for similar increases, as they are often related.

Review the Enterprise Manager metrics for the infrastructure database, the Oracle directory server, and the Oracle Collaboration Suite Database instance(s). Common issues include:

1. Network Latencies. Check the response time between this IMAP Server and the Oracle Collaboration Suite Database(s).
2. Insufficient processor or memory or inefficient use of memory for the Oracle Collaboration Suite Database. Apply more resources to the Oracle Collaboration Suite Database or tune the Oracle Collaboration Suite Database. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about tuning

a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.

3. Too many connections are configured for the mail protocol servers. All mail protocol servers have a minimum, maximum and increment value. The minimum number of connections is an aggregate of all server instances minimums. The maximum is an aggregate of all instances maximums. The servers grow and shrink their pools dynamically. Sustained jumps in latency during peak loads followed by returns to normal could be caused by insufficient RAM on the database to process the number of connection requests. Increase the RAM or tune the number of instances and connection pool parameters. (For more information, see *Oracle Email Administrator's Guide Release 2 (9.0.4.1)*)
4. If a slow but gradual increase in response time is noted and one or more of your Oracle Collaboration Suite Databases is large, datasets may have become too large. Consider partitioning your Oracle Collaboration Suite Database.

46.3.2 COPY Failure Rate (Failures/minute)

This metric measures the rate of COPY commands that failed per minute.

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 46–3 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 10 Minutes	After Every Sample	>	300	500	1	The number of failed COPY operations are %value%

User Action

The COPY command fails if the IMAP Server is unable to contact an Oracle Collaboration Suite Database. A sudden increase in failures can also occur when an Oracle Collaboration Suite Database runs out of resources, such as disk space.

1. Check that the network between the IMAP Server and the Oracle Collaboration Suite Database is up and running
2. Check that the Oracle Collaboration Suite Database and the listener for the Oracle Collaboration Suite Database is up and running, and that the connect string is accurately registered in the infrastructure Oracle directory server
3. Check that your Oracle Collaboration Suite Database has enough available tablespace to copy the message

46.3.3 COPY Rate (Requests/minute)

This metric measures the rate of COPY commands invoked per minute. This is an informational metric used to gain an understanding of the usage patterns and resource requirements of the mail system.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.4 FETCH Details

This category charts the rate of FETCH commands requested by all clients of IMAP Server instances on this target over the collection period. An IMAP client will use the FETCH command to get most types of message data from an Oracle Collaboration Suite Database, including message identifiers, header information, messages, and message body parts.

46.4.1 FETCH Average Time (milliseconds)

This metric graphs the average time (in milliseconds) required by an IMAP Server to respond to a FETCH command. This metric represents an aggregate average and can be used to identify the presence of long term trends in the latency of the FETCH command. Trending increases in average time typically mean that the IMAP reads from an Oracle Collaboration Suite Database cannot keep up with the number of requests received. An increase in FETCH latency is often accompanied by an increase in the latencies of other IMAP and SMTP process commands.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

When an increase in the latency of a command is detected, check the latency of other mail protocol server commands (POP and SMTP) for similar increases that could indicate degradation of one or more of a system's Oracle Collaboration Suite Databases. Review the Enterprise Manager metrics for the Oracle Collaboration Suite Database instance. Common reasons for latency increases include:

1. Insufficient processor or memory or inefficient use of memory for the Oracle Collaboration Suite Database may indicate that the database or host do not have enough memory allocated to support the transaction load against the database. Apply more resources to the Oracle Collaboration Suite Database or tune the Oracle Collaboration Suite Database. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about tuning a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.
2. Too many connections are configured for the mail protocol servers. All mail protocol servers have a minimum, maximum, and increment value. The minimum number of connections is an aggregate of all server instance minimums. The maximum is an aggregate of all instance maximums. The servers grow and shrink their pools dynamically. Sustained jumps in latency during peak loads followed by returns to normal could be caused by insufficient RAM on the database to process the number of connection requests. Increase the RAM or tune the number of

instances and connection pool parameters. (For more information, see *Oracle Email Administrator's Guide Release 2 (9.0.4.1)*

3. If a slow but gradual increase in response times is noted and one or more of your Oracle Collaboration Suite Databases is large, datasets may have become too large. Consider partitioning your Oracle Collaboration Suite Database.

46.4.2 FETCH Failure Rate (Failures/minute)

This metric graphs the number of FETCH commands per minute that failed to return the message information requested by a client .

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 46–4 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 10 Minutes	After Every Sample	>	300	500	1	The number of failed FETCHes are %value%

User Action

FETCH command failures are often a result of the IMAP Server not being able to connect to one or more of the Oracle Collaboration Suite Databases. Check the following:

1. Verify that the Oracle Collaboration Suite Database and the listener for the Oracle Collaboration Suite Database is up and running.
2. Verify that the connection pool maximum is sufficient for the Oracle Collaboration Suite Database. Email protocol servers share connection pools for all client connections to the Oracle Collaboration Suite Database. This enables a large number of mail client connections to share a smaller number of connections without contention issues. While the multiplier for connection pools will vary widely based upon how the mail system is used, the maximum connect pool value is typically in the 10's to support a concurrent user base in the low thousands. If there is capacity, consider adding another IMAP instance on this host or increasing the maximum connection pool size per IMAP instance.

46.4.3 FETCH Rate (Requests/minute)

This informational metric represents the rate of FETCH commands occurring over a period of time. This rate should vary proportionally to the number and type of mail clients concurrently connected. Changes in this value can be caused by a "rogue" client or by users changing from one type of mail client to another. The FETCH commands rate indicates the usage patterns and resource requirements of the mail system.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.5 LOGIN Details

This category contains metrics that provide information about the LOGIN command. The IMAP protocol is a session-oriented protocol. Mail clients authenticate and log into an IMAP Server. A successful login results in a session that is maintained between the client and the server until the mail client disconnects or the session times out.

46.5.1 LOGIN Average Time (milliseconds)

This metric represents the average time between an IMAP Server receiving a valid login command and responding successfully. The average login time is recorded in hundredths of a second. Processing of the LOGIN command includes an authentication between the IMAP and Oracle directory servers and a check to make sure there is an available connection into the user's default Oracle Collaboration Suite Database.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Increases in the response times to the login command may indicate problems in the Oracle directory server, your network, or Oracle Collaboration Suite Database. When an increase in the latency of a command is detected, check the latency of commands to other mail protocol servers (POP and SMTP) for similar increases.

Review the Enterprise Manager metrics for the infrastructure database, the Oracle directory server, and the Oracle Collaboration Suite Database instance(s). Common issues include:

1. (1) Network Latencies. Check the response time between this IMAP Server and the host where the Oracle directory server is running. Check the response time between this IMAP Server and the Oracle Collaboration Suite Database(s).
2. (2) Insufficient processor or memory or inefficient use of memory for the Oracle Collaboration Suite Database. Apply more resources to the Oracle Collaboration Suite Database or tune the Oracle Collaboration Suite Database. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about tuning a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.
3. (3) Too many connections are configured for the mail protocol servers. All mail protocol servers have a minimum, maximum and increment value. The minimum number of connection is an aggregate of all server instances minimums. The maximum is an aggregate of all instances maximums. The servers grow and shrink their pools dynamically. Sustained jumps in latency during peak loads followed by a return to normal could be caused by insufficient RAM on the database to process the number of connection requests. Increase the RAM or tune the number of

instances and connection pool parameters. (For more information, see *Oracle Email Administrator's Guide Release 2 (9.0.4.1)*

4. (4) If a slow but gradual increase in response times is noted and one or more of your Oracle Collaboration Suite Databases is quite large, datasets may have become too large. Consider partitioning your Oracle Collaboration Suite Database.

46.5.2 LOGIN Failure Rate (Failures/minute)

This metric graphs a rate of IMAP LOGIN command failures. It is an aggregate value, counting login failures due to invalid user names or passwords, account validatation failures against an Oracle directory server, and failures to access an Oracle Collaboration Suite Database after successfully validating the account.

To successfully process an IMAP LOGIN command, the IMAP Server first communicates with the Oracle directory server to authenticate the user. A successful authentication with the Oracle directory server returns an Oracle Collaboration Suite Database to which the client will need a connection. If the IMAP Server is not able to communicate with the default Oracle Collaboration Suite Database, the login returns a failure.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

When an increase in LOGIN command failures is noted, check for the following:

1. Connectivity to the Oracle directory server and the Oracle Collaboration Suite Database. Check that the Oracle Collaboration Suite Database is up and running, the listener for the Oracle Collaboration Suite Database is up and running, and the connect string is registered properly in the infrastructure Oracle directory server. Also, check whether a process on the target is able to connect to and log into the Oracle directory server for the installation.
2. Unusually large numbers of invalid user account and password pairs attempting to log in. You can test for these conditions on a test account for each Oracle Collaboration Suite Database. If you are able to log into the IMAP Server successfully with a test account and you still notice a large number of failures, this could indicate an attack on your IMAP Server.
3. Check the log files to make sure there are sufficient Oracle directory server resources for your valid clients. Use esd_logscan.pl to scan the server log files.
4. While the IMAP Server is running with a log level of "17" or higher, the IP addresses of clients trying to log in to the server are logged in the log files. Check the log files to find out the IP addresses of clients with large numbers of failed login requests. Use esd_logscan.pl to scan the server log files.

46.5.3 LOGIN Rate (Requests/minute)

This informational metric graphs the rate of LOGIN commands per minute during the period since the last capture of the information. Login behavior is specific to the mail client. Some mail clients will log into an IMAP Server multiple times in order to gain

performance advantages. Use the LOGIN command rate to better understand the usage patterns and resource requirements of the mail system.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.6 Network

This section contains metrics that provide information on network resources used by the IMAP Server. This includes the number of bytes transferred to and from this server and the number of client connections to this server.

46.6.1 Client Connection Rate (Connections/minute)

This metric shows the number of new client sessions created per minute. Mail clients typically have two type of sessions. One is a "long running session", which is usually open indefinitely and is used to get new mails in a user's Inbox. The other is type is a "short lived" session used for other housekeeping work like "check for changes in all folders" or "put a copy of sent message on server".

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

An increasing trend in this metric may indicate one or more of following:

1. An increase in user population and a greater number of users currently using IMAP.
2. A possible change in the type of mail client used by the majority of the user population. Different mail clients behave differently and may need greater or fewer numbers of IMAP sessions for normal usage.
3. A possible denial-of-service attack on server. Check the IMAP Server log files for any rejected connections. Use esd_logscan.pl to scan the server log files. You can can decrease the number of connections allowed from a given IP address by tuning the native flood control mechanism.

46.6.2 Client Connection Timeout Rate (Timeouts/Minute)

This metric indicates the rate of sessions terminated per minute by the IMAP Server due to "timeout". IMAP clients typically keep a session alive by issuing another command on the session before the timeout occurs.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Configure the session timeout parameter of the IMAP Server as needed. It is generally not necessary to increase the session timeout parameter to more than 30 minutes.

46.6.3 Current Client Connections

This metric shows the number of client sessions currently open on the IMAP Server. Mail clients typically have two type of sessions. One is a "long running session", which is usually open indefinitely and is used to get new mails in a user's Inbox. The other is type is a "short lived" session used for other housekeeping work like "check for changes in all folders" or "put a copy of sent message on server".

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

An increasing trend in this metric may indicate one or more of following:

1. An increase in user population and a greater number of users currently using IMAP.
2. A possible change in the type of mail client used by the majority of the user population. Different mail clients behave differently and may need different numbers of IMAP sessions for normal usage.
3. A possible denial-of-service attack on server. Check the IMAP Server log files for any rejected connections. Use esd_logscan.pl to scan the server log files. A native flood control mechanism can be tuned to lower the number of connections allowed from a given IP address.

46.6.4 Data Reception Rate (Kb/minute)

This informational metric measures the amount of data the IMAP Server received per minute from IMAP clients. It includes data related to normal IMAP commands and data due to messages appended back to the server, typically to the "Sent" or "Sent Items" folder.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.6.5 Data Transmission Rate (Kb/minute)

This informational metric measures the amount of data sent to clients per minute by the IMAP Server. The data includes mail and IMAP responses.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.7 New Mail Check

This category provides information about IMAP Server's internal mechanism for detecting the arrival of new mail or any other changes to message metadata in a currently selected folder.

46.7.1 Client New Mail Check Average Time (milliseconds)

This metric shows the average time the IMAP Server took to respond to New Mail Check commands. The latency includes the time required for the IMAP Server to communicate with an Oracle Collaboration Suite Database to be alerted to new email messages or changes to metadata for existing email messages and the time required to update information in an Oracle Collaboration Suite Database.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Increases in the response times may indicate problems in your network or your Oracle Collaboration Suite Databases. When an increase in the latency of a command is detected, check the latency of commands to other mail protocol servers (POP and SMTP) for similar increases, as they are often related.

Review the Enterprise Manager metrics for the infrastructure database, the Oracle directory server, and the Oracle Collaboration Suite Database instance(s). Common issues include:

1. Network Latencies. Check the response time between this IMAP Server and the Oracle Collaboration Suite Database(s).
2. Insufficient processor or memory or inefficient use of memory for the Oracle Collaboration Suite Database. Apply more resources to the Oracle Collaboration Suite Database or tune the Oracle Collaboration Suite Database. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about tuning a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.
3. Too many connections are configured for the mail protocol servers. All mail protocol servers have a minimum, maximum and increment value. The minimum number of connections is an aggregate of all server instances minimums. The

maximum is an aggregate of all instances maximums. The servers grow and shrink their pools dynamically. Sustained jumps in latency during peak loads followed by returns to normal could be caused by insufficient RAM on the database to process the number of connection requests. Increase the RAM or tune the number of instances and connection pool parameters. (For more information, see *Oracle Email Administrator's Guide Release 2 (9.0.4.1)*)

4. If a slow but gradual increase in response time is noted, it means that the average size of the mailboxes in your system is also growing. If datasets have become too large, consider partitioning your Oracle Collaboration Suite Database. Also, check the usage of the sort area in your Oracle Collaboration Suite Databases. The larger the mailbox size, the more sort space in required in the sort area for this New Mail Check.

46.7.2 Client New Mail Check Rate (Requests/minute)

This metric represents the rate at which the IAMP Server is actually performing a "New Mail Check" for clients. This can be controlled to some extent by the "New Mail Pool Interval" parameter for the IMAP Server. The higher the value for this parameter the fewer times the server will do a "New Mail Check". Doing this check more often will increase the load on your Oracle Collaboration Suite Database and doing it less often means users may see a longer delay in getting notification about new mails. The rate of New Mail Check is an informational metric used to gain an understanding of the usage patterns and resource requirements of the mail system

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.8 Resource Usage

This category measures the resource usage by the IMAP Server for resources like Oracle Collaboration Suite Databases and Oracle directory server connections used by the IMAP Server.

46.8.1 Database Connection Failure Rate (Failures/minute)

This metric indicates the number of times per minute that the IMAP Server failed to get a database connection from the pool of database connections. This value should ideally be zero. A connection failure count of greater than zero can occur when the Oracle Collaboration Suite Database receives too many user requests within a short time span. For example, this scenario can occur after the Oracle Collaboration Suite Database comes back online after being offline for some time and all the users try to reconnect to it. In this case, the pool of connections usually stablizes on its own within a few minutes.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

To prevent the Oracle Collaboration Suite Database from being overloaded with new connections in a short span of time, limit the number of new connections allowable per per minute or increase the maximum number of connections allowed to the Oracle Collaboration Suite Database. Increase the maximum number of connections allowed to the Oracle Collaboratin Suite Database if the current maximum is to small to handle user needs under ordinary circumstances.

46.8.2 Database Connections In Use

This metric indicates the number of database connections currently in use by the IMAP Server. This does not represent the total number of connections in pool, but a subset consisting of database connections in the pool that are currently in use.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

An increase in the number of connections currently in use may indicate an increase in IMAP workload or a slowdown in database response time. Use standard database monitoring tools to resolve resource issues.

46.8.3 Protocol Threads In Use

This metric represents the number of Service Provisioning System (SPS) threads busy in the IMAP Server right now. Each busy thread represents one currently active request on an IMAP session.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

An increase in SPS threads may indicate an increase in IMAP workload or a slowdown in database response time. Use standard database monitoring tools to resolve resource issues.

46.9 Response

The IMAP Server Response category checks the IMAP Server process to see if the IMAP Server is running. Note that the IMAP Server response does not check the IMAP service. To see if a user can log into the IMAP Server and perform mail work, refer to the IMAP Service response metrics.

46.9.1 Status

Status is checked by looking for one or more IMAP processes on the target. It does not check whether or not the process has all the required resources needed to support IMAP client connections.

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 46–5 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	=	0	Not Defined	1	Failed to connect to IMAP Server

User Action

You can restart the IMAP Server by selecting the target and clicking the Restart button on the Email home page in the Enterprise Manager. To investigate why the server is down, check for alerts that may have been generated. If the IMAP server does not restart, a probable cause is that the server cannot connect to at least one of the Oracle Collaboration Suite Databases or it cannot connect to the system's Oracle directory server.

1. Check that a process on the target is able to connect to and log into the system's Oracle directory server.
2. Make sure the Oracle Collaboration Suite Database is up and running and the connect string is correctly and accurately registered in the Oracle directory server.

46.10 Security

This category contains metrics that provide information about IMAP service security.

46.10.1 Flood Connections Refusal Rate (Connections/minute)

This represents the rate of new connection requests rejected by IMAP Server per minute. A connection refusal occurs when a server detects that too many new connection requests are coming in a short period of time from any one IP address or there are too many concurrent connections from a given IP address. You can change the number of connections allowed or the time window in which the IMAP Server counts new connection requests.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Check the IMAP Server log files to find out the IP address from which "flooding" is detected. Use esd_logscan.pl to scan the server log files. Make sure only a reasonable number of mail clients are running on this machine. If the machine is running several mail clients for the same (or different) users, the IMAP Server may detect a "flooding". If required, either increase the number of connections allowed or decrease the amount of time in which flooding is detected to the values appropriate for your site and type of mail clients used.

46.11 SELECT Details

This category contains metrics that provide information about the SELECT command. The SELECT command is used by mail clients to 'open' the desired mailbox to start downloading new mails arrived since the last time the mailbox was opened by this client.

46.11.1 SELECT Average Time (milliseconds)

This metric represents the average time the IMAP Server took to respond to a SELECT command. The latency would include the time it took the IMAP Server to communicate with an Oracle Collaboration Suite Database and the time required to update information in an Oracle Collaboration Suite Database. This latency is proportional to the average size of the mailboxes in the mail system. Larger mailboxes will take longer to open.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Increases in the response times to the SELECT command may indicate problems in your network or your Oracle Collaboration Suite Databases. When an increase in the latency of a command is detected, check the latency of commands to other mail protocol servers (POP and SMTP) for similar increases, as they are often related.

Review the Enterprise Manager metrics for the infrastructure database, the Oracle directory server, and the Oracle Collaboration Suite Database instance(s). Common issues include:

1. Network Latencies. Check the response time between this IMAP Server and the Oracle Collaboration Suite Database(s).
2. Insufficient processor or memory or inefficient use of memory for the Oracle Collaboration Suite Database. Apply more resources to the Oracle Collaboration Suite Database or tune the Oracle Collaboration Suite Database. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about tuning a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.
3. Too many connections are configured for the mail protocol servers. All mail protocol servers have a minimum, maximum and increment value. The minimum number of connections is an aggregate of all server instances minimums. The

maximum is an aggregate of all instances maximums. The servers grow and shrink their pools dynamically. Sustained jumps in latency during peak loads followed by returns to normal could be caused by insufficient RAM on the database to process the number of connection requests. Increase the RAM or tune the number of instances and connection pool parameters. (For more information, see *Oracle Email Administrator's Guide Release 2 (9.0.4.1)*)

4. If a slow but gradual increase in response time is noted and one or more of your Oracle Collaboration Suite Databases is large, datasets may have become too large. Consider partitioning the Oracle Collaboration Suite Database.
5. In the case of a slow but gradual increase in response time, check the usage of sort area on your Oracle Collaboration Suite Database. The larger the mailbox size, the more sort space in the sort area is required to initially open the mailbox.

46.11.2 SELECT Failure Rate (Failures/minute)

This metric measures the rate of SELECT commands that failed per minute.

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 46–6 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 10 Minutes	After Every Sample	>	300	500	1	The number of failed SELECTs are %value%

User Action

The SELECT command fails if the IMAP Server is unable to contact an Oracle Collaboration Suite Database. A sudden increase in failures could also occur when an Oracle Collaboration Suite Database runs out of resources, such as disk space.

1. Check that the network between the IMAP Server and the Oracle Collaboration Suite Database is up and running
2. Check that the Oracle Collaboration Suite Database and the listener for the Oracle Collaboration Suite Database is up and running, and that the connect string is accurately registered in the infrastructure Oracle directory server.
3. Check that the selected folders actually exist in the system. Some mail clients work off a "subscribed" folder list. Sometimes folders in this list get deleted by other mail clients but still remain in the "subscribed" folder list. The SELECT command for such folders will always fail. In these cases the issue can be fixed by asking users to refresh their "subscribed" folder list.

46.11.3 SELECT Rate (Requests/minute)

This metric represents the rate of SELECT commands invoked per minute. This an informational metric used to gain an understanding of the usage patterns and resource requirements of the mail system.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.12 STATUS Details

This category contains metrics that provide information about the STATUS command. The STATUS command checks a mailbox for information including the number of messages in the folder, the next message ID that will be given, or the number of recent messages.

Some mail clients use the STATUS command on an Inbox as the mechanism to check for new mail.

46.12.1 STATUS Average Time (milliseconds)

This metric measures the average time the IMAP Server took to respond to a STATUS request. The latency includes the time it took the IMAP Server to communicate with an Oracle Collaboration Suite Database and the time required to find information in an Oracle Collaboration Suite Database.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Increases in the response times to the STATUS command may indicate problems in your network or your Oracle Collaboration Suite Datatbase(s). When an increase in the latency of a command is detected, check the latency of commands to other mail protocol servers (POP and SMTP) for similar increases, as they are often related.

Review the Enterprise Manager metrics for the infrastructure database, the Oracle directory server, and the Oracle Collaboration Suite Database instance(s). Common issues include:

1. Network Latencies. Check the response time between this IMAP Server and the Oracle Collaboration Suite Database(s).
2. Insufficient processor or memory or inefficient use of memory for the Oracle Collaboration Suite Database. Apply more resources to the Oracle Collaboration Suite Database or tune the Oracle Collaboration Suite Database. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about tuning a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.
3. Too many connections are configured for the mail protocol servers. All mail protocol servers have a minimum, maximum and increment value. The minimum number of connections is an aggregate of all server instances minimums. The maximum is an aggregate of all instances maximums. The servers grow and shrink their pools dynamically. Sustained jumps in latency during peak loads followed by

returns to normal could be caused by insufficient RAM on the database to process the number of connection requests. Increase the RAM or tune the number of instances and connection pool parameters. (For more information, see *Oracle Email Administrator's Guide Release 2 (9.0.4.1)*)

4. If a slow but gradual increase in response time is noted and one or more of your Oracle Collaboration Suite Databases is large, datasets may have become too large. Consider partitioning your Oracle Collaboration Suite Database(s).

46.12.2 STATUS Failure Rate (Failures/minute)

This metric represents the rate of STATUS commands that failed per minute.

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 46–7 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 10 Minutes	After Every Sample	>	300	500	1	The number of failed STATUSes are %value%

User Action

The STATUS command fails if the IMAP Server is unable to connect to or retrieve results from an Oracle Collaboration Suite Database.

1. Check that the network between the IMAP Server and the Oracle Collaboration Suite Databaseis up and running
2. Check that the Oracle Collaboration Suite Database is up and running, the listener for the Oracle Collaboration Suite Database is up and running, and the connect string is accurately registered in the infrastructure Oracle directory server

46.12.3 STATUS Rate (Requests/minute)

This informational metric represents the rate of STATUS commands invoked per minute.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

46.13 STORE Details

The STORE command is used by mail clients to change a message's flags (for example, from "unread" to "read") or to annotate a message with additional data.

46.13.1 STORE Average Time (milliseconds)

This metric measures the average time the IMAP Server took to respond to a STORE command. The latency includes the time it took the IMAP Server to communicate with an Oracle Collaboration Suite Database and the time required to update information in an Oracle Collaboration Suite Database.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Increases in the response times to the STORE command may indicate problems in your network or your Oracle Collaboration Suite Database. When an increase in the latency of a command is detected, check the latency of commands to other mail protocol servers (POP and SMTP) for similar increases, as they are often related.

Review the Enterprise Manager metrics for the infrastructure database, the Oracle directory server, and the Oracle Collaboration Suite Database instance(s). Common issues include:

1. Network Latencies. Check the response time between this IMAP Server and the Oracle Collaboration Suite Database(s).
2. Insufficient processor or memory or inefficient use of memory for the Oracle Collaboration Suite Database. Apply more resources to the Oracle Collaboration Suite Database or tune the Oracle Collaboration Suite Database. For more information about an Enterprise Manager metric for a database, see the Oracle Enterprise Manager online help for that metric. For more information about tuning a database, see the *Oracle Database Performance Tuning Guide* or other associated manuals.
3. Too many connections are configured for the mail protocol servers. All mail protocol servers have a minimum, maximum and increment value. The minimum number of connections is an aggregate of all server instances minimums. The maximum is an aggregate of all instances maximums. The servers grow and shrink their pools dynamically. Sustained jumps in latency during peak loads followed by a return to normal could be caused by insufficient RAM on the database to process the number of connection requests. Increase the RAM or tune the number of instances and connection pool parameters. (For more information, see *Oracle Email Administrator's Guide Release (9.0.4.1)*)
4. If a slow but gradual increase in response time is noted and one or more of your Oracle Collaboration Suite Databases is quite large, datasets may have become too large. Consider partitioning the Oracle Collaboration Suite Database.

46.13.2 STORE Failure Rate (Failures/minute)

This metric represents the rate of failed STORE commands per minute.

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 46–8 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 10 Minutes	After Every Sample	>	300	500	1	The number of failed STOREs are %value%

User Action

The STORE command fails if the IMAP Server is unable to connect to or retrieve results from an Oracle Collaboration Suite Database.

1. Check that the network between the IMAP Server and the Oracle Collaboration Suite Database is up and running
2. Check that the Oracle Collaboration Suite Database is up and running, the listener for the Oracle Collaboration Suite Database is up and running, and the connect string is accurately registered in the infrastructure Oracle directory server

46.13.3 STORE Rate (Requests/minute)

This metric measures the rate of STORE commands invoked to this IMAP target per minute. The rate of STORE command is an informational metric used to gain an understanding of the usage patterns and resource requirements of the mail system.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

47

E-Mail IMAP Service

The E-Mail IMAP Service target allows you to monitor the availability and responsiveness of the Oracle Email IMAP Service to client requests. This target is monitored by periodically performing client-like protocol operations in order to determine whether the IMAP Service is available and responding in a reasonable time. This target must be configured manually to refer to the host name and port number that clients use to connect to the Oracle Email IMAP Service. The IMAP Service can be running on a single host or, in large installations, behind a network load balancer or network address translator.

47.1 Response

This metric category captures the response characteristics of the Oracle Email IMAP service as seen by a client application.

47.1.1 Connect Time (ms)

This metric shows the time it takes for the IMAP server to accept a network connection from a client. It also reflects the performance of the Oracle Net Services Listener.

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 47–1 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	>	100	2000	2	Time taken to connect to mail service is %value% (ms)

47.1.2 Login Time (ms)

This metric shows the time it takes for a connected client to log in to the IMAP Server. It is also indicative of the Oracle Internet Directory response time because clients are authenticated against the Oracle directory server.

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 47–2 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	>	2000	5000	2	Time taken to login is %value% (ms)

47.1.3 Status

This metric indicates whether clients are able to access e-mail through the IMAP Service. At least one IMAP server and Oracle Net Services Listener must be running in order for the IMAP Service to be available.

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 47–3 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	=	Not Defined	0	1	Failed to connect to IMAP service

User Action

The IMAP Service logically consists of the Oracle Email IMAP Server and an associated Oracle Net Services Listener listening for IMAP network connection requests. If this service is down, check to see if at least one IMAP server process is running. Also check to see if the Oracle Net Services Listener configured for the Oracle Email system is running.

47.1.4 Time to List Folders (ms)

This metric shows the time it takes to retrieve a user's folder list from the Oracle Collaboration Suite Database (mailstore) through the IMAP server. The folder list includes the Shared and Public folders that a user has access to. This metric is also indicative of the database and directory performance.

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 47–4 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	>	2000	5000	2	Time taken to list folders is %value% (ms)

47.1.5 Time to Retrieve E-Mail (ms)

This metric shows the time it takes to retrieve a message from the Oracle Collaboration Suite Database (mailstore) through the IMAP server. This metric is also indicative of the database performance.

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 47–5 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	>	2000	5000	2	Time taken to read an e-mail is %value% (ms)

47.1.6 Total Time (ms)

This metric shows the total time it takes for one simulated IMAP session. This metric is directly dependent on the performance characteristics of the IMAP Server target.

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 47–6 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	>	5000	10000	2	Total Time taken to read an e-mail is %value% (ms)

User Action

To reduce the total response time, tune your IMAP servers after observing their performance levels. You can also identify which operations in a client session are taking significant time to complete by looking at the other columns in this metric.

48

E-Mail List Server

The E-Mail List Server processes messages sent to Oracle Email public distribution lists. Messages sent to mailing lists of type 'List Server List' are queued into the List Queue by the SMTP Inbound Server. These messages are then picked up by the List Server for further processing and delivery.

48.1 Messages

This category graphs various metrics concerning the receipt and delivery of e-mail messages sent to distribution lists.

48.1.1 Message Processing Rate

This metric indicates the efficiency of the list servers. However, the value depends on several factors such as the type of list to which the messages are being sent, the number of members in the distribution list, the size and type of incoming messages.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

This metric must be interpreted in conjunction with the Length of List Queue metric of the Oracle Collaboration Suite Database (mailstore) target. If the List Queue is also empty or near empty, there is no problem. It means there are very few messages being sent to distribution lists. This is normal. If the List Queue is long but the Message Processing Rate is low then users will experience delays in receiving messages delivered to distribution lists. Check the following:

1. First, use the monitoring tools available on your operating system (for example, sar and top,) to check for sufficient operating system resources.
2. If operating system resources are available, message delivery may be slow. Check the list server logs files for any errors accessing the Oracle directory server access and/or the Oracle Collaboration Suite Database (mailstore).
3. Check the Messages metrics in the SMTP Inbound and Outbound Servers. These may also provide some information, because most of the delivery related problems are common to the SMTP and List Servers.

48.1.2 Number of Messages Being Processed

This metric indicates the number of messages that are currently being processed by the List Server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

48.2 Resource Usage

This category measures the resource usage by the list servers on a host. Resources usage of host resources such as CPU and Memory can be obtained from the Host target metrics.

48.2.1 Database Connections In Use

This metric measures the number of database connections to the Oracle directory server currently being used by the List Server. The List Server can be configured to pre-establish a pool of connections to the Oracle directory server, enabling the List Server to quickly access directory information when needed. The number of connections being used at a particular time depends on the number of messages being processed by the List Server at that time. Connections that are idle for long periods (as determined by the LDAP Connection Pool timeout value) will be closed automatically.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

48.3 Response

This category contains metrics that provide information about the Up/Down status of the List Server.

48.3.1 Status

This metric provides information about the Up/Down status of the List Server and alerts you when the status is down. The List Server shows a status of Down when all List processes on the host are down.

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 48–1 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	E-Mail List Server not running

User Action

You can restart the List Server by selecting the target and clicking the Restart button on the Email Application home page in Enterprise Manager. To investigate why the List Server is down, check for any alerts that may have been generated. If the List Server does not restart, probable causes are an inability to connect to at least one of the mail information stores or the system's Oracle directory server. Check the server log file for more details. Use esd_logscan.pl to scan the server log files.

49

E-Mail Middle Tier

This target is an aggregate representing all middle tier Oracle Email processes on the host. A Start or Stop operation on this target applies the operation successively to all the other Oracle Email targets on the host.

49.1 Response

This indicates whether at least one Oracle Email server is running on the host.

49.1.1 Status

An 'Up' status indicates that at least one Oracle Email process is running on the host, and a 'Down' status indicates that no Oracle Email process is running. However, it does not distinguish what kind of Oracle Email process, for example, SMTP or IMAP, is running.

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 49–1 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	=	0	Not Defined	1	All Oracle Email Middle Tier processes are down

50

E-Mail NNTP Inbound Server

The Network News Transfer Protocol (NNTP) Inbound Server target provides session-oriented access for Internet Standards Based news clients. The metric categories provide statistical information on these NNTP servers.

50.1 Messages

This category includes metrics that provide information about messages for your NNTP Inbound Servers.

50.1.1 Message Posting Rate (Messages/minute)

This indicates the rate at which messages are being posted to news groups. This metric is primarily informational and indirectly indicates the message insertion load placed on the Oracle Collaboration Suite Database.

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 50–1 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 10 Minutes	After Every Sample	>	100	500	1	The messages posting rate is %value% messages/minute

User Action

Sustained high values may indicate either a high traffic system, which is normal and requires no action, or a possible security breach which should be further investigated.

50.1.2 Message Retrieval Rate (Messages/minute)

This metric indicates the rate at which messages are being retrieved from news groups in your system. This metric is primarily informational and indirectly indicates the load placed on the Oracle Collaboration Suite Database and the server message cache.

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 50–2 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 10 Minutes	After Every Sample	>	100	500	1	The messages retrieval rate is %value% messsages/ minute

User Action

Sustained high values may indicate either a high traffic system, which is normal and requires no action, or a possible security breach which should be further investigated.

50.2 Network

This category includes network related metrics for the NNTP Inbound Server.

50.2.1 Client Connection Rate (Connections/minute)

This metric represents the rate of connections opened to the NNTP_IN Server per minute.

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 50–3 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 10 Minutes	After Every Sample	>	50	100	1	The rate of inbound NNTP connections is %value% connections/minute

User Action

Sustained high values may indicate a possible security breach (denial-of-service attack) on your system and should be further investigated. Check the NNTP server log files for any rejected connections. Use esd_logscan.pl to scan the server log files.

50.2.2 Current Client Connections

This metric represents a gauge that counts the number of open connections to the NNTP Inbound Server. The counter is increased by one as soon as a connection request comes in and is decreased by one when a connection is closed.

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 50–4 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 10 Minutes	After Every Sample	>	500	1000	1	The current number of client connections are %value%

User Action

This metric should be consistent with the expected client load pattern for your system, that is, it should approximate the number of clients expected to be browsing newsgroups. Sustained high values could indicate an possible security breach (denial-of-service attack) in your system and should be further investigated. Check the NNTP server log files for any rejected connections. Use esd_logscan.pl to scan the server log files.

50.3 Newsgroups

This metric category consists of news group related protocol server activity.

50.3.1 Newsgroup Selection Rate (Requests/minute)

This metric indicates the rate at which newsgroups are being selected. Each group request also triggers a directory and database query. Thus, this metric indirectly indicates the load on your directory and database servers from the NNTP Inbound Server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Newsgroup selection by the client is a frequent activity. Sustained low values indicate that your news user population is very small or your news servers are not fully utilized. In this cased, if you are running several news server instances, some of them can be shut down.

50.3.2 Newsgroups Listing Rate (Requests/minute)

This metric indicates the rate at which clients are listing news groups. The newsgroup listing is obtained from the directory and database servers using several successive queries. Thus, this metric indirectly indicates the load on your Oracle directory server and Oracle Collaboration Suite Databases from the NNTP Inbound Server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

This is an infrequent client operation. In normal operation it must be near or at zero. Sustained high values for this metric indicate a possible security breach (denial of service attack) on your system and should be further investigated. Check the NNTP server log files for any rejected connections. Use esd_logscan.pl to scan the server log files.

50.4 Resource Usage

This category contains metrics related to NNTP Inbound Server resource usage.

50.4.1 Message Cache Hit Ratio (Hits / (Hits + Misses))

This metric is relevant only if Message Caching is enabled in the NNTP Inbound Server. This metric indicates the effectiveness of caching and should be between 0.5 and 1.0. Lower values usually mean that the caching is not useful for the client usage pattern for your system. A cache will be most effective when there are high traffic newsgroups with high levels of message retrieval.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Message caching increases the memory usage on your host. A cache hit ratio does not usually justify the extra memory used by the server. If you see sustained values below 0.25 it is probably more efficient to turn off message caching in the NNTP Inbound Servers and reduce memory usage.

50.4.2 Protocol Threads In Use

This metric indicates the number of threads which are in use in the multi-threaded NNTP Inbound Server processes on the host. Threads are destroyed if they remain idle for long (configurable) periods of time.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

50.5 Response

The NNTP Inbound Server response category checks the NNTP Inbound Server process to see if the NNTP Inbound Server is running. Note that the NNTP Inbound Server response does not check the NNTP Inbound service. To see if a user can log into the NNTP Inbound Server refer to the NNTP Inbound Service response metrics.

50.5.1 Status

This metric indiates whether at least one NNTP Server is running on the mid-tier host.

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 50–5 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	=	Not Defined	0	1	Failed to connect to NNTP server

User Action

If the NNTP Inbound processes were intentionally stopped, they can be restarted. If the NNTP Inbound processes should be up but are not, then that is an indication they were not able to successfully initialize. Probable causes are an inability to contact or connect to either one of the mail information stores or the Oracle directory server. Perform the following checks.

1. Check that a process on the target is able to connect to and log into the Oracle directory server for the installation.
2. Verify that the Oracle Collaboration Suite Database is up and running and the connect string is correctly and accurately registered in the Oracle directory server.

51

E-Mail NNTP Inbound Service

The E-Mail NNTP Service target allows you to monitor the Oracle Email system at the service level. This target is monitored by automatically performing client-like protocol operations in order to to monitor whether the NNTP Service is available and responding in a reasonable time. This target must be configured manually to refer to the host name and port number that is used to connect to the Oracle Email NNTP Service address. The NNTP service can be running from a single host or, in large installations, behind a network load balancer or network address translator.

51.1 Response

The metrics in this category capture the response characteristics of the Oracle Email NNTP service as seen by a client application.

51.1.1 Connect Time (ms)

This metric shows the time taken for the NNTP server to accept a network connection from a client. It is also indicative of the performance of the Oracle Net Services Listener.

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 51–1 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	>	100	2000	2	Time to connect to news service is %value% (ms)

User Action

None. This is for informational purposes only. This metric is aggregated into the Total Time Metric.

51.1.2 Status

This metric shows whether newsgroup clients are able to access newsgroup articles via the NNTP Service. At least one NNTP service and Oracle Net Services Listener must be running in order for the NNTP Service to be available.

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 51–2 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	=	Not Defined	0	1	Failed to connect to NNTP service

User Action

The NNTP Service logically consists of the Oracle Email NNTP Server and an associated Oracle Net Services Listener which listens for NNTP network connection requests. If this service is down, check to see if at least one NNTP server process is running. Also check to see if the Oracle Net Services Listener configured for the Oracle Email system is running.

51.1.3 Time to Post News Article (ms)

This metric shows the time taken to post a message to a newsgroup through the NNTP server. This metric is also indicative of database performance because news messages are stored in the Oracle Collaboration Suite Database (mailstore).

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 51–3 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	>	2000	5000	2	Time to post article is %value% (ms)

User Action

None. This is for informational purposes only. This metric is aggregated into the Total Time Metric.

51.1.4 Time to Retrieve News Article (ms)

This metric shows the time taken to retrieve a message from the Oracle Collaboration Suite Database (mailstore) through the NNTP server. This metric is also indicative of database performance.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 5 minutes

User Action

None. This metric is for informational purposes only. This metric is aggregated into the Total Time Metric.

51.1.5 Total Time (ms)

This metric shows the total time taken to complete one simulated NNTP session. This metric is directly dependent on the performance characteristics of the NNTP Server target.

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 51–4 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	>	2000	5000	2	Time to post article is %value% (ms)

User Action

To reduce the total response time, tune the NNTP servers after observing their performance levels. You can also identify which operations in a client session are taking time by looking at the other columns in this metric.

52

E-Mail NNTP Outbound Server

The NNTP Outbound Server propagates feed messages to other NNTP peer servers. Messages are propagated based on the server Outbound Feed settings. Messages being propagated will be queued in the Newsfeed Queue by the NNTP Inbound Server at the time the message is received.

52.1 Messages

This category includes metrics pertaining to news messages leaving the Oracle Email system.

52.1.1 Message Transmission Error Rate (Messages/minute)

This metric indicates the rate of errors in the news feed. Errors include network outages, misconfigured peer details, host connection failures, and so on. This rate should ideally be zero or very low.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Sustained high values for this metric usually indicate that there are problems with the quality of network connections between the Oracle Email system and the news peer servers. For example, a slow network is causing the peer to timeout and close connections. Check the following:

1. Check to see if sufficient network resources are available and that peer servers are functioning normally.
2. Check the NNTP Outbound Server log files to see what kind of errors, if any, have been noted by the server. Use esd_logscan.pl to scan the server log files.

52.1.2 Message Transmission Rate (Messages/minute)

This metric indicates the rate at which news messages are being fed to all NNTP peer servers configured to receive feed.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

This metric must be interpreted in conjunction with the Newsfeed Queue metric of the Oracle Collaboration Suite Database (mailstore) target. If the List Queue is also empty or near empty, this is an indication that there are very few messages being fed to peers and this is normal. If the Newsfeed Queue is long but the Message processing rate is low, then users will experience delays in receiving responses to messages posted to newsgroups. Check the following:

1. First, use the monitoring tools available on your operating system (for example, sar, and top) to verify there are sufficient operating system resources.
2. Next, check to see if the network connection between your system and peer servers are congested.
3. If operating system resources are available and the network is not congested, check the NNTP Outbound Server log files for any errors in accessing the Oracle directory server and/or the Oracle Collaboration Suite Database. Use esd_logscan.pl to scan the server log files.

52.1.3 Message Transmission Refusal Rate (Messages/minute)

This metric indicates the number of messages that were offered to a peer, but were refused because the peer had already received it from another server. It is normal for this metric to be non-zero. Sustained high values could mean that the remote peers are receiving feeds from other servers and probably are not required to be fed from the Oracle Email system.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Message refusal is not considered an error and merely indicates that the peer already has the message or does not want it for some reason, such as spam check failures. Sustained high values for this metric indicate that peer servers are receiving news messages from other news server before the Oracle Email system can propagate them. This is applicable only to messages that are passing through the system.

52.2 Resource Usage

This category contains metrics related to NNTP Outbound Server resource usage.

52.2.1 Connection Cache Hit Ratio (Hits / (Hits + Misses))

This metric details the efficiency with which network connections are opened to peer servers. For systems with high Message Transfer Rates, this metric should be close to 1. Low values for this metric do not necessarily indicate a problem.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

This metric can be used to tune the connection cache parameter of the NNTP Outbound Server. Adjust the number of connections in the cache and the timeout value of the connections so that this metric is always close to 1.0. However, if the outbound feed traffic is very low in your system, as indicated by the Message Transmission Rate, it is usually more efficient to keep this metric at zero by setting the number of cached connections to zero.

52.3 Response

This category contains metrics that provide information about the Up/Down status of the NNTP Outbound Server.

52.3.1 Status

This metric provides information about the Up/Down status of the NNTP Outbound Server and alerts you when the status is down. The NNTP Outbound Server shows a status of Down when all processes on the host are down.

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 52–1 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	Failed to connect to NNTP server

User Action

You can restart the NNTP Outbound Server by selecting the target and clicking the **Restart** button on the Email Application home page. To investigate why the service is down, check for alerts that may have been generated. If the NNTP Outbound Server does not restart, the likely cause is that the server cannot connect to at least one of the Oracle Collaboration Suite Databases (mailstores) or to the Oracle directory server.

53

E-Mail SMTP Inbound Server

The SMTP Inbound Server handles incoming SMTP connections and receives messages over those connections. Messages are either delivered locally or placed into queues for further processing.

If the Submit Only SMTP Inbound Server parameter is set to "False", the server receives incoming messages, queries the Oracle directory server to find and authenticate the addresses, rewrites addresses based on the rewriting rules, and applies anti-spam rules. If all the steps are successful, the SMTP Inbound Server accepts the message and inserts it into the corresponding queue based on the destination address.

If the recipient is an outside user, the message is stored in the Relay Queue to wait for further processing. If the recipient is local, the message is stored in the Local Queue. The list of local domains contained in the Local Domains parameter is used to determine if an address is local. The local delivery module picks up the message later, applies the rules, and delivers it to the user's inbox.

To increase throughput, you can prevent messages from being processed immediately by the SMTP Inbound Server by setting the Submit Only parameter to "True". Messages will then be stored into the Submit Queue without any additional processing. The messages will then be processed by the SMTP Outbound Server.

53.1 Messages

This category graphs various metrics on the receipt and delivery of e-mail messages. Metrics related to delivery are non-zero only if the SMTP Inbound Server has the Submit Only parameter set to "False".

53.1.1 Message Deferral Rate (Messages/minute)

This metric measures the per minute rate at which the SMTP Inbound Server is unable to complete delivery of e-mail messages to the Inboxes of users in local domains. This metric will always equal zero if the SMTP Inbound Server has the Submit Only parameter set to "True". In general, messages are deferred for later processing due to temporary failures that soon correct themselves. Possible reasons for local delivery to fail are:

1. Folder lock errors (This is the most common reason.)
2. Database access failures, for example, an Oracle Collaboration Suite Database is down or unreachable
3. Oracle Internet Directory access failures
4. Temporay filter processing errors, if filtering is enabled

5. Temporary rule processing errors

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 53–1 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 10 Minutes	After Every Sample	>	2000	3000	1	The message deferral rate is %value% messages/minute

User Action

If the SMTP Inbound Server cannot deliver a message into an Oracle Collaboration Suite Database (mailstore), check to see if the recipient's Inbox is locked. One way to do this is to check SMTP Inbound Server logs for folder lock errors. This situation is generally temporary and does not usually require that you take any action. Also, confirm that SMTP Inbound Server can access the Oracle Collaboration Suite Database and the Oracle directory server. Check for possible filter or scanner failures or server-side rule processing failures.

53.1.2 Message Reception Rate (Messages/minute)

This metric measures the number of e-mail messages received per minute. Messages can be received both from user clients and from other MTAs.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

User Action

Sustained, unusually high rates of incoming messages may be an indicator of a denial-of-service attack or a spam attack. Check to see whether the SMTP Inbound Server is configured as an open relay. Change the logging level of the SMTP Inbound Server to the Notification level. Check the server log files for ESSM-426 messages which describe where connections are coming from, and check for ESSM-427 messages which log the "Sender:" of incoming messages. Use esd_logscan.pl to scan the server log files.

53.1.3 Message Transmission Rate (Messages/minute)

This metric measures the per-minute rate of message delivery to local domain Inboxes. If the Submit Only parameter is set to "True", this metric will always be zero. This is an information metric only.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

53.2 Network

This category contains metrics that provide information on network resources used by the SMTP Inbound Server. This includes the number of bytes transfered to and from the SMTP Inbound Server and the number of client connections to this server.

53.2.1 Current Active SMTP Connections

This metric represents a gauge that measures the current number of connections to the SMTP Inbound target that are actively transmitting SMTP traffic.

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 53–2 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 10 Minutes	After Every Sample	>	1000	1500	1	The number of active inbound SMTP connections is %value%

User Action

If the number of connections exceeds the threshold, it could be an indication of a SPAM attack or some rogue server/client sending large number of mails. Change the logging level of the SMTP Inbound Server to the Notification level, Refresh the server, and then check the server log files for ESSM-426 messages which describe where the connections are coming from, and check for ESSM-427 messages which log the "Sender:" of incoming messages. Use esd_logscan.pl to scan the server log files.

If you can identify the source sender, host, or IP then take corrective actions to block them. The routing controls can be used for this purpose.

Another possible reason for a high number of connections is that the server is not accepting mails fast enough. This can be caused by a variety of problems.

1. Insufficent resources on host computers. Check CPU and memory resources on host computers to make sure there is sufficient capacity to handle the workload. Also check for any processes consuming excessive CPU or memory.
2. Database performance problems or errors. Check the Enterprise Manager pages used to monitor the performance of the database for any warnings or alerts.
3. Oracle directory server performance problems or errors. Check the Enterprise Manager pages used to monitor the peformance of the Oracle directory server for any warnings or alerts.

4. If there are no performance problems with the Oracle Collaboration Suite Database or withthe Oracle directory server, and the SMTP Inbound Server is processing at the expected rate, consider increasing the number of processes configured for the SMTP Inbound Server. Also, the throughput of the SMTP Inbound Server can be increased by configuring the Submit Only parameter to "True". It will then do minimal processing on incoming e-mail and leave most of the work to be handled by the SMTP_OUT Server.

53.2.2 Current Client Connections

This metric represents the number of client connections to the SMTP Inbound Server. The counter is incremented by one as soon as a connection request comes in, and it is decremented when the connection is closed.

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 53–3 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 10 Minutes	After Every Sample	>	1000	1500	1	The number of client connections is %value%

User Action

This metric contains information similar to the Current Active SMTP Connections metric. The values of the SMTP and client connections should be relatively close to each other. If the number of Current Client Connections is dramatically higher than the number of Current Active SMTP Connections, this could be an indication that your SMTP Inbound server is under a denial-of-service attack. The Thread Timeout parameter controls how long a connection can remain idle before the connection is closed.

If the number of connections exceeds the threshold, it could be an indication of a SPAM attack or some rogue server/client sending large number of mails. Change the logging level of the SMTP Inbound Server to the Notification level, Refresh the server, and then check the server log files for ESSM-426 messages which describe where the connections are coming from, and check for ESSM-427 messages which log the "Sender:" of incoming messages. Use esd_logscan.pl to scan the server log files. If you can identify the source sender, host, or IP then take corrective actions to block them. The routing controls can be used for this purpose.

Another possible reason for a high number of connections is that the server is not accepting mails fast enough. This can be caused by the following:

1. Insufficent resources on host computers. Check CPU and memory resources on host computers to make sure there is sufficient capacity to handle the workload. Also check for any processes consuming excessive CPU or memory.
2. Database performance problems or errors. Check the Enterprise Manager pages used to monitor the performance of the database for any warnings or alerts.

3. Oracle directory server performance problems or errors. Check the Enterprise Manager pages used to monitor the peformance of the Oracle directory server for any warnings or alerts.
4. If there are no performance problems with the Oracle Collaboration Suite Database or with the Oracle directory server, and the SMTP Inbound Server is processing at the expected rate, consider increasing the number of processes configured for the SMTP Inbound Server. Also, the throughput of the SMTP Inbound Server can be increased by configuring the Submit Only parameter to "True". It will then do minimal processing on incoming e-mail and leave most of the work to be handled by the SMTP Outbound Server.

53.2.3 Data Reception Rate (Kb/minute)

This metric measures the number of kilobytes of data received per minute over inbound SMTP connections. Data is received both from user clients and from other MTAs.

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 53–4 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 10 Minutes	After Every Sample	>	200000	250000	1	The data reception rate is %value% Kb/minute

User Action

Sustained, unusually high rates of incoming data may be an indicator of a denial-of-service attack or a spam attack. Check to see whether the SMTP Inbound Server is configured as an open relay. Change the logging level of the SMTP Inbound Server to the Notification level, and check the server log files for ESSM-426 messages which describe where connections are coming from. Use esd_logscan.pl to scan the server log files.

53.2.4 Data Transmission Rate (Kb/minute)

This metric represents the number of kilobytes per minute delivered by the SMTP Inbound Server to local domain Inboxes. If the Submit Only parameter is set to True, this metric will always be zero. This is an informational metric only.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

53.2.5 SMTP Inbound Connection Rate

This metric measures the number of inbound SMTP connections accepted per minute. Inbound connections come from both user clients and from other MTAs.

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 53–5 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 10 Minutes	After Every Sample	>	1000	1500	1	The SMTP inbound connection rate is %value% connections/minute

User Action

Sustained, unusually high rates of inbound SMTP connections may indicate of a denial-of-service attack or a spam attack. Check to see whether the SMTP Inbound Server is configured as an open relay. Change the logging level of the SMTP Inbound Server to the Notification level, and check the server log files for ESSM-426 messages which describe where the connections are coming from. Use esd_logscan.pl to scan the server log files.

53.3 Response

This category contains metrics that provide information about the Up/Down status of the SMTP Inbound Server.

53.3.1 Status

This metric provides information about the Up/Down status of the SMTP Inbound Server and alerts you when the status is down. The SMTP Inbound Server shows a status of Down when all SMTP Inbound processes on the target are down.

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 53–6 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	=	0	Not Defined	1	The SMTP Server is down

User Action

You can start the SMTP Inbound Server by selecting the target and clicking the**Start** button on the Email Application home page. If the SMTP Inbound Server does not start, a probable cause is that the server cannot connect to at least one of the mailstores or it cannot connect to the system's Oracle directory server.

1. Check that a process on the target host is able to connect to and log into the system's Oracle directory server.
2. Make sure the Oracle Collaboration Suite Database is up and running and the connect string is correctly and accurately registered in the Oracle directory server.
3. Check the log files in the OPMN log file directory for errors. Use esd_logscan.pl to scan the log files.
4. Check the SMTP Inbound Server log files for errors. Use esd_logscan.pl to scan the server log files.

53.4 Routing Control

This category graphs various metrics concerning the routing control features of the SMTP Inbound Server. Metrics in this category are applicable only if native spamming is enabled.

53.4.1 Client Connection Floods Rate

The metric measures the per minute rate at which the SMTP Inbound Server detects connection "flooding" from client hosts. Flooding from a host occurs if the number of messages plus the number of connections from a host exceeds a maximum flood count within an allowed interval. Both the flood count and the interval are configurable. When flooding is detected, further connections and/or messages from the host are rejected for the remainder of the current interval and the duration of the next interval.

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 53–7 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 10 Minutes	After Every Sample	>	500	1000	1	SMTP routing control flood connection detected: %value% rejected connections/minute

User Action

If the server is experiencing flooding from a host, consider adding this host to the rejected IP address list.

You can determine if the SMTP Inbound Server is experiencing flooding from a host by setting the logging level of the SMTP Inbound Server to the Notification level, refreshing the server, and then checking the server log files for ESSM-502 messages. Use esd_logscan.pl to scan the server log files.

53.4.2 Client IP-Address Check Failure Rate

This metric measures the rate per minute of connect request failures due to connection requests for a client associated with a rejected IP address. The detection is based upon configured parameters and flooding of messages or connections from the host. The metric measures client connection rejections due to the following conditions:

1. Whether the client host's IP address is in the list of rejected IP addresses
2. Whether the client host's domain, obtained from DNS (Domain Name Service), has an IP address that is associated with a host in the list of rejected host domains. If the client host domain cannot be obtained from DNS due to the DNS check or other failures (temporary or permanent), the metric is not updated even if the host domain is in the list of rejected host domains. However, if the DNS check is enabled, the metric is updated for both temporary and permanent failures from DNS.
3. Flooding detected from the client's host and, therefore, no further connections can be accepted for a period of time

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 53–8 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 10 Minutes	After Every Sample	>	500	1000	1	SMTP routing control client IP address check: %value% rejected messages/minute

User Action

Review the routing control settings to be sure that valid e-mail messages are not being rejected.

If the log level of the SMTP Inbound Server is set to Notification, the server will log ESSM-502 messages when it rejects messages based on the routing control settings.

53.4.3 Message Envelope Domain Check Failure Rate

If the DNS check on the HELO/EHLO domain is enabled, this metric measures the per minute rate of messages rejected because they were sent from a domain that does not exist in the Domain Name Server (DNS) or are due to temporary failures from a DNS query.

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 53–9 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 10 Minutes	After Every Sample	>	500	1000	1	SMTP routing control message envelope domain check : %value% rejected messages/minute

User Action

If the value is non-zero, check the logs to see if there is a problem with the Domain Name Service. If the problem cannot be resolved, consider disabling this check. If the domain name indicated in the SMTP_IN command indicates possible spam, consider adding the clients host the the rejected IP address list.

53.4.4 Message Envelope Recipient Check Failure Rate

This metric measures the per minute rate of messages rejected because of any of the following problems with the recipient's address:

1. The maximum number of allowed envelope recipients is reached for this message
2. The sender and recipient pair is in the configured list of rejected sender-recipient pairs
3. The recipient is non-local and is in the configured list of rejected recipients
4. The recipient is non-local and Relay based upon client authentication is enabled, and AUTH command is not given
5. The recipient is non-local and Relay is disabled.
6. The recipient is non-local and Relay is enabled, and the domain of the recipient does not match any domain in the configured list of allowed relay domains
7. The metric is not updated if the mail is determined to be trusted even if one of the above conditions are met.

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 53–10 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 10 Minutes	After Every Sample	>	500	1000	1	SMTP routing control message envelope rcpt check : %value% rejected messages/minute

User Action

Review the routing control settings to be sure that valid e-mail messages are not being rejected.

If the log level of the SMTP Inbound Server is set to Notification, the server will log ESSM-502 messages when it rejects messages based on the routing control settings.

53.4.5 Message Envelope Sender Check Failure Rate

This metric measures the per minute rate of messages rejected because of any of the following problems with the sender's address:

1. The sender is in the list of rejected senders
2. The sender's domain is in the list of rejected sender domains
3. Comparing authenticated ID with envelope sender is enabled, the AUTH command is invoked, and the sender does not match the Auth Id
4. DNS check on sender domain is enabled, and no record exists for the sender domain
5. Flooding is detected from the host
6. The metric is not updated if the mail is determined to be trusted even if one of the above conditions is met.

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 53–11 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 10 Minutes	After Every Sample	>	500	1000	1	SMTP routing control message envelope sender check: %value% rejected messages/minute

User Action

Review the routing control settings to be sure that valid e-mail messages are not being rejected.

If the log level of the SMTP Inbound Server is set to Notification, the server will log ESSM-502 messages when it rejects messages based on the routing control settings.

53.4.6 Message Header Check Failure Rate

This metric determines the rate per minute of DATA command failures due to the presence of rejected headers in the message. A message header is rejected when one of the following conditions occur:

1. When Comparing Authenticated ID with Sender in the header (based upon the From: and Sender: fields) is enabled and, 1) Auth command is given, and 2) Auth Id does not match the one in the header
2. Comparing envelope sender with header info is enabled, and the envelope sender does not match that of the header.
3. The message has an attachment that matches one in the list of rejected attachments

4. One of the header fields is in the list of rejected header fields
5. The metric does not get updated if the third or fourth conditions are met and the mail is determined to be "trusted".

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 53–12 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 10 Minutes	After Every Sample	>	500	1000	1	SMTP routing control message header check : %value% rejected messages/minute

User Action

Review the routing control settings to be sure that valid email messages are not being rejected.

If the log level of the SMTP Inbound Server is set to Notification, the server will log ESSM-502 messages when it rejects messages based on the routing control settings.

54

E-Mail SMTP Inbound Service

The E-Mail SMTP Inbound Service target allows you to monitor the availability and responsiveness of the Oracle Email SMTP Inbound Service to client requests. This target is monitored by periodically performing client-like protocol operations to determine whether the SMTP Inbound Service is available and responding in a reasonable time. This target must be configured manually to refer to the host name and port number that clients use to connect to the Oracle Email SMTP Inbound Service. The SMTP Inbound Service can be running on a single host or, in large installations, behind a network load balancer or network address translator.

54.1 Response

This metric category captures the response characteristics of the SMTP Inbound Service as seen by a client application.

54.1.1 Connect Time (ms)

This informational metric shows the time taken since the last collection of this data for the SMTP Inbound Server to accept a network connection from a client. It is also indicative of the performance of the Oracle Net Services Listener. This metric is aggregated into the Total Time Metric.

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 54–1 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	>	1000	2000	2	Time taken to connect to SMTP service is %value% (ms)

54.1.2 Status

This indicates whether clients can access e-mail through the SMTP Inbound Service. At least one SMTP Inbound Server and Oracle Net Services Listener must be running in order for the SMTP Inbound Service to be available.

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 54–2 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	=	Not Defined	0	1	Failed to connect to SMTP service

User Action

The SMTP Inbound Service logically consists of the Oracle Email SMTP Inbound Server and an associated Oracle Net Services Listener listening for SMTP Inbound network connection requests. If this service is down, check to see if at least one SMTP Inbound Server process is running. Also check to see if the Oracle Net Services Listener configured for the Oracle Email system is running.

54.1.3 Time To Send E-Mail(ms)

This informational metric shows the time taken since the last collection of this data for the SMTP server to accept a message for delivery or relay. If the SMTP Servers are not running in 'Submit' mode, this also shows the time it takes for a message to reach the recipient. The time required for Recipient lookup against the Oracle directory server and the time required to store a message in the Oracle Collaboration Suite Database is also a factor in the time indicated by this metric. This metric is aggregated into the Total Time Metric.

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 54–3 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	>	2000	5000	2	Time taken to transfer e-mail is %value% (ms)

54.1.4 Total Time (ms)

This metric shows the total time taken since the last collection of this data to complete one simulated SMTP Inbound session. This metric is directly dependent on the performance characteristics of the SMTP Inbound Server target.

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 54–4 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	>	2000	5000	2	Total Time taken to send e-mail is %value% (ms)

User Action

To reduce the total response time, tune the SMTP Inbound Servers after observing their performance levels. You can also identify which operations in a client session are taking excessive amounts of time by looking at the other columns in this metric.

55

E-Mail SMTP Outbound Server

The Oracle Message Transfer Agent uses the SMTP Outbound Server to route mail.

55.1 Messages

This category contains metrics that provide information on the receipt and delivery of e-mail messages.

55.1.1 Distribution List Message Reception Rate (Messages/minute)

This metric represents the number of distribution list messages received per minute by the SMTP Inbound and Outbound Servers.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 10 minutes

55.1.2 Message Transmission Rate (Messages/minute)

This metric represents the number of messages the SMTP Outbound Server transmitted per minute to local or foreign Message Transfer Agents for the purpose of mail delivery.

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 55–1 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 10 Minutes	After Every Sample	>	1000	1500	1	SMTP outbound message transmission rate: %value% messages/minute

User Action

Check the server logs to make sure that your server is not being used as an open relay. If a sender is flooding the server, considering adding this sender to the list of blocked IP addresses. Use esd_logscan.pl to scan the server log files.

55.2 Network

This category contains metrics that provide information about network resources used by an SMTP Outbound Server. Information includes the amount of data the server sent out and information about network connections.

55.2.1 Current SMTP Outbound Connections

This metric represents the number of socket connections to foreign or native Message Transfer Agents that the SMTP Outbound Server currently has opened for the purpose of relaying mail delivery.

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 55–2 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 10 Minutes	After Every Sample	>	200	250	1	The current outbound SMTP connections are %value%

User Action

Check the logs for connections to certain destinations that are slow in responding. Check the destination mailstore SMTP and Oracle Collaboration Suite Databases for any resource constraints. Also, check the logs to make sure that your server is not being used as a open relay.

55.2.2 Data Transmission Rate (Kb/minute)

This metric measures the number of kilobytes transmitted per minute by the SMTP Outbound Server to local or foreign Message Transfer Agents over socket connections for the purpose of mail delivery.

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 55–3 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 10 Minutes	After Every Sample	>	100000	125000	1	SMTP outbound data transmission rate: %value% Kb/minute

User Action

Check the server logs to make sure that your server is not being used as an open relay. If a sender is flooding the server, considering adding this sender to the list of blocked IP addresses. Use esd_logscan.pl to scan the server log files.

55.2.3 SMTP Outbound Connection Rate (Connections/minute)

This metric represents the rate of connections opened per minute by the SMTP Outbound Server to deliver mail to a local or foreign Message Transfer Agent.

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 55–4 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 10 Minutes	After Every Sample	>	2000	2500	1	The SMTP outbound connection rate is %value% connections/minute

User Action

Check the server logs to make sure that your server is not being used as an open relay. If a sender is flooding the server, considering adding this sender to the list of blocked IP addresses. Use esd_logscan.pl to scan the server log files.

55.3 Response

This category contains metrics that provide information about the Up/Down status of the SMTP Outbound Server.

55.3.1 Status

This metric provides information about the Up/Down status of the SMTP Outbound Server and alerts you when the status is Down. The SMTP Outbound Server shows a status of Down when all processes on the host are down.

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 55–5 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 10 Minutes	After Every Sample	>	0	Not Defined	1	No SMTP OUT server running

User Action

You can start the SMTP Outbound Server by selecting the target and clicking the**Start** button on the Email Application home page. If the SMTP Outbound Server does not start, a probable cause is that the server cannot connect to at least one of the Oracle Collaboration Suite Databases or it cannot connect to the system's Oracle directory server.

1. Check that a process on the target host is able to connect to and log into the system's Oracle directory server.
2. Make sure the Oracle Collaboration Suite Database is up and running and the connect string is correctly and accurately registered in the Oracle directory server.
3. Check the log files in the OPMN log file directory for errors. Use esd_logscan.pl to scan the log files.
4. Check the SMTP Outbound Server log files for errors. Use esd_logscan.pl to scan the server log files.

56

E-Mail SMTP Outbound Service

The E-Mail SMTP Outbound Service target allows you to monitor the Oracle Email system at the service level. The SMTP Outbound service is required to deliver messages destined for users outside your Oracle Email system. An SMTP Outbound Service configured for a particular Oracle Collaboration Suite Database collectively represents all SMTP Outbound Servers that are running for that Oracle Collaboration Suite Database.

56.1 Response

This category includes a metric that indicates service availability.

56.1.1 Status

This metric indicates whether at least one SMTP Outbound Server is connected to the Oracle Collaboration Suite Database with which the SMTP Outbound Service is configured.

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 56–1 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	No SMTP OUT service running

User Action

If the status of this service is "Down", check if at least one SMTP Outbound Server process is running. If required, you can start this service by starting at least one SMTP Outbound Server.

57

E-Mail Virus Scrubber

The E-Mail Virus Scrubber target is a background service that periodically selects and scans high-risk messages for virus intrusion with the presence of a supported third-party virus scanning engine. The selection criteria, also known as prescan filters, can be configured by the administrator. Provided for this target are metrics and gauges used to determine the availability, progress, and health of the Virus Scrubber services.

57.1 Messages

The Messages category contains the metrics that provide information about the progress and status of the virus scanning task.

57.1.1 Infected Message Discovery Rate (Infections Found/minute)

This metric measures the number of messages each minute that have been identified by the supported third-party scan engine to be virus infected. This is an informational metric only.

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 57–1 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 60 Minutes	After Every Sample	>	1	10	1	Virus infected messages found: %value%

57.1.2 Infected Message Repair Rate (Repairs/minute)

This metric measures the number of infected messages each minute that have been identified, repaired, and restored to the original user's folders. This is an informational metric only.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 60 minutes

57.1.3 Message Pre-Scan Rate (Messages/minute)

This metric measures the number of messages selected each minute by the Virus Scrubber Server for virus scanning. This is an informational metric only.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 60 minutes

57.1.4 Message Scan Rate (Messages/minute)

This metric measures the number of messages submitted and scanned each minute by the supported third-party scan engine. This is an informational metric only.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 60 minutes

57.1.5 Number of Messages Pending Scan

This metric is a gauge displaying the number of messages that have been selected by the Virus Scrubber Service to be scanned for the supported third-party scanning engine. This metric value indicates how many messages have been removed from user folders but are yet to be scanned by the Virus Scrubber. A small and steady value is desirable at all times. A large value or a continuously growing value means that virus scanning by the supported third-party scan engine is not fast enough to keep up with the rate of messages being selected by the Virus Scrubber Server using the prescan filter. The larger the value gets, the longer that e-mail users will experience messages missing from their folders.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
All Versions	Every 60 minutes

User Action

When the metric value increases significantly and is not decreasing fast enough, perform the following:

1. Check whether the third-party scan engine is configured correctly and efficiently and make sure the engine is working well. Consult your third-party scan engine vendor documentation for more information.

2. Consider increasing the Virus Scrubber Service parameter "Concurrency Level" moderately to increase the scan rate. Refresh the server when any parameter value is changed.
3. Consider choosing the option "Stepwise prescan" in the Virus Scrubber Server parameter settings. Refresh the server when any parameter value is changed.

57.2 Response

The Response category contains metrics that provide information about the Up/Down status of the Virus Scrubber service.

57.2.1 Status

The Status metric provides information about the Up/Down status of the Virus Scrubber service. The Virus Scrubber service shows a status of Down when all configured instances for this service are down. By default, the service is not started.

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 57–2 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	E-Mail Virus Scrubber not running

User Action

A response status failure means the Virus Scrubber Server is not running. A server that is not running will not be able to perform virus scanning on existing e-mail messages. You can start the Virus Scrubber Service by selecting the Virus Scrubber Service target and clicking on the **Start** button on the Email Application home page. To investigate why the service is down, check for alerts that may have been generated by the Virus Scrubber service, specific instances of the Virus Scrubber ervice, and the Oracle Email application that this Virus Scrubber Service is a member of. Also, perform the following checks:

1. Check the OPMN log files
2. Log file content for any errors. Correct any error condition that might have occurred.
3. Restart the service.

58

Mail Housekeeper

The Mail Housekeeper Service monitors the availability, performance, and usage of the Mail housekeeping functionality provided by the underlying Mail system.

58.1 Messages

The Messages category contains metrics regarding the rate at which the Housekeeper processes are working.

58.1.1 Messages Pending Pruning

This metric indicates the number of messages that are yet to be pruned. The value is the sum of all the messages that are not yet pruned for the Housekeeper Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

58.1.2 Messages Pruned

This metric indicates the number of messages that have been pruned. The value is the sum of all the messages pruned for the Housekeeper Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

58.2 Response

The Mail Housekeeper Response category checks and displays whether or not the Mail Housekeeper Server processes are running within this Oracle Home.

58.2.1 Status

This metric indicates whether or not the Mail Housekeeper Service is available. Its status is the status of all Housekeeper Redundancy Groups and other dependent targets. Specifically, all the Housekeeper Redundancy Groups and dependent targets must be available for this Mail Housekeeper Service to be available.

User Action

If the Status of the Mail Housekeeper Service is down, then check the results obtained by Root Cause Analysis on the Mail Housekeeper Service Home Page.

59

Mail Housekeeper Redundancy Group

The Mail Housekeeper Redundancy Group target is a grouping of Housekeeper agent monitored targets that have identical configuration, characteristics, and functionality. While a single Housekeeper server instance is vulnerable to the failure of its host or system, a redundant group of Housekeepers continues to function despite the loss of a Housekeeper server instance, hiding any such failure from clients, and allowing other Housekeeper server instances in the group to service the requests.

59.1 Messages

The Messages category contains metrics regarding the rate at which the processes of Housekeeper agent monitored targets are working.

59.1.1 Messages Pending Pruning

This metric indicates the number of messages that are yet to be pruned. The value is the sum of all the messages that are not yet pruned for the Housekeeper agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

59.1.2 Messages Pruned

This metric indicates the number of messages that have been pruned. The value is the sum of all the messages pruned for the Housekeeper agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

59.2 Response

The Response category checks and displays whether or not the processes of Housekeeper agent monitored targets are running within this Oracle Home.

59.2.1 Status

This metric indicates whether or not the Housekeeper agent monitored target is available. The status is "up" as long as at least one of the Housekeeper agent monitored targets is available.

User Action

If the Status of Mail Housekeeper Redundancy Group is down, then check the status of the individual Housekeeper agent monitored targets to identify which particular one is down.

60

Mail IMAP Redundancy Group

The Mail IMAP Redundancy Group target is a grouping of IMAP agent monitored targets that have identical configuration, characteristics, and functionality. While a single IMAP server instance is vulnerable to the failure of its host or system, a redundant group of IMAP servers continues to function despite the loss of an IMAP server instance, hiding any such failure from clients, and allowing other IMAP server instances in the group to service the requests.

60.1 Bytes Transferred

The Bytes Transferred category provides information about the data transferred between IMAP Server and IMAP Clients.

60.1.1 Bytes Received By Server

This metric measures the amount of data received by the IMAP Server from the IMAP Clients. The value is the sum of all the data received by the IMAP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

60.1.2 Bytes Sent By Server

This metric measures the amount of data sent to IMAP clients by the IMAP Server. This value is the sum of all the data sent by the IMAP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

60.2 Client Connections

The Client Connections category provides information about the client connections on the IMAP Server.

60.2.1 Total Client Connections

This metric shows the total number of client connections open on the IMAP Server. The value is the sum of all open connections for IMAP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

60.3 Fetch Details

The Fetch Details category charts the rate of FETCH commands requested by all clients of IMAP Server instances on this target over the collection period. An IMAP client will use the FETCH command to get most types of message data from an Oracle Collaboration Suite Database, including message identifiers, header information, messages, and message body parts.

60.3.1 Number of Messages Fetched

This informational metric represents the rate of FETCH commands occurring over a period of time. This rate should vary proportionally to the number and type of mail clients concurrently connected. Changes in this value can be caused by a "rogue" client or by users changing from one type of mail client to another. The FETCH commands rate indicates the usage patterns and resource requirements of the mail system. This rate is calculated by considering the sum of all the fetch count values of all IMAP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

60.4 Login Details

The Login Details category provides information about the time taken by the IMAP client to login to the IMAP server.

60.4.1 Login Average Time

This metric shows the average time taken for a connected client to login to the IMAP Server. It is also indicative of the Oracle Internet Directory response time because clients are authenticated against the Oracle directory server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

60.5 NOOP Details

The NOOP Details category provides information about the operations performed using NOOP commands.

60.5.1 NOOP Count

This metric shows the number of times the IMAP client connected and received feedback from the IMAP Server by using the NOOP command. The value is the sum of all NOOP counts of all IMAP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

60.6 Response

The Response category captures the response characteristics of the IMAP agent monitored target as seen by a client application.

60.6.1 Status

This metric indicates whether or not clients are able to access Mail through the IMAP Server. Its availability depends upon the status of all IMAP agent monitored targets. The status is "up" as long as at least one of the IMAP agent monitored targets is up.

User Action

If the Status of Mail IMAP Redundancy Group is down, then check the status of the individual IMAP agent monitored targets to identify which particular one is down.

60.7 Security

The Security category provides information about security related activities.

60.7.1 Refused Flood Connections

This metric shows the connections refused by the IMAP Server. The value is the sum of all the connections refused by the IMAP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

61

Mail IMAP Service

The Mail IMAP Service monitors the availability, performance, and usage of the IMAP functionality provided by the underlying Mail system.

61.1 Bytes Transferred

The Bytes Transferred category provides information about the data transferred between IMAP Server and IMAP Clients.

> **Note:** For target Version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 61–1 Bytes Transferred Metrics

Metric	Description
Bytes Received By Server	Measures the amount of data received by the IMAP Server from the IMAP Clients. It includes data related to normal IMAP commands and data due to messages appended back to the server, typically to the "Sent" or "Sent Items" folder. This value is the sum of all the data received by the IMAP Redundancy Groups.
Bytes Sent By Server	Measures the amount of data sent to IMAP clients by the IMAP Server. The data includes mail and IMAP responses. This value is the sum of all the data sent by the IMAP Redundancy Groups.

61.2 Client Connections

The Client Connections category provides information about the client connections on the IMAP Server.

61.2.1 Total Client Connections

This metric shows the total number of client connections open on the IMAP Server. The value is the sum of all open connections for IMAP Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

61.3 Fetch Details

The Fetch Details category charts the rate of FETCH commands requested by all clients of IMAP Server instances on this target over the collection period. An IMAP client will use the FETCH command to get most types of message data from an Oracle Collaboration Suite Database, including message identifiers, header information, messages, and message body parts.

61.3.1 Fetch Count

This informational metric represents the rate of FETCH commands occurring over a period of time. This rate should vary proportionally to the number and type of mail clients concurrently connected. Changes in this value can be caused by a "rogue" client or by users changing from one type of mail client to another. The FETCH commands rate indicates the usage patterns and resource requirements of the mail system. This rate is the sum of all the fetch count values of all IMAP Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

61.4 IMAP Response

The IMAP Response category captures the response characteristics of the Oracle Mail IMAP service as seen by a client application.

Note: For target Version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 61–2 IMAP Response Metrics

Metric	Description
Connect Time (ms)	Time taken for the IMAP server to accept a network connection from a client. It also reflects the performance of the Oracle Net Services Listener. The connection time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total connection time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
IMAP Timing (ms)	Total time taken for one simulated IMAP session. This metric is directly dependent on the performance characteristics of the IMAP Server target. The timing is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

Table 61–2 (Cont.) IMAP Response Metrics

Metric	Description
Login Time (ms)	Time taken for a connected client to login to the IMAP Server. It is also indicative of the Oracle Internet Directory response time because clients are authenticated against the Oracle directory server. The login time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total login time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
Status	Indicates whether or not clients are able to access Mail through the IMAP Service. The availability depends upon the status determined by the Beacon monitoring this service. If the Status of Mail IMAP Service is down, then check the results obtained by Root Cause Analysis on the Mail IMAP Service Home Page.
Status Message	Describes the status. If the Mail IMAP Service is down, this metric shows why the service is down. The availability depends upon the status determined by the Beacon monitoring this service.
Time to List Folders (ms)	Time it takes to retrieve a user's folder list from the Oracle Collaboration Suite Database (mailstore) through the IMAP server. The folder list includes the Shared and Public folders that a user has access to. This metric is also indicative of the database and directory performance. The timing is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total connection time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
Time to Read Email (ms)	Time taken to retrieve a message from the Oracle Collaboration Suite Database (mailstore) through the IMAP server. This metric is also indicative of the database performance. The timing is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

61.5 Response

The IMAP Service Response category captures the response characteristics of the Oracle Mail IMAP service as seen by a client application.

61.5.1 Status

This metric indicates whether or not clients are able to access Mails through the IMAP Service. The availability of IMAP Service depends upon the status determined by the Beacon monitoring this service.

User Action

If the Status of Mail IMAP Service is not up, then check the results obtained by Root Cause Analysis on the Mail IMAP Service Home Page.

61.6 Response Time

The Response Time category provides information about the average time taken to login and read the messages from IMAP Server.

61.6.1 Average Login Time

This metric shows the average time taken to login to the IMAP Server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

61.6.2 Average Read Email Time

This metric shows the average time taken to retrieve a message from the Oracle Collaboration Suite Database (mailstore) through the IMAP server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

61.7 Security

The Security category provides information about security related activities.

61.7.1 Refused Flood Connections

This metric shows the connections refused by the IMAP Server. The value is the sum of all the connections refused by the IMAP Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

62

Mail Infrastructure Service

The Mail Infrastructure Service is an aggregate of all Mail administrative services, including Housekeeping Service, List Service, and Virus Scrubber Service.

62.1 Queue Messages

The Queue Messages category provides information about queued messages.

62.1.1 Queued Messages Pending Pruning

This metric indicates the number of messages that are yet to be pruned. The value is the sum of all the messages that are not yet pruned for the Housekeeper Services and Redundancy Group and List Services and Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

62.1.2 Queued Messages Pruned

This metric indicates the number of messages that have been pruned. The value is the sum of all the messages that have been pruned for Housekeeper Services and Redundancy Group and List Services and Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

62.2 Response

The Mail Infrastructure Response category checks and displays whether or not the Mail Infrastructure Service is running.

62.2.1 Status

This metric indicates whether or not the Mail Infrastructure Service is available. Its status is the status of all Housekeeper Services and Redundancy Groups, Virus Scrubber Services and Redundancy Groups, List Services and Redundancy Groups, and other dependent targets. The Mail Infrastructure Service is available only when all these services, redundancy groups, and dependent targets are available.

User Action

If the Status of Mail Infrastructure Service is not up, then check the results obtained by Root Cause Analsis on the Mail Infrastructure Service Home Page.

63

Mail List Server Redundancy Group

The Mail List Server Redundancy Group target is a logical grouping of List Server agent monitored targets that have identical configuration, characteristics, and functionality. While a single List Server instance is vulnerable to the failure of its host or system, a redundant group of List Servers continues to function despite the loss of a List Server instance, hiding any such failure from clients, and allowing other List Server instances in the group to service the requests.

63.1 Queue Messages

The Queued Messages category provides information about queued messages.

63.1.1 Queued Messages Pending Pruning

This metric indicates the number of queued messages that are yet to be pruned. The value is the sum of all the queued messages that are not pruned for the List Server agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

63.1.2 Queued Messages Pruned

This metric indicates the number of queued messages that have been pruned. The value is the sum of all the queued messages pruned for the List Server agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

63.2 Response

The Mail List Response category checks and displays whether or not the List Service agent monitored targets are running.

63.2.1 Status

This metric indicates whether or not the List Server agent monitored target is available. The status is "up" as long as at least one of the List Server agent monitored targets is available.

User Action

If the Status of Mail List Server Redundancy Group is down, then check the status of the individual List Server agent monitored targets to identify which particular one is down.

64

Mail List Service

The Mail List Service monitors the availability, performance, and usage of the Mail List functionality provided by the underlying Mail system.

64.1 Queued Messages

The Queued Messages category provides information about queued messages.

64.1.1 Queued Messages Pending Pruning

This metric indicates the number of queued messages that are yet to be pruned. The value is the sum of all the queued messages that are not yet pruned for the List Server Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

64.1.2 Queued Messages Pruned

This metric indicates the number of queued messages that have been pruned. The value is the sum of all the queued messages pruned for the List Server Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

64.2 Response

The Mail List Response category checks and displays whether or not the Mail List Service is running.

64.2.1 Status

This metric indicates whether or not the Mail List Service is available. Its status is the status of all List Server Redundancy Groups and other dependent targets. Specifically, all the List Server Redundancy Groups and dependent targets must be available for the Mail List Service to be available.

User Action

If the Status of Mail List Service is not up, then check the results obtained by Root Cause Analysis on the Mail List Service Home Page.

65

Mail NNTP Redundancy Group

The Mail NNTP Redundancy Group target is a grouping of NNTP agent monitored targets that have identical configuration, characteristics, and functionality. While a single NNTP server instance is vulnerable to the failure of its host or system, a redundant group of NNTP servers continues to function despite the loss of an NNTP server instance, hiding any such failure from clients, and allowing other NNTP server instances in the group to service the requests.

65.1 Messages

The Messages category provides information about messages.

65.1.1 Total Number of Messages Posted

This metric shows the number of messages posted on the NNTP Server. The value is the sum of all the messages posted on the NNTP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

65.1.2 Total Number of Messages Retrieved

This metric shows the number of messages retrieved from the NNTP Server. The value is the sum of all the messages retrieved from the NNTP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

65.2 Network

The Network category provides information about the connections on the NNTP Server.

65.2.1 Total NNTP Connections

This metric shows the total number of connections open on the NNTP Server. The value is the sum of all open connections for NNTP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

65.3 Response

The Response category captures the response characteristics of the NNTP server as seen by a client application.

65.3.1 Status

This metric indicates whether or not clients are able to access emails through the NNTP server. The availability of NNTP server depends upon the status of all the NNTP agent monitored targets. The status is "up" as long as at least one of the agent monitored targets is available.

User Action

If the Status of Mail NNTP Redundancy Group is down, then check the status of the individual NNTP agent monitored targets to identify which particular one is down.

66

Mail NNTP Service

The Mail NNTP Service monitors the availability, performance and usage of the NNTP functionality provided by the underlying Mail system.

66.1 Messages

The Messages category provides information about messages.

66.1.1 Total number of messages posted

This metric shows the number of messages posted on the NNTP Server. The value is the sum of all the messages posted on the NNTP Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

66.1.2 Total number of messages retrieved

This metric shows the number of messages retrieved from the NNTP Server. The value is the sum of all the messages retrieved from the NNTP Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

66.2 Network

The Network category provides information about the connections on the NNTP Server.

66.2.1 Total NNTP Connections

This metric shows the total number of connections open on the NNTP Server. The value is the sum of all open connections for NNTP Redundancy Group.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

66.3 NNTP Response

The NNTP Response category captures the response characteristics of the Oracle Mail NNTP service as seen by a client application.

Note: For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 66–1 NNTP Response Metrics

Metric	Description
[NNTP] Connect Time (ms)	Time taken for the NNTP server to accept a network connection from a client. It is also indicative of the performance of the Oracle Net Services Listener. The connection time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total connection time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[NNTP] Status	Indicates whether or not clients are able to access emails through the NNTP Service. The availability depends upon the status determined by the Beacon monitoring this service. If the Status of Mail NNTP Service is down, then check the results obtained by Root Cause Analysis on the Mail NNTP Service Home Page.
[NNTP] Status Message	Describes the status of the messages. The status depends upon the status determined by the Beacon monitoring this service.
[NNTP] Time to post news article (ms)	Time taken to post a message to a newsgroup through the NNTP server. This metric is also indicative of database performance because news messages are stored in the Oracle Collaboration Suite Database (mailstore). The time taken is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[NNTP] Time to retrieve news article (ms)	Time taken to retrieve a message from the Oracle Collaboration Suite Database (mailstore) through the NNTP server. This metric is also indicative of database performance. The time taken is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

Table 66–1 (Cont.) NNTP Response Metrics

Metric	Description
[NNTP] Total Time (ms)	Total time taken to connect (to the NNTP Server), send, and receive a message. The total time taken is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

66.4 Response

The Response category captures the response characteristics of the Oracle Mail NNTP service as seen by a client application.

66.4.1 Status

This metric indicates whether or not clients are able to access emails through the NNTP Service. The availability of NNTP Service depends upon the status determined by the Beacon monitoring this service.

User Action

If the Status of Mail NNTP Service is down, then check the results obtained by Root Cause Analysis on the Mail NNTP Service Home Page.

66.5 Response Time

The Response Time category provides information about the time taken to connect to the NNTP Server.

66.5.1 Avg. Connect Time (ms)

This metric shows the average time taken to connect to the NNTP Server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

67

Mail POP Redundancy Group

The Mail POP Redundancy Group target is a grouping of POP agent monitored targets that have identical configuration, characteristics, and functionality. While a single POP server instance is vulnerable to the failure of its host or system, a redundant group of POP servers continues to function despite the loss of a POP server instance, hiding any such failure from clients, and allowing other POP server instances in the group to service the requests.

67.1 Network

The Network category provides information about the connected POP clients, and the data transferred between POP clients and POP Server.

67.1.1 Data Received

This metric measures the amount of data received by the POP Server from the POP Clients. The value is the sum of all the data received by POP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

67.1.2 Data Transmitted

This metric measures the amount of data sent to POP clients by the POP Server. This value is the sum of all the data sent by the POP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

67.1.3 Network Clients

This metric shows the total number of client connections open on the POP Server. The value is the sum of all open connections for POP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

67.2 Response

The Response category captures the response characteristics of the POP agent monitored target as seen by a client application.

67.2.1 Status

This metric indicates whether or not clients are able to access Mails through the POP Server. Its availability depends upon the status of all POP agent monitored targets. The status is "up" as long as at least one of the POP agent monitored targets is up.

User Action

If the Status of Mail POP Redundancy Group is down, then check the status of the individual POP agent monitored targets to identify which particular one is down.

67.3 Security

The Security category provides information about security related activities.

67.3.1 Refused Flood Connections

This metric shows the connections refused by the POP Server. The value is the sum of all the connections refused by the POP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

68

Mail POP Service

The Mail POP Service monitors the availability, performance and usage of the POP functionality provided by the underlying Mail system.

68.1 Network

The Network category provides information about the data transferred between POP Server and POP Clients.

> **Note:** For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 68–1 Network Metrics

Metric	Description
Connectted Clients	Total number of client connections open on the POP Server. The value is the sum of all open connections for the POP Redundancy Groups.
Data Received (kb)	Measures the amount of data received by the POP Server from the POP Clients. It includes data related to normal POP commands and data due to messages appended back to the server, typically to the "Sent" or "Sent Items" folder. This value is the sum of all the data received by the POP Redundancy Groups.
Data Transmitted (kb)	Measures the amount of data sent to clients by the POP Server. The data includes mail and POP responses. This value is the sum of all the data sent by the POP Redundancy Groups.

68.2 POP Response

The POP Response category captures the response characteristics of the Oracle Mail POP service as seen by a client application.

> **Note:** For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 68–2 POP Response Metrics

Metric	Description
[POP] Connect Time (ms)	Shows the time taken for the POP server to accept a network connection from a client. It also reflects the performance of the Oracle Net Services Listener. The connection time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total connection time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[POP] Login Time (ms)	Shows the time taken for a connected client to log into the POP Server. It is also indicative of the Oracle Internet Directory response time because clients are authenticated against the Oracle directory server. The login time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the login time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[POP] Status	Indicates whether or not clients are able to access emails through the POP Service. The availability depends upon the status determined by the Beacon monitoring this service. If the Status of Mail POP Service is down, then check the results obtained by Root Cause Analysis on the Mail POP Service Home Page.
[POP] Status Message	Describes the status. If the Mail POP Service is down, this metric shows why the service is down. The status depends upon the value determined by the Beacon monitoring this service.
[POP] Time to Read Email (ms)	Shows the time taken to retrieve a message from the Oracle Collaboration Suite Database (mailstore) through the POP server. This metric is also indicative of the database performance. The timing is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[POP] Timing (ms)	Shows the total time taken for one simulated POP session. This metric is directly dependent on the performance characteristics of the POP Server target. The timing is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

68.3 Response

The Status category captures the response characteristics of the Oracle Email POP service as seen by a client application.

68.3.1 Status

This metric indicates whether or not clients are able to access email through the POP Service. The availability of POP Service depends upon the status determined by the Beacon monitoring this service.

User Action

If the Status of Mail POP Service is not up, then check the results obtained by Root Cause Analysis on the Mail POP Service Home Page.

68.4 Response Time

The Response Time category provides information about the average time taken to connect, login, and read the messages from POP Server.

Note: For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 68–3 Response Time Metrics

Metric	Description
Avg. Connect Time (ms)	Average time taken for the POP server to accept a network connection from a client. This metric also reflects the performance of the Oracle Net Services Listener.
Avg. Login Time (ms)	Average time taken by a connected client to log into the POP Server. This metric also reflects the Oracle directory server response time, because clients are authenticated against the Oracle directory server.
Avg. Read Email Time (ms)	Average time taken to retrieve a message from the Oracle Collaboration Suite Database (mailstore) through the POP server. This metric also reflects database performance.

68.5 Security

The Security category provides information about security related activities.

68.5.1 Refused Flood Connections

This metric shows the connections refused by the POP Server. The value is the sum of all the connections refused by the POP Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

69

Mail Service

The Mail Service is an aggregate of all Mail services, including Infrastructure Services and User Access Services. Infrastructure Services include Housekeeping Services, Virus Scrubber Services, and List Services; and User Access Services include IMAP Services, POP Services, SMTP Services, and NNTP Services.

69.1 Network

The Network category provides information about the data transferred between the various mail services i.e. Infrastructure Services and User Access Services.

> **Note:** For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 69–1 Network Metrics

Metric	Description
Total Client Connections (current)	Shows the total number of open connections for User Access Services like IMAP Service, POP Service, SMTP Service, and NNTP Service.
Total Messages Received (current)	Measures the total number of messages received by the mail servers of the User Access Services (i.e. IMAP Service, SMTP Service, and NNTP Service) from their respective mail clients.
Total Messages Sent (current)	Measures the total number of messages transmitted by the mail servers of the User Access Services (i.e. SMTP Service and NNTP Service) from their respective mail clients.

69.2 Queue Messages

The Queue Messages category provides information about queued messages.

69.2.1 Queued messages pending pruning

This metric indicates the number of messages that are yet to be pruned. The value is the sum of all the messages that are not yet pruned for Mail Infrastructure Services like the Housekeeper Service and List Service.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

69.2.2 Queued messages pruned

This metric indicates the number of messages that have been pruned. The value is the sum of all the messages that have been pruned for Mail Infrastructure Services like the Housekeeper Service and the List Service.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

69.3 Resource Usage

The Resource Usage category provides information about resources used.

Note: For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 69–2 Resource Usage Metrics

Metric	Description
Length of List Queue	Number of messages that are in the list server queue. The value is the sum of all messages that are in the queues of all the list servers.
Local Queue Length	Number of messages that are in the local delivery queue. The value is the sum of all messages of all the local delivery queues of the mailstore.
Messages Being Processed	Number of messages which are currently being processed by the various Mail servers, including SMTP server, list server, and NNTP server. The value is the sum of all messages being processed by all infrastructure services and user access services.
Relay Queue Length	Number of messages that are in the relay queue. The value is the sum of all messages that are in all the relay queues of the mailstore.
Submit Queue Length	Number of messages that are in the submit queue. The value is the sum of all messages that are in all the submit queues of the mailstore.

69.4 Response

The Response category captures the response characteristics of all the mail services (Infrastructure Services and User Access Services) as seen by a client application.

69.4.1 Status

This metric indicates whether or not all mail services (Infrastructure Services and User Access Services) are available. The status is the status of all Housekeeper Services, Virus Scrubber Services, List Services, IMAP Services, POP Services, NNTP Services, SMTP Services, Send Services, Read Services, and other dependent targets. The status is "up" only when all of these services are available.

User Action

If the Status of the Mail Service is down, then check the results obtained by Root Cause Analysis on the Mail Service Home Page.

69.5 Response Time

The Response Time category provides information about the average time taken to connect, login, read, and send emails utilizing the various Mail User Access services.

Note: For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 69–3 Response Time Metrics

Metric	Description
Avg. Connect Time (ms)	Average time taken by mail servers of the Mail User Access Services to accept network connections from their clients. This value is computed by taking the average of the time taken by SMTP Servers, POP Servers, and NNTP Servers to accept connections from their clients.
Avg. Login Time (ms)	Average time taken by connected clients to log into their respective mail servers. This value is computed by taking the average of the login time of the IMAP Service and POP Service.
Avg. Read Email Time (ms)	Average time taken to retrieve messages from the Oracle Collaboration Suite Database (mailstore) through Mail User Access Services. This value is the average of the time taken for reading emails through the IMAP service and POP service.
Avg. Send Email Time (ms)	Average time taken to transmit messages from the Oracle Collaboration Suite Database (mailstore) through the SMTP Servers.

69.6 Security

The Security category provides information about security-related activity.

69.6.1 Refused Flood Connections

This metric shows the total number of connections refused by IMAP and POP servers.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

70

Mail SMTP Redundancy Group

The Mail SMTP Redundancy Group target is a grouping of SMTP agent monitored targets that have identical configuration, characteristics, and functionality. While a single SMTP server instance is vulnerable to the failure of its host or system, a redundant group of SMTP servers continues to function despite the loss of an SMTP server instance, hiding any such failure from clients, and allowing other SMTP server instances in the group to service the requests.

70.1 Bytes Transferred

The Bytes Transferred category provides information about the data transferred between SMTP Server and SMTP Clients.

70.1.1 Bytes Transmitted

This metric measures the amount of data sent to clients by the SMTP Server. This value is the sum of all the data sent by the SMTP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

70.2 Client Connections

The Client Connections category provides information about the client connections on the SMTP Server.

70.2.1 Current Client Connections

This metric shows the number of client connections currently open on the SMTP Server. The value is the sum of all currently open connections for SMTP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

70.3 Messages

The Messages category provides information about the messages sent and received by the SMTP Server.

70.3.1 Total Number of Messages Received

This metric measures the number of messages received by the SMTP Server from the SMTP Clients. This value is the sum of all the messages received by the SMTP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

70.3.2 Total Number of Messages Transmitted

This metric measures the number of messages sent to SMTP clients by the SMTP Server. This value is the sum of all the data sent by the SMTP agent monitored targets.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

70.4 Response

The Response category captures the response characteristics of the SMTP server as seen by a client application.

70.4.1 Status

This metric indicates whether or not the clients can access emails through the SMTP Service. The availability of SMTP Service depends upon the status of all SMTP agent monitored targets. The status is "up" as long as at least one of the agent monitored targets is available.

User Action

If the Status of Mail SMTP Redundancy Group is down, then check the status of the individual SMTP agent monitored targets to identify which particular one is down.

71

Mail SMTP Service

The Mail SMTP Service monitors the availability, performance and usage of the SMTP functionality provided by the underlying Mail system.

71.1 Bytes Transferred

The Bytes Transferred category provides information about the data transferred between SMTP Server and SMTP Clients.

71.1.1 Bytes Transmitted

This metric measures the amount of data sent to clients by the SMTP Server. The data includes mail and SMTP responses. This value is the sum of all the data sent by the SMTP Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

71.2 Client Connections

The Client Connections category provides information about the client connections on the SMTP Server.

71.2.1 Current Client Connections

This metric shows the number of client connections currently open on the SMTP Server. The value is the sum of all currently open connections for SMTP Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

71.3 Messages

The Messages category provides information about the messages sent and received by the SMTP Server.

71.3.1 Total number of messages received

This metric measures the number of messages received by the SMTP Server from the SMTP Clients. It includes data related to normal SMTP commands and data due to messages appended back to the server, typically to the "Sent" or "Sent Items" folder. This value is the sum of all the messages received by the SMTP Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

71.3.2 Total number of messages transmitted

This metric measures the number of messages sent to SMTP clients by the SMTP Server. The data includes mail and SMTP responses. This value is the sum of all the data sent by the SMTP Redundancy Groups.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

71.4 Response

The Response category captures the response characteristics of the Mail SMTP Service as seen by a client application.

71.4.1 Status

This metric indicates whether or not the clients can access emails through the SMTP Service. The availability of SMTP Service depends upon the status determined by the Beacon monitoring this service.

User Action

If the Status of Mail SMTP Service is down, then check the results obtained by Root Cause Analysis on the Mail SMTP Service Home Page.

71.5 Response Time

The Response Time category provides information about the average time taken to connect and send emails from the SMTP Server.

71.5.1 Avg. Connect Time (ms)

This metric shows the average time taken for the SMTP server to accept a network connection from a client. This metric also indicates the performance of the Oracle Net Services Listener. The average connection time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the average connection time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

71.5.2 Avg. Send Email Time (ms)

This metric shows the average time taken to transmit an email from the Oracle Collaboration Suite Database (mailstore) through the SMTP server. This metric also indicates database performance. The average time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the average email transmission time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

71.6 SMTP Response

The SMTP Response category captures the response characteristics of the Oracle Mail SMTP service as seen by a client application.

Note: For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 71–1 SMTP Response Metrics

Metric	Description
[SMTP] Connect Time (ms)	Shows the time taken for the SMTP server to accept a network connection from a client. It is also indicative of the performance of the Oracle Net Services Listener. The connection time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total connection time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

Table 71–1 (Cont.) SMTP Response Metrics

Metric	Description
[SMTP] Status	Indicates whether or not clients are able to access emails through the SMTP Service. The availability depends upon the status determined by the Beacon monitoring this service.
[SMTP] Status Message	Describes the status. If the Mail SMTP Service is down, this metric shows why the service is down. Its status depends upon the value determined by the Beacon monitoring this service.
[SMTP] Time to Send Email (ms)	Shows the time taken since the last collection of this data for the SMTP server to accept a message for delivery or relay. If the SMTP Servers are not running in 'Submit' mode, this also shows the time it takes for a message to reach the recipient. The time required for Recipient lookup against the Oracle directory server and the time required to store a message in the Oracle Collaboration Suite Database are also factors in the time indicated by this metric. This time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.
[SMTP] Total Time (ms)	Shows the total time taken since the last collection of this data to complete one simulated SMTP session. This metric is directly dependent on the performance characteristics of the SMTP Server target. The total time is the value determined by the Beacon(s) monitoring this service. The Beacon(s) is(are) responsible for executing the perl script to ping the host and determine the total time. If multiple Beacons are monitoring this service, the value displayed is the average of all the values determined by all the Beacons.

72

Mail User Access Service

The Mail User Access Service is an aggregate of all Mail services accessed by general users, including IMAP Service, NNTP Service, SMTP Service, POP Service, Read Web Application and Send Web Application.

72.1 Network

The Network category provides information about the data transferred between the clients and the various Mail User Access Services (i.e. IMAP Service, POP Service, SMTP Service, NNTP Service, Read Web Application and Send Web Application).

> **Note:** For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 72–1 Network Metrics

Metric	Description
Total Client Connections (current)	Shows the total number of client connections on the various Mail User Access Services. This value is the sum of all open connections for IMAP Service, POP Service, SMTP Service, and NNTP Service.
Total Messages Received (current)	Measures the number of messages received by all the mail servers from all their respective mail clients. This value is the sum of all the messages received by IMAP Service, NNTP Service, and SMTP Service.
Total Messages Sent (current)	Measures the number of messages sent to various mail clients by their respective mail servers. This value is the sum of all the messages sent by SMTP Service and NNTP Service.

72.2 Resource Usage

The Resource Usage category provides information about the resources used.

> **Note:** For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 72–2 Resource Usage Metrics

Metric	Description
Length of List Queue	Number of messages that are in the list server queue. The messages in this queue are sent to mailing lists and have to be processed by the list server.
Local Queue Length	Number of messages that are in the local delivery queue. The messages in this queue have to be processed by SMTP or list server.
Messages Being Processed	Number of messages that are currently being processed by the various Oracle Mail servers, including SMTP, list server, and NNTP.
Relay Queue Length	Number of messages that are in the relay queue. The messages in this queue have to be processed by the SMTP or list server.
Submit Queue Length	Number of messages that are in the submit queue. The messages in this queue have to be processed by the SMTP server.

72.3 Response

The Response category captures the response characteristics of all the Mail User Access services (i.e. IMAP Service, NNTP Service, POP Service, SMTP Service, Read Web Application and Send Web Application) as seen by a client application.

72.3.1 Status

This metric shows whether or not the clients are able to access emails through the mail services. Its status depends upon the status of all mail services (i.e. IMAP Service, NNTP Service, POP Service, SMTP Service, Read Service, and Send Service). The status is "up" only when all of these services are available.

72.4 Response Time

The Response Time category provides information about the average time taken to connect, login, read, and send emails from the various Mail User Access Services.

Note: For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 72–3 Response Time Metrics

Metric	Description
Avg. Connect Time (ms)	Average time taken by the mail servers to accept network connections from their clients. This value is computed by taking the average of the time taken by SMTP Servers, IMAP Servers, POP Servers, and NNTP Servers to accept connections from their clients.
Avg. Login Time (ms)	Average time taken by connected clients to log into their respective mail servers. This value is computed by taking the average of the login time of IMAP Service and POP Service.

Table 72–3 (Cont.) Response Time Metrics

Metric	Description
Avg. Read Email Time (ms)	Average time taken to retrieve messages from the Oracle Collaboration Suite Database (mailstore) through various mail servers. This value is the average of the time taken for reading emails through IMAP Servers and POP Servers.
Avg. Send Email Time (ms)	Average time taken to transmit messages from the Oracle Collaboration Suite Database (mailstore) through various mail servers. This value is the average of the time taken for sending emails through the SMTP Servers.

72.5 Security

The Security category provides information about security related activities.

72.5.1 Refused Flood Connections

This metric shows the total number of connections refused by the mail servers. The value is the sum of all the connections refused by IMAP Server and POP Server.

Metric Summary

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

Target Version	Evaluation and Collection Frequency
Version 1.0	Every 15 minutes

73

Mail Virus Scrubber Redundancy Group

The Mail Virus Scrubber Redundancy Group target is a logical grouping of Virus Scrubber agent monitored targets that have identical configuration, characteristics, and functionality. While a single Virus Scrubber server instance is vulnerable to the failure of its host or system, a redundant group of Virus Scrubbers continues to function despite the loss of a Virus Scrubber server instance, hiding any such failure from clients, and allowing other Virus Scrubber server instances in the group to service the requests.

73.1 Messages

The Messages category provides information about messages.

Note: For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 73–1 Messages Metrics

Metric	Description
Number of Infections Found	Number of messages that are infected with viruses. The number of infections is the sum of all the infected messages of Virus Scrubber agent monitored targets.
Number of Infections Repaired	Number of infected messages that have been repaired. The number of infections repaired is the sum of all the infected messages of Virus Scrubber agent monitored targets that have been repaired.
Number of Messages Pending Scan	Number of messages that are yet to be scanned for viruses. The value is the sum of all the messages of Virus Scrubber agent monitored targets that are not yet scanned.
Number of Messages Pre-scanned	Number of messages that have been pre-scanned for viruses. The value is the sum of all the messages of Virus Scrubber agent monitored targets that have been pre-scanned for viruses.
Number of Messages Scanned	Number of messages that have been scanned for viruses. The value is the sum of all the messages of Virus Scrubber agent monitored targets that have been scanned for viruses.

73.2 Response

The Response category checks and displays whether or not the Virus Scrubber agent monitored targets are running.

73.2.1 Status

This metric indicates whether or not the Virus Scrubber agent monitored target is available. Its status is "up" as long as at least one of the Virus Scrubber agent monitored targets is available.

User Action

If the Status of Mail Virus Scrubber Redundancy Group is down, then check the status of the individual Virus Scrubber agent monitored targets to identify which particular one is down.

74

Mail Virus Scrubber Service

The Mail Virus Scrubber Service monitors the availability, performance, and usage of the Mail virus scrubbing functionality provided by the underlying Mail system.

74.1 Messages

The Messages category provides information about messages.

Note: For target version 1.0, the collection frequency for each metric is every 15 minutes.

The following table lists the metrics and their descriptions.

Table 74–1 Messages Metrics

Metric	Description
Number of Infections Found	Number of messages that are infected with viruses. The number of infections is the sum of all the infected messages of Virus Scrubber Redundancy Group.
Number of Infections Repaired	Number of infected messages that have been repaired. The number of infections repaired is the sum of all the infected messages of Virus Scrubber Redundancy Group that have been repaired.
Number of Messages Pending Scan	Number of messages that are yet to be scanned for viruses. The value is the sum of all the messages across the Virus Scrubber Redundancy Group that are not yet scanned.
Number of Messages Pre-scanned	Number of messages that have been pre-scanned for viruses. The value is the sum of all the messages of Virus Scrubber Redundancy Group that have been pre-scanned for viruses.
Number of Messages SCanned	Number of messages that have been scanned for viruses. The value is the sum of all the messages of Virus Scrubber Redundancy Group that have been scanned for viruses.

74.2 Response

The Mail Virus Scrubber Response category checks and displays whether or not the Mail Virus Scrubber Service is running.

74.2.1 Status

This metric indicates whether or not the Mail Virus Scrubber Service is available. Its status is the status of all Virus Scrubber Redundancy Groups and other dependent

targets. Specifically, all the Virus Scrubber Redundancy Groups and dependent targets must be available for this Mail Virus Scrubber Service to be available.

User Action

If the Status of Mail Virus Scrubber Service is not up, then check the results obtained by Root Cause Analysis on the Mail List Service Home Page.

75

Oracle Web Access

Enterprise Manager can be used to manage Oracle Collaboration Suite Web Access. Use the All Metrics page to view the metrics that have been collected for a target by the Oracle Management Agent.

75.1 Response

This category contains the metrics used to indicate the status and responsiveness of Web Access.

75.1.1 UpDown Status

Indicates if the application is running. This metric is based on the status of the OC4J_OCSClient container in which the application is deployed.

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 75–1 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 Minute	After Every Sample	=	Not Defined	0	1	%target%, the associated OC4J instance is down

75.2 Web Access Connection Metrics

This category contains the metrics used to capture the use of HTTP sessions between the browser-side and middle tier portions of Web Access.

> **Note:** For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 75–2 Web Access Connections Metrics

Metric	Description
HTTP Sessions - Active Requests	Current number of concurrent requests for an HTTP session.
HTTP Sessions - Average Time (ms)	Average amount of time that HTTP sessions are open.
HTTP Sessions - Completed Requests	Number of HTTP sessions that have been closed.
HTTP Sessions - Cumulative Time (ms)	Cumulative total of all HTTP session durations.
HTTP Sessions - Maximum Concurrent Requests	Maximum number of concurrent requests for an HTTP session.
HTTP Sessions - Maximum Time (ms)	Maximum amount of time that an HTTP session was open.
HTTP Sessions - Minimum Time (ms)	Minimum amount of time that an HTTP session was open.
HTTP Sessions Created	Number of HTTP sessions that have been created.
Total User Logins	Total number of logins to Web Access.

75.3 Web Access Directory Cache Metrics

This category contains the metrics used to measure the performance of the Web Access directory cache. These metrics are only available if directory cache is enabled for Web Access.

Note: For all target versions, the collection frequency for each metric is every 10 minutes.

The following table lists the metrics and their descriptions.

Table 75–3 Web Access Directory Cache Metrics

Metric	Description
Directory Cache Loading - Active Requests	Current number of concurrent requests to load user information from Oracle Internet Directory into the Web Access directory cache. This is unlikely to be more than 1, since only a single application thread refreshes the directory cache each cycle.
Directory Cache Loading - Average Time (ms)	Average amount of time to load user information from Oracle Internet Directory into the Web Access directory cache.
Directory Cache Loading - Completed Requests	Number of completed requests to load user information from Oracle Internet Directory into the Web Access directory cache. This should increment by 1 every cache refresh cycle.
Directory Cache Loading - Cumulative Time (ms)	Cumulative total time to load user information from Oracle Internet Directory into the Web Access directory cache.
Directory Cache Loading - Maximum Concurrent Requests	Maximum number of concurrent requests to load user information from Oracle Internet Directory into the Web Access directory cache. This is unlikely to be more than 1, since only a single application thread refreshes the directory cache each cycle.

Table 75–3 (Cont.) Web Access Directory Cache Metrics

Metric	Description
Directory Cache Loading - Maximum Time (ms)	Maximum amount of time to load user information from Oracle Internet Directory into the Web Access directory cache.
Directory Cache Loading - Minimum Time (ms)	Minimum amount of time to load user information from Oracle Internet Directory into the Web Access directory cache.

75.4 Web Access Midtier Operation Metrics

This category contains the metrics used to measure the use and performance of Web Access middle tier operations. Note that this does not measure click-to-render performance experienced by an end-user. The metrics here should not be construed as anything more than an estimation of the responsiveness and health of the middle tier portion of Web Access.

Note: For all target versions, the collection frequency for each metric is every 5 minutes.

The following table lists the metrics and their descriptions.

Table 75–4 Web Access Midtier Operation Metrics

Metric	Description
Get Address Book Headers - Active Requests	Current number of concurrent requests to get Address Book headers.
Get Address Book Headers - Average Time (ms)	Average amount of time to get Address Book headers.
Get Address Book Headers - Completed Requests	Number of completed requests to get Address Book headers.
Get Address Book Headers - Cumulative Time (ms)	Cumulative total time to get Address Book headers.
Get Address Book Headers - Maximum Concurrent Requests	Maximum number of concurrent requests to get Address Book headers.
Get Address Book Headers - Maximum Time (ms)	Maximum amount of time to get Address Book headers.
Get Address Book Headers - Minimum Time (ms)	Minimum amount of time to get Address Book headers.
Get Address Book Unique Identifiers - Active Requests	Current number of concurrent requests to get Address Book unique identifiers.
Get Address Book Unique Identifiers - Average Time (ms)	Average amount of time to get Address Book unique identifiers.
Get Address Book Unique Identifiers - Completed Requests	Number of completed requests to get Address Book unique identifiers.
Get Address Book Unique Identifiers - Cumulative Time (ms)	Cumulative total time to get Address Book unique identifiers.
Get Address Book Unique Identifiers - Maximum Concurrent Requests	Maximum number of concurrent requests to get Address Book unique identifiers.
Get Address Book Unique Identifiers - Maximum Time (ms)	Maximum amount of time to get Address Book unique identifiers.

Table 75–4 (Cont.) Web Access Midtier Operation Metrics

Metric	Description
Get Address Book Unique Identifiers - Minimum Time (ms)	Minimum amount of time to get Address Book unique identifiers.
Get Calendar Meetings by Date Range - Active Requests	Current number of concurrent requests to get Calendar meetings by date range.
Get Calendar Meetings by Date Range - Average Time (ms)	Average amount of time to get Calendar meetings by date range.
Get Calendar Meetings by Date Range - Completed Requests	Number of completed requests to get Calendar meetings by date range.
Get Calendar Meetings by Date Range - Cumulative Time (ms)	Cumulative total time to get Calendar meetings by date range.
Get Calendar Meetings by Date Range - Maximum Concurrent Requests	Maximum number of concurrent requests to get Calendar meetings by date range.
Get Calendar Meetings by Date Range - Maximum Time (ms)	Maximum amount of time to get Calendar meetings by date range.
Get Calendar Meetings by Date Range - Minimum Time (ms)	Minimum amount of time to get Calendar meetings by date range.
Get Mail Folder Unique Identifiers - Active Requests	Current number of concurrent requests to get mail folder unique identifiers.
Get Mail Folder Unique Identifiers - Average Time (ms)	Average amount of time to get mail folder unique identifiers.
Get Mail Folder Unique Identifiers - Completed Requests	Number of completed requests to get mail folder unique identifiers.
Get Mail Folder Unique Identifiers - Cumulative Time (ms)	Cumulative total time to get mail folder unique identifiers.
Get Mail Folder Unique Identifiers - Maximum Concurrent Requests	Maximum number of concurrent requests to get mail folder unique identifiers.
Get Mail Folder Unique Identifiers - Maximum Time (ms)	Maximum amount of time to get mail folder unique identifiers.
Get Mail Folder Unique Identifiers - Minimum Time (ms)	Minimum amount of time to get mail folder unique identifiers.
Get Message Details - Active Requests	Current number of concurrent requests to get message details.
Get Message Details - Average Time (ms)	Average amount of time to get message details.
Get Message Details - Completed Requests	Number of completed requests to get message details.
Get Message Details - Cumulative Time (ms)	Cumulative total time to get message details.
Get Message Details - Maximum Concurrent Requests	Maximum number of concurrent requests to get message details.
Get Message Details - Maximum Time (ms)	Maximum amount of time to get message details.
Get Message Details - Minimum Time (ms)	Minimum amount of time to get message details.
Get Message Headers - Active Requests	Current number of concurrent requests to get message headers.

Table 75–4 (Cont.) Web Access Midtier Operation Metrics

Metric	Description
Get Message Headers - Average Time (ms)	Average amount of time to get message headers.
Get Message Headers - Completed Requests	Number of completed requests to get message headers.
Get Message Headers - Cumulative Time (ms)	Cumulative total time to get message headers.
Get Message Headers - Maximum Concurrent Requests	Maximum number of concurrent requests to get message headers.
Get Message Headers - Maximum Time (ms)	Maximum amount of time to get message headers.
Get Message Headers - Minimum Time (ms)	Minimum amount of time to get message headers.
Get Personal Message Folders - Active Requests	Current number of concurrent requests to get personal message folders.
Get Personal Message Folders - Average Time (ms)	Average amount of time to get personal message folders.
Get Personal Message Folders - Completed Requests	Number of completed requests to get personal message folders.
Get Personal Message Folders - Cumulative Time (ms)	Cumulative total time to get personal message folders.
Get Personal Message Folders - Maximum Concurrent Requests	Maximum number of concurrent requests to get personal message folders.
Get Personal Message Folders - Maximum Time (ms)	Maximum amount of time to get personal message folders.
Get Personal Message Folders - Minimum Time (ms)	Minimum amount of time to get personal message folders.
Get Shared Message Folders - Active Requests	Current number of concurrent requests to get shared message folders.
Get Shared Message Folders - Average Time (ms)	Average amount of time to get shared message folders.
Get Shared Message Folders - Completed Requests	Number of completed requests to get shared message folders.
Get Shared Message Folders - Cumulative Time (ms)	Cumulative total time to get shared message folders.
Get Shared Message Folders - Maximum Concurrent Requests	Maximum number of concurrent requests to get shared message folders.
Get Shared Message Folders - Maximum Time (ms)	Maximum amount of time to get shared message folders.
Get Shared Message Folders - Minimum Time (ms)	Minimum amount of time to get shared message folders.
Search Corporate Directory - Active Requests	Current number of concurrent requests to search the Corporate Directory.
Search Corporate Directory - Average Time (ms)	Average amount of time to search the Corporate Directory.
Search Corporate Directory - Completed Requests	Number of completed searches done in the Corporate Directory.

Table 75–4 (Cont.) Web Access Midtier Operation Metrics

Metric	Description
Search Corporate Directory - Cumulative Time (ms)	Cumulative total time spent searching the Corporate Directory.
Search Corporate Directory - Maximum Concurrent Requests	Maximum number of concurrent requests to search the Corporate Directory.
Search Corporate Directory - Maximum Time (ms)	Maximum amount of time spent searching the Corporate Directory.
Search Corporate Directory - Minimum Time (ms)	Minimum amount of time spent searching the Corporate Directory.
Send Message - Active Requests	Current number of concurrent requests to send a message.
Send Message - Average Time (ms)	Average amount of time to send a message.
Send Message - Completed Requests	Number of completed requests to send messages.
Send Message - Cumulative Time (ms)	Cumulative total time to send messages.
Send Message - Maximum Concurrent Requests	Maximum number of concurrent requests to send a message.
Send Message - Maximum Time (ms)	Maximum amount of time to send a message.
Send Message - Minimum Time (ms)	Minimum amount of time to send a message.

Part III

Oracle Voice Mail and FAX

Part III provides the metrics related to the Oracle Collaboration Suite Oracle Voice Mail and FAX targets.

Part III contains the following chapters:

- Chapter 101, "Voicemail and Fax Service"
- Chapter 102, "Voicemail and Fax Recording Service"
- Chapter 103, "Voicemail and Fax Retrieval Service"

76

Call Transfer Service

This target represents the Call Transfer Service. The Call Transfer Service transfers calls to the phone number configured as the operator or attendant number. When the voice mail user chooses the menu option to transfer the call to an attendant, the call is handed off to the Call Transfer Service which looks up attendants number in the Oracle Internet Directory. It starts with the user profile, and if none is configured at the user level, it looks up the users parent hierarchy. The call is transferred to the attendant through the PBX. Who the user is varies depending on from where the call is handed off. If the Retrieval Service hands off the call, then the user is the authenticated voice mail user who is logged into their mail box. If the Recording Service hands off the call, then the user is the voice mail user for whom the caller recorded a message or for whom the caller intended to record a message.

76.1 Call Transfer Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Call Transfer Service instance. It provides a snapshot of how the Call Transfer Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Call Transfer Service instance.

76.1.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Call Transfer Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 76–1 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	>	70	75	2	CPU utilization of Call Transfer Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Call Transfer Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Call Transfer Service instance, the Voicemail and Fax Application that this Call Transfer Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

76.1.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

76.1.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Call Transfer Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 76–2 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	>	80	90	2	Memory utilization of Call Transfer Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Call Transfer Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Call Transfer Service instance, the Voicemail and Fax Application that this Call Transfer Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

76.1.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Call Transfer Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Call Transfer Service instance.

76.1.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

76.1.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

76.1.7 Status

This metric provides information about the Up/Down status of the Call Transfer Service instance and alerts you when the Call Transfer Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 76–3 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	=	Not Defined	0	1	Call Transfer Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Call Transfer Service by selecting the Call Transfer Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Call Transfer Service instance, the Voicemail and Fax Application that this Call Transfer Service instance is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

76.1.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

76.2 Call Transfer Service Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Call Transfer Service. It provides a snapshot of how the Call Transfer Service instances are performing. If a particular metric is empty, it is likely that an Call Transfer Service instance is down and unavailable. Check the Up/Down status metric for all the Call Transfer Service instances.

76.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 76–4 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	>	70	75	2	CPU utilization of Call Transfer Service, %target%, is %value%%%

User Action

You can use this metric to determine if the Call Transfer Service is using the most CPU on your system, thereby leading to high end-user response times. If the Call Transfer Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Call Transfer Service, the Voicemail and Fax Application that this Call Transfer Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

76.2.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 76–5 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	>	80	90	2	Memory utilization of Call Transfer Service, %target%, is %value%%%

User Action

You can use this metric to determine if the Call Transfer Service is using the most memory on your system and leading to high end-user response times. If the Call Transfer Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Call Transfer Service instances, the Voicemail and Fax Application that this Call Transfer Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

76.2.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Call Transfer Service.

76.2.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

76.2.5 Status

This metric provides information about the Up/Down status of the Call Transfer Service. The Call Transfer Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Call Transfer Service by selecting the Call Transfer Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Call Transfer Service, specific instances of the Call Transfer Service, the Voicemail and Fax Application that this Call Transfer Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

76.2.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

76.2.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

76.3 Call Transfer Service Response

This category contains metrics that provide information about the Up/Down status of the Call Transfer Service.

76.3.1 Status

This metric provides information about the Up/Down status of the Call Transfer Service and alerts you when the Call Transfer Service is down. The Call Transfer Service shows a status of Down when all configured instances for this service are down. By default, a critical threshold value is set for this metric. Alerts are 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 76–6 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	=	Not Defined	0	1	Call Transfer Service, %target%, is down

User Action

You can restart the Call Transfer Service by selecting the Call Transfer Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Call Transfer Service, specific instances of the Call Transfer Service, the Voicemail and Fax Application that this Call Transfer Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

77

Fax Receiving Service

This target represents the Fax Receiving Service. When a forwarded call is passed to the Recording Service and it detects a fax tone, it passes the call to the Fax Receiving Service which looks up the callees information in the Oracle Internet Directory. If the Fax Receiving Service determines that the callee is a valid user with the fax access feature enabled, it receives the fax and sends it to the callees Inbox in the Collaboration Suite Database.

77.1 Fax Receiving Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Fax Receiving Service instance. It provides a snapshot of how the Fax Receiving Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Fax Receiving Service instance.

77.1.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Fax Receiving Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 77–1 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	>	70	75	2	CPU utilization of Fax Receiving Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Fax Receiving Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Fax Receiving Service instance, the Voicemail and Fax Application that this Fax Receiving Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

77.1.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

77.1.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Fax Receiving Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 77–2 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	>	80	90	2	Memory utilization of Fax Receiving Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Fax Receiving Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Fax Receiving Service instance, the Voicemail and Fax Application that this Fax Receiving Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

77.1.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Fax Receiving Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Fax Receiving Service instance.

77.1.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

77.1.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

77.1.7 Status

This metric provides information about the Up/Down status of the Fax Receiving Service instance and alerts you when the Fax Receiving Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 77–3 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	=	Not Defined	0	1	Fax Receiving Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Fax Receiving Service by selecting the Fax Receiving Service target and clicking on the Restart button on the Oracle Voicemail and Fax Home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Fax Receiving Service instance, the Voicemail and Fax Application that this Fax Receiving Service instance is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

77.1.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

77.2 Fax Receiving Service Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Fax Receiving Service. It provides a snapshot of how the Fax Receiving Service instances are performing. If a particular metric is empty, it is likely that an Fax Receiving Service instance is down and unavailable. Check the Up/Down status metric for all the Fax Receiving Service instances.

77.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 77–4 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	>	70	75	2	CPU utilization of Fax Receiving Service, %target%, is %value%%%

User Action

You can use this metric to determine if the Fax Receiving Service is using the most CPU on your system, thereby leading to high end-user response times. If the Fax Receiving Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Fax Receiving Service, the Voicemail and Fax Application that this Fax Receiving Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

77.2.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 77–5 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	>	80	90	2	Memory utilization of Fax Receiving Service, %target%, is %value%%%

User Action

You can use this metric to determine if the Fax Receiving Service is using the most memory on your system and leading to high end-user response times. If the Fax Receiving Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Fax Receiving Service instances, the Voicemail and Fax Application that this Fax Receiving Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

77.2.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Fax Receiving Service.

77.2.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

77.2.5 Status

This metric provides information about the Up/Down status of the Fax Receiving Service. The Fax Receiving Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Fax Receiving Service by selecting the Fax Receiving Service target and clicking on the Restart button on the Oracle Voicemail and Fax Home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Fax Receiving Service, specific instances of the Fax Receiving Service, the Voicemail and Fax Application that this Fax Receiving Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

77.2.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

77.2.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

77.3 Fax Receiving Service Response

This category contains metrics that provide information about the Up/Down status of the Fax Receiving Service.

77.3.1 Status

This metric provides information about the Up/Down status of the Fax Receiving Service and alerts you when the Fax Receiving Service is down. The Fax Receiving Service shows a status of Down when all configured instances for this service are

down. By default, a critical threshold value is set for this metric. Alerts are 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 77–6 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	=	Not Defined	0	1	Fax Receiving Service, %target%, is down

User Action

You can restart the Fax Receiving Service by selecting the Fax Receiving Service target and clicking on the Restart button on the Oracle Voicemail and Fax Home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Fax Receiving Service, specific instances of the Fax Receiving Service, the Voicemail and Fax Application that this Fax Receiving Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

78

Interactive Voice Response Service

This target represents the IVR (Interactive Voice Response) Service. IVR runs simple call answering programs that administrators can define and customize. The IVR plays messages, transfers calls, searches the user directory, offers simple DTMF menus, and integrates with the Recording Service and Retrieval Service. The IVR Service supports multiple administrator-defined IVR deployments, each of which may specify a behavior for business hours, non-business hours, holidays, and special times that fit none of these categories. When the Routing Service is handed a call, it consults the PBX-Application Clusters call routing map, which contains a mapping of telephone numbers to IVR deployment names. If the call routing map contains a mapping for the originally dialed telephone number, the Routing Service sends the call to the IVR Service. The IVR Service then executes the applicable behavior for the appropriate IVR deployment.

78.1 Interactive Voice Response Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Interactive Voice Response Service instance. It provides a snapshot of how the Interactive Voice Response Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Interactive Voice Response Service instance.

78.1.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Interactive Voice Response Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 78–1 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	>	70	75	2	CPU utilization of Interactive Voice Response Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Interactive Voice Response Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Interactive Voice Response Service instance, the Voicemail and Fax Application that this Interactive Voice Response Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

78.1.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

78.1.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Interactive Voice Response Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 78–2 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	>	80	90	2	Memory utilization of Interactive Voice Response Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Interactive Voice Response Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Interactive Voice Response Service instance, the Voicemail and Fax Application that this Interactive Voice Response Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

78.1.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Interactive Voice Response Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Interactive Voice Response Service instance.

78.1.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

78.1.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

78.1.7 Status

This metric provides information about the Up/Down status of the Interactive Voice Response Service instance and alerts you when the Interactive Voice Response Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 78–3 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	=	Not Defined	0	1	Interactive Voice Response Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Interactive Voice Response Service by selecting the Interactive Voice Response Service target and clicking on the Restart button on the Oracle Voicemail and Fax Home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Interactive Voice Response Service instance,

the Voicemail and Fax Application that this Interactive Voice Response Service instance is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

78.1.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

78.2 Interactive Voice Response Service Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Interactive Voice Response Service. It provides a snapshot of how the Interactive Voice Response Service instances are performing. If a particular metric is empty, it is likely that an Interactive Voice Response Service instance is down and unavailable. Check the Up/Down status metric for all the Interactive Voice Response Service instances.

78.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 78–4 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	>	70	75	2	CPU utilization of Interactive Voice Response Service, %target%, is %value%%%

User Action

You can use this metric to determine if the Interactive Voice Response Service is using the most CPU on your system, thereby leading to high end-user response times. If the Interactive Voice Response Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Interactive Voice Response Service, the

Voicemail and Fax Application that this Interactive Voice Response Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

78.2.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 78–5 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	>	80	90	2	Memory utilization of Interactive Voice Response Service, %target%, is %value%%

User Action

You can use this metric to determine if the Interactive Voice Response Service is using the most memory on your system and leading to high end-user response times. If the Interactive Voice Response Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Interactive Voice Response Service instances, the Voicemail and Fax Application that this Interactive Voice Response Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

78.2.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Interactive Voice Response Service.

78.2.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

78.2.5 Status

This metric provides information about the Up/Down status of the Interactive Voice Response Service. The Interactive Voice Response Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Interactive Voice Response Service by selecting the Interactive Voice Response Service target and clicking on the Restart button on the Oracle Voicemail and Fax Home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Interactive Voice Response Service, specific instances of the Interactive Voice Response Service, the Voicemail and Fax Application that this Interactive Voice Response Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

78.2.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

78.2.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

78.3 Interactive Voice Response Service Response

This category contains metrics that provide information about the Up/Down status of the Interactive Voice Response Service.

78.3.1 Status

This metric provides information about the Up/Down status of the Interactive Voice Response Service and alerts you when the Interactive Voice Response Service is down. The Interactive Voice Response Service shows a status of Down when all configured instances for this service are down. By default, a critical threshold value is set for this metric. Alerts are 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 78–6 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	=	Not Defined	0	1	Interactive Voice Response Service, %target%, is down

User Action

You can restart the Interactive Voice Response Service by selecting the Interactive Voice Response Service target and clicking on the Restart button on the Oracle Voicemail and Fax Home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Interactive Voice Response Service, specific instances of the Interactive Voice Response Service, the Voicemail and Fax Application that this Interactive Voice Response Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

79

Message Delivery Monitor Service

This target represents the Message Delivery Monitor Service. The Message Delivery Monitor Service measures the time it takes to send a message to the Collaboration Suite Database. It sends test messages to a test account on each Collaboration Suite Database, and reports the time it takes for the test message to arrive in the Inbox of the target Collaboration Suite Database.

79.1 Message Delivery Monitor Instance Performance Metrics

This category includes a set of metrics that provides information about the message delivery times of this service instance in the Message Delivery Monitor Service.

Once a caller confirms that he or she has completed recording a message, the message is sent to the called party's mailbox, at which time the message is available for the called party's retrieval. The message delivery time for a call is the length of time, in seconds, it takes to deliver the recorded message to the target Collaboration Suite Database. Each instance can service one or more calls.

The number of calls with a specific range of message delivery times collected for this instance are labelled as *Calls with < range of message delivery times > ms. Message Delivery Time*, where < *range of message delivery times* > can range from 0 to 10000 seconds (ms), in increments of 500 ms. The number of calls with over 1000 seconds message delivery time is reported in *Calls with over 10000 ms. Message Delivery Time*.

The average, minimum, and maximum message delivery times, as well as the number of calls engaging in message delivery activity for this instance, are also reported.

79.1.1 Average Message Delivery Time (sec.)

Average Message Delivery Time is the average message delivery time for this instance, over the time period specified in the View Data field. Message delivery time is the time, in seconds, it takes to deliver a message to the mail box.

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 79–1 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	Not Defined	1	Average OVF Message Delivery Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Message Delivery Monitor Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Message Delivery Monitor Service instances, resource shortage among key components in the instances.

To investigate why the message delivery time exceeded the response time value set, check for alerts that may have been generated by the Message Delivery Monitor Service or specific instances of the Message Delivery Monitor Service, the Voicemail & Fax Application that this Message Delivery Monitor Service is a member of (check the status of dependent components -- Oracle Internet Directory, Collaboration Suite Databases, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific message delivery instances, you can restart the message delivery service by selecting the Message Delivery Monitor Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting the components, review the resource usage of the Message Delivery Monitor Service and its dependent components.

79.1.2 Maximum Message Delivery Time (sec.)

Maximum Message Delivery Time is the longest message delivery time for this instance, over the time period specified in the View Data field. Message delivery time is the time, in seconds, it takes to deliver a message to the mail box.

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 79–2 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	>	Not Defined	Not Defined	1	Maximum OVF Message Delivery Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Message Delivery Monitor Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Message Delivery Monitor Service instances, resource shortage among key components in the instances.

To investigate why the message delivery time exceeded the response time value set, check for alerts that may have been generated by the Message Delivery Monitor Service or by specific instances of the Message Delivery Monitor Service, the Voicemail & Fax Application that this Message Delivery Monitor Service is a member of (check the dependent component status -- Oracle Internet Directory, Collaboration Suite Databases, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific message delivery instances, you can restart the Message Delivery Monitor Service by selecting the Message Delivery Monitor Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting the components, review the resource usage of the Message Delivery Monitor Service and its dependent components.

79.1.3 Minimum Message Delivery Time (sec.)

Minimum Message Delivery Time is the shortest message delivery time for this instance, over the time period specified in the View Data field. Message delivery time is the time, in seconds, it takes to deliver a message to the mail box.

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 79–3 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	>	Not Defined	Not Defined	1	Minimum OVF Message Delivery Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Message Delivery Monitor Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Message Delivery Monitor Service instances, resource shortage among key components in the instances.

To investigate why the message delivery time exceeded the response time value set, check for alerts that may have been generated by the Message Delivery Monitor Service or by specific instances of the Message Delivery Monitor Service, the Voicemail

& Fax Application that this Message Delivery Monitor Service is a member of (check the dependent component status -- Oracle Internet Directory, Collaboration Suite Databases, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific message delivery instances, you can restart the Message Delivery Monitor Service by selecting the Message Delivery Monitor Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their status. If you suspect contention for resources is affecting the components, review the resource usage of the Message Delivery Monitor Service and its dependent components.

79.1.4 Number of Calls with 0-500 s. Message Delivery Time

This metric reports the number of calls with 0-500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–4 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	>	Not Defined	Not Defined	1	Calls with 0-500 s Message Delivery Time exceeded.

79.1.5 Number of Calls with 1001-1500 s. Message Delivery Time

This metric reports the number of calls with 1001-1500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–5 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	>	Not Defined	Not Defined	1	Calls with 1001-1500 s Message Delivery Time exceeded.

79.1.6 Number of Calls with 1501-2000 s. Message Delivery Time

This metric reports the number of calls with 1501-2000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–6 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	>	Not Defined	Not Defined	1	Calls with 1501-2000 s Message Delivery Time exceeded.

79.1.7 Number of Calls with 2001-2500 s. Message Delivery Time

This metric reports the number of calls with 2001-2500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–7 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 2001-2500 s Message Delivery Time exceeded.

79.1.8 Number of Calls with 2501-3000 s. Message Delivery Time

This metric reports the number of calls with 2501-3000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–8 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	After Every Sample	>	Not Defined	Not Defined	1	Calls with 2501-3000 s Message Delivery Time exceeded.

79.1.9 Number of Calls with 3001-3500 s. Message Delivery Time

This metric reports the number of calls with 3001-3500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–9 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	After Every Sample	>	Not Defined	Not Defined	1	Calls with 3001-3500 s Message Delivery Time exceeded.

79.1.10 Number of Calls with 3501-4000 s. Message Delivery Time

This metric reports the number of calls with 3501-4000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–10 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 3501-4000 s Message Delivery Time exceeded.

79.1.11 Number of Calls with 4001-4500 s. Message Delivery Time

This metric reports the number of calls with 4001-4500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–11 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 4001-4500 s Message Delivery Time exceeded.

79.1.12 Number of Calls with 4501-5000 s. Message Delivery Time

This metric reports the number of calls with 4501-5000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–12 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 4501-5000 s Message Delivery Time exceeded.

79.1.13 Number of Calls with 5001-5500 s. Message Delivery Time

This metric reports the number of calls with 5001-5500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–13 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 5001-5500 s Message Delivery Time exceeded.

79.1.14 Number of Calls with 501-1000 s. Message Delivery Time

This metric reports the number of calls with 501-1000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–14 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 501-1000 s Message Delivery Time exceeded.

79.1.15 Number of Calls with 5501-6000 s. Message Delivery Time

This metric reports the number of calls with 5501-6000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–15 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 5501-6000 s Message Delivery Time exceeded.

79.1.16 Number of Calls with 6001-6500 s. Message Delivery Time

This metric reports the number of calls with 6001-6500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–16 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 6001-6500 s Message Delivery Time exceeded.

79.1.17 Number of Calls with 6501-7000 s. Message Delivery Time

This metric reports the number of calls with 6501-7000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–17 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 6501-7000 s Message Delivery Time exceeded.

79.1.18 Number of Calls with 7001-7500 s. Message Delivery Time

This metric reports the number of calls with 7001-7500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–18 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 7001-7500 s Message Delivery Time exceeded.

79.1.19 Number of Calls with 7501-8000 s. Message Delivery Time

This metric reports the number of calls with 7501-8000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–19 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 7501-8000 s Message Delivery Time exceeded.

79.1.20 Number of Calls with 8001-8500 s. Message Delivery Time

This metric reports the number of calls with 8001-8500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–20 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 8001-8500 s Message Delivery Time exceeded.

79.1.21 Number of Calls with 8501-9000 s. Message Delivery Time

This metric reports the number of calls with 8501-9000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–21 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 8501-9000 s Message Delivery Time exceeded.

79.1.22 Number of Calls with 9001-9500 s. Message Delivery Time

This metric reports the number of calls with 9001-9500 seconds message delivery times, collected for all calls serviced by this instance.

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 79–22 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 9001-9500 s Message Delivery Time exceeded.

79.1.23 Number of Calls with 9501-10000 s. Message Delivery Time

This metric reports the number of calls with 9501-10000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–23 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 9501-10000 s Message Delivery Time exceeded.

79.1.24 Number of Calls with over 10000 s. Message Delivery Time

This metric reports the number of calls with over 10000 seconds message delivery times, collected for all calls serviced by this instance.

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 79–24 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with greater than 10000 s Message Delivery Time exceeded.

79.1.25 Recipient Collaboration Suite Database Name

Name of the Collaboration Suite Database where the recorded message is stored. This is the Collaboration Suite Database where the message delivery test account is set up.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.1.26 Sender Host Name

Host name of system where message delivery instance is running.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.2 Message Delivery Monitor Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Message Delivery Monitor Service instance. It provides a snapshot of how the Message Delivery Monitor Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Message Delivery Monitor Service instance.

79.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Message Delivery Monitor Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 79–25 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
All Versions	Every 5 Minutes	After Every Sample	>	70	75	2	CPU utilization of Message Delivery Monitor Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Message Delivery Monitor Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Message Delivery Monitor Service instance, the Voicemail and Fax Application that this Message Delivery Monitor Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

79.2.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.2.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Message Delivery Monitor Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 79–26 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
All Versions	Every 5 Minutes	After Every Sample	>	80	90	2	Memory utilization of Message Delivery Monitor Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Message Delivery Monitor Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Message Delivery Monitor Service instance, the Voicemail and Fax Application that this Message Delivery Monitor Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

79.2.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Message Delivery Monitor Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Message Delivery Monitor Service instance.

79.2.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.2.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.2.7 Status

This metric provides information about the Up/Down status of the Message Delivery Monitor Service instance and alerts you when the Message Delivery Monitor Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 79–27 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
All Versions	Every 5 Minutes	After Every Sample	=	Not Defined	0	1	Message Delivery Monitor Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Message Delivery Monitor Service by selecting the Message Delivery Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Message Delivery Monitor Service instance, the Voicemail and Fax Application that this Message Delivery Monitor Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

79.2.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.3 Message Delivery Monitor Service Message Delivery Time Distribution

This metric reports the number of calls with message delivery times that fall within specified intervals, for example, the number of calls with a message delivery time of 0-500 milliseconds. "Number of Calls" is the calls reported for all instances during the collection interval. See the Number of Calls metric for additional details.

79.3.1 Number of Calls

This metric provides additional metrics on message delivery time for each specified interval.

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 79–28 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with Message Delivery Response Time range (s) exceeded.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Message Delivery Time (sec.)" object.

If warning or critical threshold values are currently set for any "Message Delivery Time (sec.)" 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 "Message Delivery Time (sec.)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

79.4 Message Delivery Monitor Service Performance Metrics

This category includes a set of metrics that provides summary information about the message delivery times of all service instances in the Message Delivery Monitor Service. Once a caller confirms that he or she has completed recording a message, the message is sent to the called party's mailbox, at which time the message is available for the called party's retrieval. The message delivery time for a call is the length of time, in seconds, it takes to deliver the recorded message to the target Collaboration Suite Database. Each instance can service one or more calls. The average, minimum, and maximum message delivery times are reported.

79.4.1 Average Message Delivery Time (sec.)

Average Message Delivery Time is the average message delivery time for all instances, over the time period specified in the View Data field. Message delivery time is the time, in seconds, it takes to deliver a message to the mail box.

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 79–29 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Average OVF Message Delivery Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Message Delivery Monitor Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Message Delivery Monitor Service instances, resource shortage among key components in the instances.

To investigate why the message delivery time exceeded the response time value set, check for alerts that may have been generated by the Message Delivery Monitor Service or by specific instances of the Message Delivery Monitor Service, the Voicemail & Fax Application that this Message Delivery Monitor Service is a member of (check

the dependent component status -- Oracle Internet Directory, Collaboration Suite Databases, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific message delivery instances, you can restart the Message Delivery Monitor Service by selecting the Message Delivery Monitor Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting the components, review the resource usage of the Message Delivery Monitor Service and its dependent components.

79.4.2 Maximum Message Delivery Time (sec.)

Maximum Message Delivery Time is the longest message delivery time for all instances, over the time period specified in the View Data field. Message delivery time is the time, in seconds, it takes to deliver a message to the mail box.

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 79–30 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Average OVF Maximum Message Delivery Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Message Delivery Monitor Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Message Delivery Monitor Service instances, resource shortage among key components in the instances.

To investigate why the message delivery time exceeded the response time value set, check for alerts that may have been generated by the Message Delivery Monitor Service or by specific instances of the Message Delivery Monitor Service, the Voicemail & Fax Application that this Message Delivery Monitor Service is a member of (check the status of dependent components -- Oracle Internet Directory, Collaboration Suite Databases, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific message delivery instances, you can restart the Message Delivery Monitor Service by selecting the Message Delivery Monitor Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting the components, review the resource usage of the Message Delivery Monitor Service and its dependent components.

79.4.3 Minimum Message Delivery Time (sec.)

Minimum Message Delivery Time is the shortest message delivery time for all instances, over the time period specified in the View Data field. Message delivery time is the time, in seconds, it takes to deliver a message to the mail box.

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 79–31 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Average OVF Minimum Message Delivery Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Message Delivery Monitor Service instances, outage of one or more key components in the instances, contention for common resourcesd (for example, Oracle Internet Directory) among Message Delivery Monitor Service instances, resource shortage among key components in the instances.

To investigate why the message delivery time exceeded the response time value set, check for alerts that may have been generated by the Message Delivery Monitor Service or by specific instances of the Message Delivery Monitor Service, the Voicemail & Fax Application that this Message Delivery Monitor Service is a member of (check the dependent component status -- Oracle Internet Directory, Collaboration Suite Databases, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific message delivery instances, you can restart the Message Delivery Monitor Service by selecting the Message Delivery Monitor Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting the components, review the resource usage of the Message Delivery Monitor Service and its dependent components.

79.4.4 Recipient Collaboration Suite Database Name

Name of the Collaboration Suite Database where the recorded message is stored. This is the Collaboration Suite Database where the message delivery test account is set up.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.4.5 Sender Host Name

Host name of the system that the Message Delivery Monitor Service is running.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.5 Message Delivery Monitor Service Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Message Delivery Monitor Service. It provides a snapshot of how the Message Delivery Monitor Service instances are performing. If a particular metric is empty, it is likely that a Message Delivery Monitor Service instance is down and unavailable. Check the Up/Down status metric for all the Message Delivery Monitor Service instances.

79.5.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 79–32 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
All Versions	Every 5 Minutes	After Every Sample	>	70	75	2	CPU utilization of Message Delivery Monitor Service, %target%, is %value%%

User Action

You can use this metric to determine if the Message Delivery Monitor Service is using the most CPU on your system, thereby leading to high end-user response times. If the Message Delivery Monitor Service is consuming a large amount of CPU, consider

changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Message Delivery Monitor Service, the Voicemail and Fax Application that this Message Delivery Monitor Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

79.5.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 79–33 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
All Versions	Every 5 Minutes	After Every Sample	>	80	90	2	Memory utilization of Message Delivery Monitor Service, %target%, is %value%%

User Action

You can use this metric to determine if the Message Delivery Monitor Service is using the most memory on your system and leading to high end-user response times. If the Message Delivery Monitor Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Message Delivery Monitor Service instances, the Voicemail and Fax Application that this Message Delivery Monitor Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

79.5.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Message Delivery Monitor Service.

79.5.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.5.5 Status

This metric provides information about the Up/Down status of the Message Delivery Monitor Service. The Message Delivery Monitor Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Message Delivery Monitor Service by selecting the Message Delivery Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Message Delivery Monitor Service, specific instances of the Message Delivery Monitor Service, the Voicemail and Fax Application that this Message Delivery Monitor Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

79.5.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.5.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

79.6 Message Delivery Monitor Service Response

This category includes metrics that provide information about the Up/Down status of the Message Delivery Monitor Service.

79.6.1 Status

This metric provides information about the Up/Down status of the Message Delivery Monitor Service and alerts you when the Message Delivery Monitor Service is down. The Message Delivery Monitor Service shows a status of Down when all configured instances for this service are down. By default, a critical threshold value is set for this metric. Alerts are 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 79–34 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
All Versions	Every 5 Minutes	After Every Sample	=	Not Defined	0	1	Message Delivery Monitor Service, %target%, is down

User Action

You can restart the Message Delivery Monitor Service by selecting the Message Delivery Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Message Delivery Monitor Service, specific instances of the Message Delivery Monitor Service, the Voicemail and Fax Application that this Message Delivery Monitor Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

79.7 Raw Message Delivery Monitor Instance Performance Metrics

This metric is for internal use only.

80

Message Recovery Service

This target represents the Message Recovery Service. The Message Recovery Service recovers messages that are not successfully delivered. If the voice mail Recording Service or Fax Receiving Service encounters errors when communicating with the Information Store, the Message Recovery Service attempts to redeliver the message. The Message Recovery Service periodically attempts to send any messages in its file system queue. Once the Message Recovery Service successfully sends a message, the message is deleted from the queue.

80.1 Message Recovery Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Message Recovery Service instance. It provides a snapshot of how the Message Recovery Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Message Recovery Service instance.

80.1.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Message Recovery Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 80–1 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	>	70	75	2	CPU utilization of Message Recovery Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Message Recovery Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Message Recovery Service instance, the Voicemail and Fax Application that this Message Recovery Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

80.1.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

80.1.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Message Recovery Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 80–2 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	>	80	90	2	Memory utilization of Message Recovery Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Message Recovery Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Message Recovery Service instance, the Voicemail and Fax Application that this Message Recovery Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

80.1.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Message Recovery Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Message Recovery Service instance.

80.1.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

80.1.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

80.1.7 Status

This metric provides information about the Up/Down status of the Message Recovery Service instance and alerts you when the Message Recovery Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 80–3 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	=	Not Defined	0	1	Message Recovery Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Message Recovery Service by selecting the Message Recovery Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Message Recovery Service instance, the Voicemail and Fax Application that this Message Recovery Service instance is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

80.1.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

80.2 Message Recovery Service Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Message Recovery Service. It provides a snapshot of how the Message Recovery Service instances are performing. If a particular metric is empty, it is likely that an Message Recovery Service instance is down and unavailable. Check the Up/Down status metric for all the Message Recovery Service instances.

80.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 80–4 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	>	70	75	2	CPU utilization of Message Recovery Service, %target%, is %value%%

User Action

You can use this metric to determine if the Message Recovery Service is using the most CPU on your system, thereby leading to high end-user response times. If the Message Recovery Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Message Recovery Service, the Voicemail and Fax Application that this Message Recovery Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

80.2.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 80–5 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	>	80	90	2	Memory utilization of Message Recovery Service, %target%, is %value%%%

User Action

You can use this metric to determine if the Message Recovery Service is using the most memory on your system and leading to high end-user response times. If the Message Recovery Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Message Recovery Service instances, the Voicemail and Fax Application that this Message Recovery Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

80.2.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Message Recovery Service.

80.2.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

80.2.5 Status

This metric provides information about the Up/Down status of the Message Recovery Service. The Message Recovery Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Message Recovery Service by selecting the Message Recovery Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Message Recovery Service, specific instances of the Message Recovery Service, the Voicemail and Fax Application that this Message Recovery Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

80.2.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

80.2.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

80.3 Message Recovery Service Response

This category contains metrics that provide information about the Up/Down status of the Message Recovery Service.

80.3.1 Status

This metric provides information about the Up/Down status of the Message Recovery Service and alerts you when the Message Recovery Service is down. The Message Recovery Service shows a status of Down when all configured instances for this

service are down. By default, a critical threshold value is set for this metric. Alerts are 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 80–6 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	=	Not Defined	0	1	Message Recovery Service, %target%, is down

User Action

You can restart the Message Recovery Service by selecting the Message Recovery Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Message Recovery Service, specific instances of the Message Recovery Service, the Voicemail and Fax Application that this Message Recovery Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

81

MWI Service

This target represents the MWI Service. The MWI (Message Waiting Indicator) Service activates and deactivates users message waiting indicators. This is in response to requests stored on each Collaboration Suite Database associated with the services Voicemail and Fax Application.

81.1 MWI Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Message Waiting Indicator Service instance. It provides a snapshot of how the Message Waiting Indicator Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Message Waiting Indicator Service instance.

81.1.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Message Waiting Indicator Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 81–1 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	>	70	75	2	CPU utilization of MWI Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Message Waiting Indicator Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Message Waiting Indicator Service instance, the Voicemail and Fax Application that this Message Waiting Indicator Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

81.1.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

81.1.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Message Waiting Indicator Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 81–2 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	>	80	90	2	Memory utilization of MWI Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Message Waiting Indicator Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Message Waiting Indicator Service instance, the Voicemail and Fax Application that this Message Waiting Indicator Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

81.1.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Message Waiting Indicator Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Message Waiting Indicator Service instance.

81.1.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

81.1.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

81.1.7 Status

This metric provides information about the Up/Down status of the Message Waiting Indicator Service instance and alerts you when the Message Waiting Indicator Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 81–3 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	=	Not Defined	0	1	MWI Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Message Waiting Indicator Service by selecting the Message Waiting Indicator Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Message Waiting Indicator Service instance, the Voicemail and Fax Application that this Message Waiting Indicator Service instance is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

81.1.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

81.2 MWI Service Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Message Waiting Indicator Service. It provides a snapshot of how the Message Waiting Indicator Service instances are performing. If a particular metric is empty, it is likely that an Message Waiting Indicator Service instance is down and unavailable. Check the Up/Down status metric for all the Message Waiting Indicator Service instances.

81.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 81–4 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	>	70	75	2	CPU utilization of MWI Service, %target%, is %value%%

User Action

You can use this metric to determine if the Message Waiting Indicator Service is using the most CPU on your system, thereby leading to high end-user response times. If the Message Waiting Indicator Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Message Waiting Indicator Service, the Voicemail and Fax Application that this Message Waiting Indicator Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

81.2.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 81–5 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	>	80	90	2	Memory utilization of MWI Service, %target%, is %value%%

User Action

You can use this metric to determine if the Message Waiting Indicator Service is using the most memory on your system and leading to high end-user response times. If the Message Waiting Indicator Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Message Waiting Indicator Service instances, the Voicemail and Fax Application that this Message Waiting Indicator Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

81.2.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Message Waiting Indicator Service.

81.2.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

81.2.5 Status

This metric provides information about the Up/Down status of the Message Waiting Indicator Service. The Message Waiting Indicator Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Message Waiting Indicator Service by selecting the Message Waiting Indicator Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Message Waiting Indicator Service, specific instances of the Message Waiting Indicator Service, the Voicemail and Fax Application that this Message Waiting Indicator Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

81.2.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

81.2.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

81.3 MWI Service Response

This category contains metrics that provide information about the Up/Down status of the Message Waiting Indicator Service.

81.3.1 Status

This metric provides information about the Up/Down status of the Message Waiting Indicator Service and alerts you when the Message Waiting Indicator Service is down. The Message Waiting Indicator Service shows a status of Down when all configured

instances for this service are down. By default, a critical threshold value is set for this metric. Alerts are 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 81–6 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	=	Not Defined	0	1	MWI Service, %target%, is down

User Action

You can restart the Message Waiting Indicator Service by selecting the Message Waiting Indicator Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Message Waiting Indicator Service, specific instances of the Message Waiting Indicator Service, the Voicemail and Fax Application that this Message Waiting Indicator Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

82

PBX-Application Cluster

This target represents the PBX-Application Cluster. Oracle Voicemail and Fax supports multiple locations in one voice mail system. Because there may be different types of PBXes in the same system, Oracle provides a way to define integrations through the concept of a PBX-Application Cluster. A PBX-Application Cluster defines a relationship between a PBX and one or more Voicemail and Fax Applications, called an application cluster, that support the PBX. For example, there may be two sites, San Francisco and Denver, served by two PBXes. The PBX that serves San Francisco is integrated with the Voicemail and Fax Application using analog and SMDI. The PBX that serves Denver is integrated using Voice Over IP (VOIP) and Host Media Processing (HMP). Each site is supported by a separate PBX-Application Cluster. San Francisco is supported by SF_Nortel and Denver is supported by Denver_VOIP.You set parameters in the PBX-Application Cluster for the specific Voicemail and Fax Applications that are servicing a specific PBX. The parameters define how the application integrates with the PBX. These parameters include the PBX integration type, PBX dialing rules, telephony number translation rules, Message Waiting Indicator (MWI) phone number conversion rules, Interactive Voice Response (IVR) mapping, and phone numbers belonging to the PBX. This configuration applies to any Voicemail and Fax Application that is associated with the PBX-Application Cluster. Therefore, once you configure a PBX-Application Cluster, you can change which application is associated with the PBX without having to reconfigure the application.

82.1 PBX-Application Cluster Response

This category contains metrics that provide information about the Up/Down status of the PBX-Application Cluster.

82.1.1 Status

This metric provides information about the Up/Down status of the PBX-Application Cluster. It alerts you when the PBX-Application Cluster is down. The PBX-Application Cluster is considered down when any of its member targets, that is, when any one of its Voicemail and Fax Application targets, is down. The evaluation of this metric is triggered whenever there is a change in the Up/Down status of any of its member targets. The alert message for the status of the PBX-Application Cluster lists the members followed by their state. The possible states are: Up, Down, Unreachable, Blackout, Agent Down, Metric Error, and Status Pending.

Metric Summary

The following table shows how this metric is evaluated and the alerts that get generated.

Target Version	Evaluation and Collection Frequency	Alert Text	Alert Example
All Versions	Every time there is a change in the Response Status of its member targets	Members status --> %Non-zero count of members% Up; %Non-zero count of members% Down; %Non-zero count of members% Unreachable; %Non-zero count of members% Blackout; %Non-zero count of members% Agent Down; %Non-zero count of members% Metric Error; %Non-zero count of members% Status Pending;	Members status --> 1 Up; 3 Status Pending;

User Action

The status of the PBX-Application Cluster is dependent on the status of its members. To investigate why the PBX-Application Cluster is down, check for alerts that may have been generated by its member targets, that is, the Voicemail and Fax Applications, or by their corresponding host and agent targets.

83

OVF AQMWI Application

Gives status of the OVF AQMWI application.

83.1 Response

Gives status of the OVF AQMWI application.

83.1.1 Status

Gives status of the OVF AQMWI application.

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 83–1 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 3 Minutes	After Every Sample	=	Not Defined	0	1	AQMWI Application is down

84

OVF FaxIn Application

Gives status of the OVF FaxIn application.

84.1 Response

Gives the status of the OVF FaxIn application.

84.1.1 Status

Gives status of the OVF FaxIn application.

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 84–1 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 3 Minutes	After Every Sample	=	Not Defined	0	1	FaxIn Application is down

85

OVF MWI Service

You can use Enterprise Manager to view metrics for the Oracle Voicemail and Fax MWI Service.

85.1 Response

This category contains metrics about the response of the Oracle Voicemail and Fax MWI Service.

85.1.1 Status

This metric shows the status of the Oracle Voicemail and Fax MWI Service.

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 85–1 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 3 Minutes	After Every Sample	=	Not Defined	0	1	MWI Service is down

86

OVF Recording Application

You can use Enterprise Manager to view metrics for the Oracle Voicemail and Fax recording application.

86.1 Activity Total Time

This category contains metrics about the number of users performing each activity, total time spent in each activity, and the average time spent in each activity for the last five minutes.

86.1.1 Recording Activity Total Response Time

The total time (in milliseconds) spent performing the activity for the last five minutes.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

86.1.2 Recording Activity User Count

The number of users performing the activity for the last five minutes.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

86.1.3 Recording Avg Response Time

The average time (in milliseconds) it took to perform the activity for the last five 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 86–1 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
All Versions	activity_ name: "GREETING"	Every 5 Minutes	After Every Sample	>	3000	4000	1	The vm average recording message time is %value%

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Voicemail Activity" 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 "Voicemail Activity" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

86.2 Caller Greeting Wait Time

This category contains metrics about the time callers had to wait for a greeting.

86.2.1 Num Users waiting for Greeting

The number of users waiting for a greeting in each five minute interval.

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 86–2 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
All Versions	response_ duration: ">10000"	Every 5 Minutes	After Every Sample	>	1	5	1	The user greeting time is more than 10000ms for %value% users

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Duration (msec)" object.

If warning or critical threshold values are currently set for any "Duration (msec)" 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 "Duration (msec)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

86.3 Response

This category contains metrics about the response of the Oracle Voicemail and Fax recording application.

86.3.1 Response Status

This metric shows the status of the Oracle Voicemail and Fax recording application.

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 86–3 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 3 Minutes	After Every Sample	=	Not Defined	0	1	Recording Application is down

87

OVF Recovery Application

You can use Enterprise Manager to view metrics for the Oracle Voicemail and Fax recovery application.

87.1 Response

This category contains metrics about the response of the Oracle Voicemail and Fax recovery application.

87.1.1 Status

This metric shows the status of the Oracle Voicemail and Fax recovery application.

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 87–1 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 3 Minutes	After Every Sample	=	Not Defined	0	1	Recovery Application is down

88

OVF Retrieval Application

You can use Enterprise Manager to view metrics for the Oracle Voicemail and Fax retrieval application.

88.1 Activity Total Time

This category contains metrics about the total amount of time it took to perform the activity, the total number of users performing the activity, and the average time it takes to perform the activity.

Examples of activities are play message times and user password times.

88.1.1 Retrieval Avg Response Time

The average time it took to perform the activity in the last 5 minute interval.

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 88–1 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
All Versions	activity_ name: "USER_ PWD"	Every 5 Minutes	After Every Sample	>	2000	2500	1	The vm average User Password time is %value%

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Retrieval Voicemail Activity" object.

If warning or critical threshold values are currently set for any "Retrieval Voicemail Activity" 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 "Retrieval Voicemail Activity" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

88.1.2 Retrieval Number of Users

The number of users performing the activity in the last 5 minute interval.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

88.1.3 Retrieval Sum of Response Time

The total amount of time it took to perform the activity in the last five minutes.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

88.2 Database Login Time

This category contains metrics about the amount of time it took users to login to the database.

88.2.1 DB Login Time User Count

The number of users waiting to login to the database in each 5 minute interval.

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 88–2 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
All Versions	response_ duration: ">2000"	Every 5 Minutes	After Every Sample	>	1	5	1	The DB login time is more than 2000ms for %value% users

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Response Duration (msec)" object.

If warning or critical threshold values are currently set for any "Response Duration (msec)" 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 "Response Duration (msec)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

88.3 Listen To Message Time

This category contains metrics about the amount of time users had to wait to listen to a message.

88.3.1 Listen Time User Count

The number of users waiting to listen to messages in each 5 minute interval.

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 88–3 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
All Versions	response_ duration: ">10000"	Every 5 Minutes	After Every Sample	>	1	5	1	The play message time is more than 10000ms for %value% users

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Response Duration (msec)" object.

If warning or critical threshold values are currently set for any "Response Duration (msec)" 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 "Response Duration (msec)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

88.4 Response

This category contains metrics about the response of the Oracle Voicemail and Fax retrieval application.

88.4.1 Status

This metric shows the status of the Oracle Voicemail and Fax retrieval application.

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 88–4 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 3 Minutes	After Every Sample	=	Not Defined	0	1	Retrieval Application is down

88.5 User Login Time

This category contains metrics about the amount of time users had to wait to login.

88.5.1 Login Time User Count

Number of users waiting to login in each five minute interval.

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 88–5 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
All Versions	response_ duration: ">10000"	Every 5 Minutes	After Every Sample	>	1	5	1	The retrieval time is more than 10000ms for %value% users

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Response Duration (msec)" object.

If warning or critical threshold values are currently set for any "Response Duration (msec)" 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 "Response Duration (msec)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

89

OVF Routing Application

You can use Enterprise Manager to view metrics for the Oracle Voicemail and Fax routing application.

89.1 Response

This category contains metrics about the response of the Oracle Voicemail and Fax routing application.

89.1.1 Status

This metric shows the status of the Oracle Voicemail and Fax routing application.

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 89–1 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 3 Minutes	After Every Sample	=	Not Defined	0	1	Routing Application is down

90

OVF Telephony Midtier

You can use Enterprise Manager to view metrics for the Oracle Voicemail and Fax telephony midtier.

90.1 Number of Callers

This category provides metrics about the number of callers.

90.1.1 Current Number of Callers

This metric shows the number of callers at the current time.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

90.1.2 Total Number of Callers

This metric shows the total number of callers since the startup of the machine.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

90.2 Response

This category contains metrics about the response of the Oracle Voicemail and Fax telephony midtier machine's telephony subsystem.

90.2.1 Status

This metric shows the status of the Oracle Voicemail and Fax telephony midtier machine's telephony subsystem.

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 90–1 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 3 Minutes	After Every Sample	=	Not Defined	0	1	Voicemail Server down

91

OVF Mailstore

Provides the status of the backend mailstore database.

91.1 Activity Time

This is the key column. The key is the type of activity. Examples of activity types are login time, play message time, user password.

91.1.1 Activity User Count

Number of users who performed that activity in the last five minutes.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

91.1.2 Average Response Time

Sum of response time divided by number of users.

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 91–1 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
All Versions	activity_name: "PLAY_MSG"	Every 5 Minutes	After Every Sample	>	2000	2500	1	The vm average play message time is %value%

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Voicemail Activity" 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 "Voicemail Activity" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

91.1.3 Sum of Response Time

Total response time for all the users for a particular activity for the last five minutes.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

91.2 Database Login Time

Divides the amount of time it takes to login to database into intervals. Gives the number of users whose database login times fits into each interval.

91.2.1 DB Login Time User Count

Number of users for each interval.

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 91–2 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
All Versions	response_duration: ">2000"	Every 5 Minutes	After Every Sample	>	1	5	1	The DB login time is greater than 2000 for %value% users

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Response Duration (msec)" object.

If warning or critical threshold values are currently set for any "Response Duration (msec)" 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 "Response Duration (msec)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

91.3 Delivery Time

Provides a measurement of the mail delivery times.

91.3.1 Elapsed Time (msec)

Provides a measurement of the mail delivery times.

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 91–3 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	>	300000	600000	1	The voicemail delivery time is %value%

91.4 Listen To Message Time

Divides the amount of time it takes to listen to messages into intervals. Gives the number of users whose listen times fits into each interval.

91.4.1 Listen Time User Count

Number of users for each interval.

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 91–4 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
All Versions	response_duration: ">10000"	Every 5 Minutes	After Every Sample	>	1	5	1	The play message time is greater than 10000 for %value% users

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Response Duration (msec)" object.

If warning or critical threshold values are currently set for any "Response Duration (msec)" 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 "Response Duration (msec)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

91.5 Response

Provides the status of the backend mailstore database.

91.5.1 Status

Provides the status of the backend mailstore database.

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 91–5 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	=	Not Defined	0	1	Failed to connect to the database

91.6 User Login Time

Divides the login time into intervals. For example, 0-100ms, 100-200ms, 200 - 300ms. Gives the number of users whose login time fits into each interval. For example, It took 8 users 0-100ms to login, 3 users 100-200ms, and 1 user 200-300ms. This type of metric is common in OVF and repeated several times below.

91.6.1 User Count for Login Time

Displays the number of users for each interval.

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 91–6 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
All Versions	response_duration: ">10000"	Every 5 Minutes	After Every Sample	>	1	5	1	The response duration is > 10000 for %value% users

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Response Duration (msec)" object.

If warning or critical threshold values are currently set for any "Response Duration (msec)" 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 "Response Duration (msec)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

92

OVF Transfer Application

You can use Enterprise Manager to view metrics for the Oracle Voicemail and Fax transfer application.

92.1 Response

This category contains metrics about the response of the Oracle Voicemail and Fax transfer application.

92.1.1 Status

This metric shows the status of the Oracle Voicemail and Fax transfer application.

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 92–1 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 3 Minutes	After Every Sample	=	Not Defined	0	1	Transfer Application is down

93

Recording Service

This target represents the Recording Service. There are two basic scenarios in which the Recording Service is used. In the first instance, a call comes in and the callee does not pick up the call. The call is forwarded to the voice mail system, where the Recording Service retrieves the callees information from the Oracle Internet Directory and verifies that the callee has voice mail access. Then the Recording Service plays the callee's greeting, records the caller's message and sends it. In the second instance, a voice mail user accesses the voice mail system and after being authenticated by the voice mail system chooses to send a message to another voice mail user, reply to the sender of the voice mail message, or forward the voice mail message to one or more recipients.

93.1 Raw Recording Instance Performance Metrics

This metric is for internal use only.

93.2 Recording Instance Performance Metrics

This category includes a set of metrics that provides information about the greeting response times of each individual service instance of the Recording Service.

The greeting response time for a call is the time it takes for the caller to hear the voice mail greeting once the caller has successfully logged in. Each instance can service one or more calls.

The number of calls with a specific range of greeting response times collected for each instance is labelled as *Calls with < range of response times > ms. Greeting Response Time*, where *< range of response times >* can range from 0 to 10000 milliseconds (ms), in increments of 500 ms.

The average, minimum, and maximum greeting response times, as well as the number of calls engaging in greeting activity for each instance, are also reported.

93.2.1 Active Recording Calls

Active Recording Calls is the total number of calls playing a greeting. This total is calculated for calls serviced by this instance, over the time period specified in the View Data field.

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 93–1 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	Not Defined	1	Active Greeting calls exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Recording Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

93.2.2 Average Greeting Response Time (ms)

Average Greeting Response Time is the average greeting response time for this instance, over the time period specified in the View Data field. Greeting response time is the length of time, in milliseconds, to hear the voice mail system greeting once the user has successfully logged in.

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 93–2 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	>	Not Defined	Not Defined	1	Average OVF Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Recording Service instances, outage of one or more key components in the instances, contention of common resources (for instance, Oracle Internet Directory) among Recording Service instances, resource shortage among key components in the instances.

To investigate why the greeting response time exceeded the response time value set, check for alerts that may have been generated by this Recording Service instance, the Routing Service, the Voicemail & Fax Application that this Recording Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific recording instances, you can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting the components, review the resource usage of the Recording Service and its dependent components.

93.2.3 Host

Host name of system where recording instance is running

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.2.4 Maximum Greeting Response Time (ms)

Maximum Greeting Response Time is the longest greeting response time for this instance, over the time period specified in the View Data field. Greeting response time is the length of time, in milliseconds, to hear the voice mail system greeting once the user has successfully logged in.

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 93–3 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	>	Not Defined	Not Defined	1	Maximum OVF Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Recording Service instances, outage of one or more key components in the instances, contention of common resources (for instance, Oracle Internet Directory) among Recording Service instances, resource shortage among key components in the instances.

To investigate why the greeting response time exceeded the response time value set, check for alerts that may have been generated by this Recording Service instance, the Routing Service, the Voicemail & Fax Application that this Recording Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific recording instances, you can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting components, review the resource usage of the Recording Service and its dependent components.

93.2.5 Metric Name

Name of the metric.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.2.6 Minimum Greeting Response Time (ms)

Minimum Greeting Response Time is the shortest greeting response time for this instance, over the time period specified in the View Data field. Greeting response time is the length of time, in milliseconds, to hear the voice mail system greeting once the user has successfully logged in.

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 93–4 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	>	Not Defined	Not Defined	1	Minimum OVF Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Recording Service instances, outage of one or more key components in the instances, contention of common resources (for instance, Oracle Internet Directory) among Recording Service instances, resource shortage among key components in the instances.

To investigate why the greeting response time exceeded the response time value set, check for alerts that may have been generated by this Recording Service instance, the Routing Service, the Voicemail & Fax Application that this Recording Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific recording instances, you can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources affecting the components, review the resource usage of the Recording Service and its dependent components.

93.2.7 Number of Calls with 0-500 ms. Greeting Response Time

This metric reports the number of calls with 0-500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–5 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	>	Not Defined	Not Defined	1	Calls with 0-500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.8 Number of Calls with 1001-1500 ms. Greeting Response Time

This metric reports the number of calls with 1001-1500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–6 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	>	Not Defined	Not Defined	1	Calls with 1001-1500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.9 Number of Calls with 1501-2000 ms. Greeting Response Time

This metric reports the number of calls with 1501-2000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–7 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1501-2000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.10 Number of Calls with 2001-2500 ms. Greeting Response Time

This metric reports the number of calls with 2001-2500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–8 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	After Every Sample	>	Not Defined	Not Defined	1	Calls with 2001-2500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.11 Number of Calls with 2501-3000 ms. Greeting Response Time

This metric reports the number of calls with 2501-3000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–9 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	After Every Sample	>	Not Defined	Not Defined	1	Calls with 2501-3000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.12 Number of Calls with 3001-3500 ms. Greeting Response Time

This metric reports the number of calls with 3001-3500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–10 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 3001-3500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.13 Number of Calls with 3501-4000 ms. Greeting Response Time

This metric reports the number of calls with 3501-4000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–11 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 3501-4000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.14 Number of Calls with 4001-4500 ms. Greeting Response Time

This metric reports the number of calls with 4001-4500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–12 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 4001-4500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.15 Number of Calls with 4501-5000 ms. Greeting Response Time

This metric reports the number of calls with 4501-5000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–13 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 4501-5000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.16 Number of Calls with 5001-5500 ms. Greeting Response Time

This metric reports the number of calls with 5001-5500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–14 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 5001-5500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.17 Number of Calls with 501-1000 ms. Greeting Response Time

This metric reports the number of calls with 501-1000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–15 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 501-1000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.18 Number of Calls with 5501-6000 ms. Greeting Response Time

This metric reports the number of calls with 5501-6000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–16 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 5501-6000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.19 Number of Calls with 6001-6500 ms. Greeting Response Time

This metric reports the number of calls with 6001-6500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–17 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 6001-6500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.20 Number of Calls with 6501-7000 ms. Greeting Response Time

This metric reports the number of calls with 6501-7000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–18 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 6501-7000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.21 Number of Calls with 7001-7500 ms. Greeting Response Time

This metric reports the number of calls with 7001-7500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–19 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 7001-7500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.22 Number of Calls with 7501-8000 ms. Greeting Response Time

This metric reports the number of calls with 7501-8000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–20 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 7501-8000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.23 Number of Calls with 8001-8500 ms. Greeting Response Time

This metric reports the number of calls with 8001-8500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–21 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 8001-8500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.24 Number of Calls with 8501-9000 ms. Greeting Response Time

This metric reports the number of calls with 8501-9000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–22 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 8501-9000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.25 Number of Calls with 9001-9500 ms. Greeting Response Time

This metric reports the number of calls with 9001-9500 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–23 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 9001-9500 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.26 Number of Calls with 9501-10000 ms. Greeting Response Time

This metric reports the number of calls with 9501-10000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–24 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 9501-10000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.27 Number of Calls with over 10000 ms. Greeting Response Time

This metric reports the number of calls with over 10000 milliseconds greeting response times, collected for all calls serviced by this instance.

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 93–25 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with greater than 10000 ms Greeting Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.2.28 Port Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.3 Recording Instance Resource Usage Metrics

This category contains a set of related metrics that provide you with information about the CPU and Memory being used by the Recording Service instance. Its provides a snapshot of how the Recording Service instance is performing. If a particular metric is empty, a Recording Service instance is likely down and unavailable. Check the Up/Down status metric for all the Recording Service instances.

93.3.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Recording Service. By default, a critical and warning threshold value is set for this

metric. 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 93–26 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
All Versions	Every 5 Minutes	After Every Sample	>	70	75	2	CPU utilization of Recording Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Recording Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the amount of CPU consumption. To investigate why the instance is consuming a large amount of CPU, check for alerts that may have been generated by the Recording Service instance, or by the Voicemail and Fax Application that this Recording Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or by the host computer.

93.3.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.3.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Recording Service instance.

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 93–27 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
All Versions	Every 5 Minutes	After Every Sample	>	80	90	2	Memory utilization of Recording Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Recording Service instance is using the most memory on your system, thereby leading to high end-user response times.If the instance is consuming a large amount of memory, consider changing the configuration settings to reduce the amount of memory consumption. To investigate why the instance is consuming a large amount of memory, check for alerts that may have been generated by the Recording Service instance, or by the Voicemail and Fax Application that this Recording Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or by the host computer.

93.3.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Recording Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Recording Service instance.

93.3.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.3.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.3.7 Status

This metric provides information about the Up/Down status of the Recording Service instance. This metric alerts you when the instance is down. If the status for an instance is down, it could mean that the instance may be in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical and warning threshold value is set for this metric. 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 93–28 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
All Versions	Every 5 Minutes	After Every Sample	=	Not Defined	0	1	Recording Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the Recording Service instance, or by the Voicemail and Fax Application that this Recording Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or by the central agent on the host computer or by the host computer.

93.3.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.4 Recording Service Greeting Response Time Distribution

This metric reports the number of calls with greeting response times that fall within specified intervals, for example, the number of calls with a greeting response time of 0-500 milliseconds. "Number of Calls" is the calls reported for all instances during the collection interval. See the Number of Calls metric for additional details.

93.4.1 Number of Calls

This metric provides additional metrics on greeting response time for each specified interval.

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 93–29 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with Greeting Response Time range (ms) exceeded.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Greeting Response Time (ms)" object.

If warning or critical threshold values are currently set for any "Greeting Response Time (ms)" 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 "Greeting Response Time (ms)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

93.5 Recording Service Performance Metrics

This category includes a set of metrics that provides summary information about the greeting response times of all service instances of the Recording Service. The greeting response time for a call is the time it takes for the caller to hear the voice mail greeting once the caller has successfully logged in. Each instance can service one or more calls. The average, minimum, and maximum greeting response times, as well as the number of calls engaging in greeting activity for all instances, are also reported.

93.5.1 Active Recording Calls

Active Recording Calls is the total number of calls playing a greeting. This total is calculated for all instances over the time period specified in the View Data field.

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 93–30 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Active Greeting calls exceeded.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Recording Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

93.5.2 Average Greeting Response Time (ms)

Average Greeting Response Time is the average greeting response time for all instances, over the time period specified in the View Data field. Greeting response time is the length of time, in milliseconds, to hear the voice mail system greeting once the user has successfully logged in.

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 93–31 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Average OVF Greeting Response Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Recording Service instances, outage of one or more key components in the instances, contention of common resources (for instance, Oracle Internet Directory) among Recording Service instances, resource shortage among key components in the instances.

To investigate why the greeting response time exceeded the response time value set, check for alerts that may have been generated by the Recording Service or by specific instances of the Recording Service, the Routing Service, the Voicemail & Fax Application that this Recording Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific recording instances, you can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting the components, review the resource usage of the Recording Service and its dependent components.

93.5.3 Maximum Greeting Response Time (ms)

Maximum Greeting Response Time is the longest greeting response time across all instances, over the time period specified in the View Data field. Greeting response time is the length of time, in milliseconds, to hear the voice mail system greeting once the user has successfully logged in.

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 93–32 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Average OVF Maximum Greeting Response Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Recording Service instances, outage of one or more key components in the instances, contention of common resources (for instance, Oracle Internet Directory) among Recording Service instances, resource shortage among key components in the instances.

To investigate why the greeting response time exceeded the response time value set, check for alerts that may have been generated by the Recording Service or by specific instances of the Recording Service, the Routing Service, the Voicemail & Fax Application that this Recording Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific recording instances, you can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting components, review the resource usage of the Recording Service and its dependent components.

93.5.4 Minimum Greeting Response Time (ms)

Minimum Greeting Response Time is the shortest greeting response time across all instances, over the time period specified in the View Data field. Greeting response time is the length of time, in milliseconds, to hear the voice mail system greeting once the user has successfully logged in.

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 93–33 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Average OVF Minimum Greeting Response Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Recording Service instances, outage of one or more key components in the instances, contention of common resources (for instance, Oracle Internet Directory) among Recording Service instances, resource shortage among key components in the instances.

To investigate why the greeting response time exceeded the response time value set, check for alerts that may have been generated by the Recording Service or by specific instances of the Recording Service, the Routing Service, the Voicemail & Fax Application that this Recording Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific recording instances, you can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect contention for resources is affecting the components, review the resource usage of the Recording Service and its dependent components.

93.6 Recording Service Resource Usage Metrics

This category contains a set of related metrics that provide you with information about the CPU and Memory being used by the Recording Service. Its provides a snapshot of how the Recording Service instances are performing. If a particular metric is empty, a Recording Service instance is likely down and unavailable. Check the Up/Down status metric for all the Recording Service instances.

93.6.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the Recording service.

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 93–34 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
All Versions	Every 5 Minutes	After Every Sample	>	70	75	2	CPU Utilization of Recording Service, %target%, is %value%%

User Action

You can use this metric to determine if the Recording Service is using the most CPU on your system, thereby leading to high end-user response times. If the Recording Service

is consuming a large amount of CPU, consider changing the configuration settings to reduce the amount of CPU consumption. To investigate why the service is consuming a large amount of CPU, check for alerts that may have been generated by specific instances of the Recording Service, or by the Voicemail and Fax Application that this Recording Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or by the host computer.

93.6.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Recording Service.

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 93–35 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
All Versions	Every 5 Minutes	After Every Sample	>	80	90	2	Memory Utilization of Recording Service, %target%, is %value%%

User Action

You can use this metric to determine if the Recording Service is using the most memory on your system, thereby leading to high end-user response times. If the Recording Service is consuming a large amount of memory, consider changing the configuration settings to reduce the amount of memory consumption. To investigate why the Recording Service is consuming a large amount of memory, check for alerts that may have been generated by the Recording Service instances, or by the Voicemail and Fax Application that this Recording Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or by the host computer.

93.6.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Recording Service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Recording Service instance.

93.6.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.6.5 Status

This metric provides information about the Up/Down status of the Recording Service. It alerts you when the Recording Service is down. The Recording Service is considered down when all of the configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the Recording Service or by specific instances of the Recording Service, or by the Voicemail and Fax Application that this Recording Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or by the central agent on the host computer or by the host computer.

93.6.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.6.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

93.7 Recording Service Response

This category contains metrics that provide information about the Up/Down status of the Recording Service.

93.7.1 Status

This metric provides information about the Up/Down status of the Recording Service. It alerts you when the Recording Service is down. The Recording Service is considered down when all of the configured instances for this service are down.

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 93–36 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
All Versions	Every 5 Minutes	After Every Sample	=	Not Defined	0	1	Recording Service, %target%, is down

User Action

You can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the Recording Service or by specific instances of the Recording Service, or by the Voicemail and Fax Application that this Recording Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or by the central agent on the host computer or by the host computer.

94

Retrieval Service

This target represents the Retrieval Service. The Retrieval Service allows users to listen to, save, delete, reply to, and forward voice mail messages, set passwords, leave a voice mail for another user, and record and activate greetings. The Retrieval Service formulates the mail box number using the caller ID or prompts the voice mail user to enter a mail box number. The Retrieval Service verifies that the user is a valid voice mail user against the data stored in the Oracle Internet Directory. Once the user has been verified, the user is prompted for a password, and the voice mail system authenticates the password against the Oracle Internet Directory. Upon successful authentication, the Retrieval Service interacts with the Collaboration Suite Database to retrieve voice mail messages and other account information. A user who cannot be validated has the option to transfer to another users voice mail box by pressing the asterisk symbol during or after the prompt to enter the mail box number is played.

94.1 Raw Retrieval Instance Performance Metrics

This is for internal use only.

94.2 Retrieval Instance Performance Metrics

This category includes a set of metrics that provides summary information about the login response time, menu play time, and message play time for this instance of the Retrieval Service.

The login response time for a call is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count.

The menu play time is the length of time, in milliseconds, it takes to play the Message Menu after the message count is played.

The message play time is the length of time, in milliseconds, between the time the user chooses to hear the message and when the message starts playing.

Each retrieval instance can service one or more calls.

The login response time metrics are called *Calls with < range of response times > ms. Login Response Time*, and the message play time metrics are called *Calls with < range of response times > ms. Message Play Time*, where < *range of response times* > can range from 0 to 10000 milliseconds (ms), in increments of 500 milliseconds. For menu play time, the range is from 0 to 2000 milliseconds, in increments of 100 milliseconds.

The average, minimum, and maximum response times, as well as the number of calls engaging in the activity for this instance, are also reported.

94.2.1 Active Logins

Active Logins is the total number of calls where the user is in the process of logging in and is waiting to hear the message count. This total is calculated for all calls serviced by this instance, over the time period specified in the View Data field.

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 94–1 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	Not Defined	1	Active OVF Logins exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, go to the Retrieval Service home page, and click the *Add One Instance* button to increase the number of service instances.

94.2.2 Active Menu Play Calls

Active Menu Play Calls is the total number of calls where the message count has been played, and the user is waiting to hear the Message Menu. This total is calculated for all calls serviced by this instance, over the time period specified in the View Data field.

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 94–2 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	>	Not Defined	Not Defined	1	Active Message Menu actions exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, go to the Retrieval Service home page, and click the *Add One Instance* button to increase the number of service instances.

94.2.3 Active Message Play Calls

Active Message Play Calls is the total number of calls where the user has chosen to hear the message and is waiting for the message to start playing. This total is calculated for this instance, over the time period specified in the View Data field.

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 94–3 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	>	Not Defined	Not Defined	1	Active Message Play actions exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, go to the Retrieval Service home page, and click the *Add One Instance* button to increase the number of service instances.

94.2.4 Average Login Response Time (ms)

Average Login Response Time is the average login response time for this instance, over the time period specified in the View Data field. Login response time is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count.

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 94–4 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	>	Not Defined	Not Defined	1	Average OVF Login Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the login response time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.5 Average Menu Play Time (ms)

Average Menu Play Time is the average length of time this instance takes to play the Message Menu after the message count is played, over the time period specified in the View Data field. The time is measured in milliseconds.

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 94–5 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	>	Not Defined	Not Defined	1	OVF Menu Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the menu play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.6 Average Message Play Time (ms)

Average Message Play Time is the average message play time for this instance, over the time period specified in the View Data field. Message Play Time is the length of time between the time the user chooses to hear the message and when the message starts playing. The time is measured in milliseconds.

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 94–6 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	>	Not Defined	Not Defined	1	Average OVF Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the message play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.7 Host

Host name of system where retrieval instance is running.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.2.8 Maximum Login Response Time (ms)

Maximum Login Response Time is the longest login response time for this instance, over the time period specified in the View Data field. Login response time for a call is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count.

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 94–7 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Maximum OVF Login Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the login response time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.9 Maximum Menu Play Time (ms)

Maximum Menu Play Time is the longest time this instance takes to play the Message Menu after the message count is played over the time period specified in the View Data field. The time is measured in milliseconds.

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 94–8 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	After Every Sample	>	Not Defined	Not Defined	1	Maximum OVF Menu Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the menu play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.10 Maximum Message Play Time (ms)

Maximum Message Play Time is the longest message play time for this instance, over the time period specified in the View Data field. Message Play Time is the length of time between the time the user chooses to hear the message and the message starts playing. The time is measured in milliseconds.

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 94–9 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	After Every Sample	>	Not Defined	Not Defined	1	Maximum OVF Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the message play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the large average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.11 Minimum Login Response Time (ms)

Minimum Login Response Time is the shortest login response time for this instance, over the time period specified in the View Data field. Login response time for a call is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count.

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 94–10 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 5 Minutes	After Every Sample	<	Not Defined	Not Defined	1	Minimum OVF Login Response Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the login response time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.12 Minimum Menu Play Time (ms)

Minimum Menu Play Time is the shortest time this instance takes to play the Message Menu after the message count is played over the time period specified in the View Data field. The time is measured in milliseconds.

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 94–11 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 5 Minutes	After Every Sample	<	Not Defined	Not Defined	1	Minimum OVF Menu Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the menu play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.13 Minimum Message Play Time (ms)

Minimum Message Play Time is the shortest message play time for this instance, over the time period specified in the View Data field. Message Play Time is the length of time between the time the user chooses to hear the message and the message starts playing. The time is measured in milliseconds.

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 94–12 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 5 Minutes	After Every Sample	<	Not Defined	Not Defined	1	Minimum OVF Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the message play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by this instance of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contentionis affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.2.14 Name

Name of the metric.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.2.15 Number of Calls with 0-100 ms. Menu Play Time

This metric reports the number of calls with 0-100 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–13 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 0-100 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.16 Number of Calls with 0-500 ms. Login Response Time

This metric reports the number of calls with 0-500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–14 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 0-500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.17 Number of Calls with 0-500 ms. Message Play Time

This metric reports the number of calls with 0-500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–15 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 0-500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.18 Number of Calls with 1001-1100 ms. Menu Play Time

This metric reports the number of calls with 1001-1100 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–16 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1001-1100 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.19 Number of Calls with 1001-1500 ms. Login Response Time

This metric reports the number of calls with 1001-1500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–17 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1001-1500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.20 Number of Calls with 1001-1500 ms. Message Play Time

This metric reports the number of calls with 1001-1500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–18 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1001-1500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.21 Number of Calls with 101-200 ms. Menu Play Time

This metric reports the number of calls with 101-200 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–19 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 101-200 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.22 Number of Calls with 1101-1200 ms. Menu Play Time

This metric reports the number of calls with 1101-1200 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–20 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1101-1200 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.23 Number of Calls with 1201-1300 ms. Menu Play Time

This metric reports the number of calls with 1201-1300 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–21 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1201-1300 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.24 Number of Calls with 1301-1400 ms. Menu Play Time

This metric reports the number of calls with 1301-1400 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–22 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1301-1400 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.25 Number of Calls with 1401-1500 ms. Menu Play Time

This metric reports the number of calls with 1401-1500 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–23 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1401-1500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.26 Number of Calls with 1501-1600 ms. Menu Play Time

This metric reports the number of calls with 1501-1600 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–24 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1501-1600 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.27 Number of Calls with 1501-2000 ms. Login Response Time

This metric reports the number of calls with 1501-2000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–25 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1501-2000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.28 Number of Calls with 1501-2000 ms. Message Play Time

This metric reports the number of calls with 1501-2000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–26 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1501-2000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.29 Number of Calls with 1601-1700 ms. Menu Play Time

This metric reports the number of calls with 1601-1700 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–27 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1601-1700 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.30 Number of Calls with 1701-1800 ms. Menu Play Time

This metric reports the number of calls with 1701-1800 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–28 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1701-1800 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.31 Number of Calls with 1801-1900 ms. Menu Play Time

This metric reports the number of calls with 1801-1900 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–29 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1801-1900 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.32 Number of Calls with 1901-2000 ms. Menu Play Time

This metric reports the number of calls with 1901-2000 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–30 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 1901-2000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.33 Number of Calls with 2001-2500 ms. Login Response Time

This metric reports the number of calls with 2001-2500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–31 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 2001-2500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.34 Number of Calls with 2001-2500 ms. Message Play Time

This metric reports the number of calls with 2001-2500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–32 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 2001-2500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.35 Number of Calls with 201-300 ms. Menu Play Time

This metric reports the number of calls with 201-300 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–33 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 201-300 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.36 Number of Calls with 2501-3000 ms. Login Response Time

This metric reports the number of calls with 2501-3000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–34 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 2501-3000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.37 Number of Calls with 2501-3000 ms. Message Play Time

This metric reports the number of calls with 2501-3000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–35 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 2501-3000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.38 Number of Calls with 3001-3500 ms. Login Response Time

This metric reports the number of calls with 3001-3500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–36 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 3001-3500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.39 Number of Calls with 3001-3500 ms. Message Play Time

This metric reports the number of calls with 3001-3500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–37 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 3001-3500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.40 Number of Calls with 301-400 ms. Menu Play Time

This metric reports the number of calls with 301-400 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–38 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 301-400 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.41 Number of Calls with 3501-4000 ms. Login Response Time

This metric reports the number of calls with 3501-4000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–39 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 3501-4000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.42 Number of Calls with 3501-4000 ms. Message Play Time

This metric reports the number of calls with 3501-4000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–40 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 3501-4000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.43 Number of Calls with 4001-4500 ms. Login Response Time

This metric reports the number of calls with 4001-4500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–41 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 4001-4500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.44 Number of Calls with 4001-4500 ms. Message Play Time

This metric reports the number of calls with 4001-4500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–42 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 4001-4500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.45 Number of Calls with 401-500 ms. Menu Play Time

This metric reports the number of calls with 401-500 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–43 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	Not Defined	1	Calls with 401-500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.46 Number of Calls with 4501-5000 ms. Login Response Time

This metric reports the number of calls with 4501-5000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–44 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 4501-5000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.47 Number of Calls with 4501-5000 ms. Message Play Time

This metric reports the number of calls with 4501-5000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–45 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Calls with 4501-5000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.48 Number of Calls with 5001-5500 ms. Login Response Time

This metric reports the number of calls with 5001-5500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–46 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	Not Defined	1	Calls with 5001-5500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.49 Number of Calls with 5001-5500 ms. Message Play Time

This metric reports the number of calls with 5001-5500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–47 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	Not Defined	1	Calls with 5001-5500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.50 Number of Calls with 501-1000 ms. Login Response Time

This metric reports the number of calls with 501-1000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–48 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	Not Defined	1	Calls with 501-1000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.51 Number of Calls with 501-1000 ms. Message Play Time

This metric reports the number of calls with 501-1000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–49 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	Not Defined	1	Calls with 501-1000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.52 Number of Calls with 501-600 ms. Menu Play Time

This metric reports the number of calls with 501-600 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–50 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	Not Defined	1	Calls with 501-600 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.53 Number of Calls with 5501-6000 ms. Login Response Time

This metric reports the number of calls with 5501-6000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–51 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	Not Defined	1	Calls with 5501-6000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.54 Number of Calls with 5501-6000 ms. Message Play Time

This metric reports the number of calls with 5501-6000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–52 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	Not Defined	1	Calls with 5501-6000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.55 Number of Calls with 6001-6500 ms. Login Response Time

This metric reports the number of calls with 6001-6500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–53 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	Not Defined	1	Calls with 6001-6500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.56 Number of Calls with 6001-6500 ms. Message Play Time

This metric reports the number of calls with 6001-6500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–54 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	Not Defined	1	Calls with 6001-6500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.57 Number of Calls with 601-700 ms. Menu Play Time

This metric reports the number of calls with 601-700 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–55 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	Not Defined	1	Calls with 601-700 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.58 Number of Calls with 6501-7000 ms. Login Response Time

This metric reports the number of calls with 6501-7000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–56 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	Not Defined	1	Calls with 6501-7000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.59 Number of Calls with 6501-7000 ms. Message Play Time

This metric reports the number of calls with 6501-7000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–57 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	Not Defined	1	Calls with 6501-7000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.60 Number of Calls with 7001-7500 ms. Login Response Time

This metric reports the number of calls with 7001-7500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–58 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	Not Defined	1	Calls with 7001-7500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.61 Number of Calls with 7001-7500 ms. Message Play Time

This metric reports the number of calls with 7001-7500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–59 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	Not Defined	1	Calls with 7001-7500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.62 Number of Calls with 701-800 ms. Menu Play Time

This metric reports the number of calls with 701-800 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–60 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	Not Defined	1	Calls with 701-800 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.63 Number of Calls with 7501-8000 ms. Login Response Time

This metric reports the number of calls with 7501-8000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–61 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	Not Defined	1	Calls with 7501-8000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.64 Number of Calls with 7501-8000 ms. Message Play Time

This metric reports the number of calls with 7501-8000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–62 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	Not Defined	1	Calls with 7501-8000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.65 Number of Calls with 8001-8500 ms. Login Response Time

This metric reports the number of calls with 8001-8500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–63 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	Not Defined	1	Calls with 8001-8500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.66 Number of Calls with 8001-8500 ms. Message Play Time

This metric reports the number of calls with 8001-8500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–64 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	Not Defined	1	Calls with 8001-8500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.67 Number of Calls with 801-900 ms. Menu Play Time

This metric reports the number of calls with 801-900 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–65 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	Not Defined	1	Calls with 801-900 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.68 Number of Calls with 8501-9000 ms. Login Response Time

This metric reports the number of calls with 8501-9000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–66 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	Not Defined	1	Calls with 8501-9000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.69 Number of Calls with 8501-9000 ms. Message Play Time

This metric reports the number of calls with 8501-9000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–67 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	Not Defined	1	Calls with 8501-9000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.70 Number of Calls with 9001-9500 ms. Login Response Time

This metric reports the number of calls with 9001-9500 milliseconds login response times, collected for all calls serviced by this instance.

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 94–68 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	Not Defined	1	Calls with 9001-9500 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.71 Number of Calls with 9001-9500 ms. Message Play Time

This metric reports the number of calls with 9001-9500 milliseconds message play times, collected for all calls serviced by this instance.

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 94–69 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	Not Defined	1	Calls with 9001-9500 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.72 Number of Calls with 901-1000 ms. Menu Play Time

This metric reports the number of calls with 901-1000 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–70 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	Not Defined	1	Calls with 901-1000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.73 Number of Calls with 9501-10000 ms. Login Response Time

This metric reports the number of calls with 9501-10000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–71 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	Not Defined	1	Calls with 9501-10000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.74 Number of Calls with 9501-10000 ms. Message Play Time

This metric reports the number of calls with 9501-10000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–72 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	Not Defined	1	Calls with 9501-10000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.75 Number of Calls with over 10000 ms. Login Response Time

This metric reports the number of calls with over 10000 milliseconds login response times, collected for all calls serviced by this instance.

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 94–73 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	Not Defined	1	Calls with greater than 10000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.76 Number of Calls with over 10000 ms. Message Play Time

This metric reports the number of calls with over 10000 milliseconds message play times, collected for all calls serviced by this instance.

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 94–74 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	Not Defined	1	Calls with greater than 10000 ms Message Play Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.77 Number of Calls with over 2000 ms. Menu Play Time

This metric reports the number of calls with over 2000 milliseconds menu play times, collected for all calls serviced by this instance.

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 94–75 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	Not Defined	1	Calls with greater than 2000 ms Login Time exceeded.

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.2.78 Port Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.3 Retrieval Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Retrieval Service instance. It provides a snapshot of how the Retrieval Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Retrieval Service instance.

94.3.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Retrieval Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 94–76 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	>	70	75	2	CPU utilization of Retrieval Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Retrieval Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Retrieval Service instance, the Voicemail and Fax Application that this Retrieval Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

94.3.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.3.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Retrieval Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 94–77 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	>	80	90	2	Memory utilization of Retrieval Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Retrieval Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Retrieval Service instance, the Voicemail and Fax Application that this Retrieval Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

94.3.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Retrieval Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Retrieval Service instance.

94.3.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.3.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.3.7 Status

This metric provides information about the Up/Down status of the Retrieval Service instance and alerts you when the Retrieval Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 94–78 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	Retrieval Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Retrieval Service by selecting the Retrieval Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Retrieval Service instance, the Voicemail and Fax Application that this Retrieval Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

94.3.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.4 Retrieval Service Login Response Time Distribution

This metric reports the number of calls with login response times that fall within specified intervals, for example, the number of calls with a login response time of 0-500 milliseconds. "Number of Calls" is the calls reported for all instances during the collection interval. See the Number of Calls metric for additional details.

94.4.1 Number of Calls

This metric provides additional metrics on login response time for each specified interval.

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 94–79 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	Not Defined	1	Calls with Login Response Time range (ms) exceeded.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Login Response Time (ms)" object.

If warning or critical threshold values are currently set for any "Login Response Time (ms)" 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 "Login Response Time (ms)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.5 Retrieval Service Menu Play Time Distribution

This metric reports the number of calls with menu play times that fall within specified intervals, for example, the number of calls with a menu play time of 0-100 milliseconds. "Number of Calls" is the calls reported for all instances during the collection interval. See the Number of Calls metric for additional details.

94.5.1 Number of Calls

This metric provides additional information on menu play time for each specified interval.

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 94–80 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	Not Defined	1	Calls with Menu Play Response Time range (ms) exceeded.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Menu Play Time (ms)" object.

If warning or critical threshold values are currently set for any "Menu Play Time (ms)" 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 "Menu Play Time (ms)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.6 Retrieval Service Message Play Time Distribution

This metric reports the number of calls with message play times that fall within specified intervals, for example, the number of calls with a message play time of 0-500 milliseconds. "Number of Calls" is the calls reported for all instances during the collection interval. See the Number of Calls metric for additional details.

94.6.1 Number of Calls

This metric provides additional metrics on menu play time for each specified interval.

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 94–81 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	Not Defined	1	Calls with Message Play Response Time range (ms) exceeded.

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Message Play Time (ms)" object.

If warning or critical threshold values are currently set for any "Message Play Time (ms)" 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 "Message Play Time (ms)" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

94.7 Retrieval Service Performance Metrics

This category contains a set of metrics that provides summary information about the login response time, menu play time and message play time of all service instances in the Retrieval Service. The login response time for a call is the time is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count. The menu play time is the length of time, in milliseconds, it takes to play the Message Menu after the message count is played. The message play time is the length of time, in milliseconds, between the time the user chooses to hear the message and when the message starts playing. Each retrieval instance can service one or more calls. The average, minimum, and maximum response times, as well as the number of calls engaging in the activity for all instances are reported.

94.7.1 Active Logins

Active Logins is the total number of calls where the user is in the process of logging in and is waiting to hear the message count. This total is calculated for all instances over the time period specified in the View Data field.

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 94–82 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	Not Defined	1	Active OVF Logins exceeded.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, go to the Retrieval Service home page, and click the *Add One Instance* button to increase the number of service instances.

94.7.2 Active Menu Play Calls

Active Menu Play Calls is the total number of calls where the message count has been played, and the user is waiting to hear the Message Menu. This total is calculated for all instances, over the time period specified in the View Data field.

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 94–83 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	Not Defined	1	Active Message Menu actions exceeded.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, go to the Retrieval Service home page, and click the *Add One Instance* button to increase the number of service instances.

94.7.3 Active Message Play Calls

Active Message Play Calls is the total number of calls where the user has chosen to hear the message and is waiting for the message to start playing. This total is calculated for all instances over the time period specified in the View Data field.

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 94–84 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	Not Defined	1	Active Message Play actions exceeded.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, go to the Retrieval Service home page, and click the *Add One Instance* button to increase the number of service instances.

94.7.4 Average Login Response Time (ms)

Average Login Response Time is the average login response time for all instances, over the time period specified in the View Data field. Login response time is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count.

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 94–85 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	Not Defined	1	OVF Login Response Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the login response time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you

suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.7.5 Average Menu Play Time (ms)

Average Menu Play Time is the average length of time it takes to play the Message Menu after the message count is played, for all instances, over the time period specified in the View Data field. The time is measured in milliseconds.

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 94–86 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	Not Defined	1	OVF Menu Play Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the menu play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.7.6 Average Message Play Time (ms)

Average Message Play Time is the message play time, averaged across all instances, over the time period specified in the View Data field. Message Play Time is the length of time between the time the user chooses to hear the message and when the message starts playing. The time is measured in milliseconds.

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 94–87 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	Not Defined	1	OVF Message Play Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the message play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.7.7 Maximum Login Response Time (ms)

Maximum Login Response Time is the longest login response time across all instances, over the time period specified in the View Data field. Login response time for a call is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count.

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 94–88 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	Not Defined	1	Maximum OVF Login Response Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the login response time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.7.8 Maximum Menu Play Time (ms)

Maximum Menu Play Time is the longest time it takes to play the Message Menu after the message count is played, for all instances, over the time period specified in the View Data field. The time is measured in milliseconds.

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 94–89 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	Not Defined	1	Maximum OVF Menu Play Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the menu play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.7.9 Maximum Message Play Time (ms)

Maximum Message Play Time is the longest message play time for call serviced by all instances, over the time period specified in the View Data field. Message Play Time is the length of time between the time the user chooses to hear the message and the message starts playing. The time is measured in milliseconds.

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 94–90 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	Not Defined	1	Maximum OVF Message Play Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the message play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the

Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.7.10 Minimum Login Response Time (ms)

Minimum Login Response Time is the shortest login response time across all instances, over the time period specified in the View Data field. Login response time for a call is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count.

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 94–91 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	Not Defined	1	Minimum OVF Login Response Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the login response time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you

suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.7.11 Minimum Menu Play Time (ms)

Minimum Menu Play Time is the shortest time it takes to play the Message Menu after the message count is played, for all instances, over the time period specified in the View Data field. The time is measured in milliseconds.

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 94–92 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	Not Defined	1	Minimum OVF Menu Play Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the menu play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or by specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.7.12 Minimum Message Play Time (ms)

Minimum Message Play Time is the shortest message play time for calls serviced by all instances, over the time period specified in the View Data field. Message Play Time is the length of time between the time the user chooses to hear the message and the message starts playing. The time is measured in milliseconds.

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 94–93 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	Not Defined	1	Minimum OVF Message Play Time exceeded.

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the message play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to the outage of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home page of the components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

94.8 Retrieval Service Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Retrieval Service. It provides a snapshot of how the Retrieval Service instances are performing. If a particular metric is empty, it is likely that an Retrieval Service instance is down and unavailable. Check the Up/Down status metric for all the Retrieval Service instances.

94.8.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 94–94 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	>	70	75	2	CPU utilization of Retrieval Service, %target%, is %value%%

User Action

You can use this metric to determine if the Retrieval Service is using the most CPU on your system, thereby leading to high end-user response times. If the Retrieval Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Retrieval Service, the Voicemail and Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

94.8.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 94–95 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	>	80	90	2	Memory utilization of Retrieval Service, %target%, is %value%%

User Action

You can use this metric to determine if the Retrieval Service is using the most memory on your system and leading to high end-user response times. If the Retrieval Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption,

check for alerts that may have been generated by the following: the Retrieval Service instances, the Voicemail and Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

94.8.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Retrieval Service.

94.8.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.8.5 Status

This metric provides information about the Up/Down status of the Retrieval Service. The Retrieval Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Retrieval Service by selecting the Retrieval Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Retrieval Service or specific instances of the Retrieval Service, the Voicemail and Fax Application that this Retrieval Service is a member of (check for check the status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

94.8.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.8.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

94.9 Retrieval Service Response

This category contains metrics that provide information about the Up/Down status of the Retrieval Service.

94.9.1 Status

This metric provides information about the Up/Down status of the Retrieval Service and alerts you when the Retrieval Service is down. The Retrieval Service shows a status of Down when all configured instances for this service are down. By default, a critical threshold value is set for this metric. Alerts are 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 94–96 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	Retrieval Service, %target%, is down

User Action

You can restart the Retrieval Service by selecting the Retrieval Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Retrieval Service or specific instances of the Retrieval Service, the

Voicemail and Fax Application that this Retrieval Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

95

Routing Service

This target represents the Routing Service. The Routing Service routes calls to Oracle Voicemail and Fax services. When the Telephony Server receives a call from the PBX, the Routing Service answers the call. There are two ways in which the Routing Service gets handed calls: direct and forwarded. A direct call is one made directly to the voice mail system. A forwarded call is a call that is diverted to the voice mail system because the call was not answered or there is a busy signal. The Routing Service retrieves call detail information from the PBX including the callers phone number, the destination phone number, and how the call arrived at the voice mail system (direct or forwarded). If call detail information is unavailable, then the Routing Service allows the caller to choose voice mail recording, retrieval, or transfer to an attendant. For forwarded calls, the Routing Service checks the PBX-Application Clusters call routing map. If the calls destination number is listed in the call routing map, the call is handed off to the IVR (Interactive Voice Response) Service. All other forwarded calls are handed off to the Recording Service.

95.1 Routing Instance Performance Metrics

This category includes a set of metrics that provides information on the type of requests being handled by this routing instance.

95.1.1 Host

Host name of system where recording instance is running.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.1.2 Metric Name

Name of the metric.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.1.3 Port Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.1.4 Recording Requests

The recording requests is the number of requests to record voicemail messages that are being handled by this instance in the Routing Service.

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 95–1 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	Not Defined	1	OVF Recording Requests overload

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Routing Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

95.1.5 Retrieval Requests

The retrieval requests is the number of requests to retrieve voicemail messages that are being handled by this instance in the Routing Service.

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 95–2 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	>	Not Defined	Not Defined	1	OVF Retrieval Requests overload

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

No action is requied. If there is evidence that the service cannot keep up with the incoming call demand, return to the Routing Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

95.2 Routing Instance Resource Usage Metrics

This category includes a set of related metrics that provides you with information about the CPU and memory being used by the Routing Service instance. It provides a snapshot of how the Routing Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Routing Service instance.

95.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Routing Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 95–3 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	>	70	75	2	CPU utilization of Routing Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Routing Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Routing Service instance, the Voicemail and Fax Application that this Routing Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

95.2.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.2.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Routing Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 95–4 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	>	80	90	2	Memory utilization of Routing Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Routing Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Routing Service instance, the Voicemail and Fax Application that this Routing Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

95.2.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Routing Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Routing Service instance.

95.2.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.2.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.2.7 Status

This metric provides information about the Up/Down status of the Routing Service instance and alerts you when the Routing Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 95–5 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	=	Not Defined	0	1	Routing Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Routing Service by selecting the Routing Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Routing Service instance, the Voicemail and Fax Application that this Routing

Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

95.2.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.3 Routing Service Performance Metrics

This category includes a set of metrics that provides information on the type of requests being handled by all the instances in the Routing Service.

95.3.1 Total Recording Requests

The total recording requests is the number of requests to record voicemail messages that are being handled by all the instances in the Routing Service.

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 95–6 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	>	Not Defined	Not Defined	1	OVF Recording requests overload

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Routing Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

95.3.2 Total Retrieval Requests

The total retrieval requests is the number of requests to retrieve voicemail messages that are being handled by all instances in the Routing Service.

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 95–7 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	OVF Retrieval requests overload

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Routing Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

95.4 Routing Service Resource Usage Metrics

This category includes a set of related metrics that provides you with information about the CPU and memory being used by the Routing Service. It provides a snapshot of how the Routing Service instances are performing. If a particular metric is empty, it is likely that an Routing Service instance is down and unavailable. Check the Up/Down status metric for all the Routing Service instances.

95.4.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 95–8 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	After Every Sample	>	70	75	2	CPU utilization of Routing Service, %target%, is %value%%

User Action

You can use this metric to determine if the Routing Service is using the most CPU on your system, thereby leading to high end-user response times. If the Routing Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Routing Service, the Voicemail and Fax Application that this Routing Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

95.4.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 95–9 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	After Every Sample	>	80	90	2	Memory utilization of Routing Service, %target%, is %value%%

User Action

You can use this metric to determine if the Routing Service is using the most memory on your system and leading to high end-user response times. If the Routing Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Routing Service instances, the Voicemail and Fax Application that this Routing Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

95.4.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Routing Service.

95.4.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.4.5 Status

This metric provides information about the Up/Down status of the Routing Service. The Routing Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Routing Service by selecting the Routing Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Routing Service, specific instances of the Routing Service, the Voicemail and Fax Application that this Routing Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

95.4.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.4.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

95.5 Routing Service Response

This category includes metrics that provide information about the Up/Down status of the Routing Service.

95.5.1 Status

This metric provides information about the Up/Down status of the Routing Service and alerts you when the Routing Service is down. The Routing Service shows a status of Down when all configured instances for this service are down. By default, a critical threshold value is set for this metric. Alerts are 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 95–10 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 5 Minutes	After Every Sample	=	Not Defined	0	1	Routing Service, %target%, is down

User Action

You can restart the Routing Service by selecting the Routing Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Routing Service, specific instances of the Routing Service, the Voicemail and Fax Application that this Routing Service is a member of (check status of dependent components - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

96

SMDI Monitor Service

This target represents the SMDI (Simplified Message Desk Interface) Monitor Service. The SMDI Monitor Service provides an interface between SMDI-enabled PBXes and Oracle Voicemail and Fax. It processes call detail messages from the PBX and passes them to the Routing Service. It also receives MWI (Message Waiting Indicator) requests from the MWI Service and dispatches these requests to the PBX.

96.1 SMDI Monitor Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the SMDI Monitor Service instance. It provides a snapshot of how the SMDI Monitor Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the SMDI Monitor Service instance.

96.1.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the SMDI Monitor Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 96–1 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	>	70	75	2	CPU utilization of SMDI Monitor Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the SMDI Monitor Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the SMDI Monitor Service instance, the Voicemail and Fax Application that this SMDI Monitor Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

96.1.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

96.1.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the SMDI Monitor Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 96–2 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	>	80	90	2	Memory utilization of SMDI Monitor Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this SMDI Monitor Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the SMDI Monitor Service instance, the Voicemail and Fax Application that this SMDI Monitor Service instance is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

96.1.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the SMDI Monitor Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the SMDI Monitor Service instance.

96.1.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

96.1.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

96.1.7 Status

This metric provides information about the Up/Down status of the SMDI Monitor Service instance and alerts you when the SMDI Monitor Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 96–3 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	=	Not Defined	0	1	SMDI Monitor Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the SMDI Monitor Service by selecting the SMDI Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the SMDI Monitor Service instance, the Voicemail and Fax Application that this SMDI Monitor Service instance is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

96.1.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

96.2 SMDI Monitor Service Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the SMDI Monitor Service. It provides a snapshot of how the SMDI Monitor Service instances are performing. If a particular metric is empty, it is likely that an SMDI Monitor Service instance is down and unavailable. Check the Up/Down status metric for all the SMDI Monitor Service instances.

96.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 96–4 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	>	70	75	2	CPU utilization of SMDI Monitor Service, %target%, is %value%%%

User Action

You can use this metric to determine if the SMDI Monitor Service is using the most CPU on your system, thereby leading to high end-user response times. If the SMDI Monitor Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the SMDI Monitor Service, the Voicemail and Fax Application that this SMDI Monitor Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

96.2.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 96–5 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	>	80	90	2	Memory utilization of SMDI Monitor Service, %target%, is %value%%%

User Action

You can use this metric to determine if the SMDI Monitor Service is using the most memory on your system and leading to high end-user response times. If the SMDI Monitor Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the SMDI Monitor Service instances, the Voicemail and Fax Application that this SMDI Monitor Service is a member of (check the status of dependent components - Internet Directory, Telephony Server), or the host computer.

96.2.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the SMDI Monitor Service.

96.2.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

96.2.5 Status

This metric provides information about the Up/Down status of the SMDI Monitor Service. The SMDI Monitor Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the SMDI Monitor Service by selecting the SMDI Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the SMDI Monitor Service, specific instances of the SMDI Monitor Service, the Voicemail and Fax Application that this SMDI Monitor Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

96.2.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

96.2.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

96.3 SMDI Monitor Service Response

This category contains metrics that provide information about the Up/Down status of the SMDI Monitor Service.

96.3.1 Status

This metric provides information about the Up/Down status of the SMDI Monitor Service and alerts you when the SMDI Monitor Service is down. The SMDI Monitor Service shows a status of Down when all configured instances for this service are down. By default, a critical threshold value is set for this metric. Alerts are 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 96–6 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	=	Not Defined	0	1	SMDI Monitor Service, %target%, is down

User Action

You can restart the SMDI Monitor Service by selecting the SMDI Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the SMDI Monitor Service, specific instances of the SMDI Monitor Service, the Voicemail and Fax Application that this SMDI Monitor Service is a member of (check for dependent component status - Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

97

Telephony Monitor Service

This target represents the Telephony Monitor Service. The Telephony Monitor Service monitors the Telephony Server and reports the status and some key metrics of the Telephony Server to the Enterprise Manager. It periodically checks the status of the Telephony Server and the number of active calls handled by the server.

97.1 Telephony Instance Performance Metrics

This category includes a set of metrics that provides information about the status of this Telephony Server instance as well as the number of current and total telephony calls serviced by this Telephony Server instance.

97.1.1 Current Number of Calls

The current number of calls is the concurrent number of telephony calls handled by this Telephony Server instance, over the time period specified in the View Data field.

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 97–1 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	Not Defined	1	Current Calls overload

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Telephony Monitor Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

97.1.2 Host

Host name of system where Telephony Server instance is running.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.1.3 Metric Name

Name of the metric.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.1.4 Port Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.1.5 Telephony Server Instance Status

This metric provides information about the Up/Down status of the Telephony Server instance. The Telephony Server instance shows a status of Down when the instance for this service is down.

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 97–2 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	=	Not Defined	0	1	Telephony Server Instance Is Down

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

97.1.6 Total Number of Calls

The total number of calls is the total number of telephony calls handled by this Telephony Server instance, since the instance was started, over the time period specified in the View Data field.

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 97–3 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	>	Not Defined	Not Defined	1	Total Calls overload

Multiple Thresholds

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

If warning or critical threshold values are currently set for any "Process 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 "Process Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Telephony Monitor Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

97.2 Telephony Monitor Instance Resource Usage Metrics

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Telephony Monitor Service instance. It provides a snapshot of how the Telephony Monitor Service instance is performing. If a particular metric is empty, it is likely that the service instance is down and unavailable. Check the Up/Down status metric of the Telephony Monitor Service instance.

97.2.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for this instance of the Telephony Monitor Service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 97–4 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	>	70	75	2	CPU utilization of Telephony Monitor Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if the Telephony Monitor Service instance is using the most CPU on your system, thereby leading to high end-user response times. If the service instance is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the Telephony Monitor Service instance, the Voicemail and Fax Application that this Telephony Monitor Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

97.2.2 Instance Number

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.2.3 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Telephony Monitor Service instance. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 97–5 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	>	80	90	2	Memory utilization of Telephony Monitor Instance, %target% (%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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can use this metric to determine if this Telephony Monitor Service instance is using the most memory on your system and leading to high end-user response times. If the service instance is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Telephony Monitor Service instance, the Voicemail and Fax Application that this Telephony Monitor Service instance is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

97.2.4 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Telephony Monitor Service instance.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Telephony Monitor Service instance.

97.2.5 Process ID

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.2.6 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.2.7 Status

This metric provides information about the Up/Down status of the Telephony Monitor Service instance and alerts you when the Telephony Monitor Service instance is down. If the status is down, it could mean that the service instance is in the process of starting up, or it is not responding to process management heartbeat checks. By default, a critical threshold value is set for this metric. Alerts are 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 97–6 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	=	Not Defined	0	1	Telephony Monitor Instance, %target% (%Name%), is down

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. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

You can restart the Telephony Monitor Service by selecting the Telephony Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the instance is down, check for alerts that may have been generated by the following: the Telephony Monitor Service instance, the Voicemail and Fax Application that this Telephony Monitor Service instance is a member of (check the dependent component status - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

97.2.8 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.3 Telephony Monitor Service Resource Usage Metrics

This category includes a set of related metrics that provides you with information about the CPU and memory being used by the Telephony Monitor Service. It provides a snapshot of how the Telephony Monitor Service instances are performing. If a particular metric is empty, it is likely that a Telephony Monitor Service instance is down and unavailable. Check the Up/Down status metric for all the Telephony Monitor Service instances.

97.3.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for all the instances of the service. By default, a critical and warning threshold value is set for this metric. Alerts are 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 97–7 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 5 Minutes	After Every Sample	>	70	75	2	CPU utilization of Telephony Monitor Service, %target%, is %value%%%

User Action

You can use this metric to determine if the Telephony Monitor Service is using the most CPU on your system, thereby leading to high end-user response times. If the Telephony Monitor Service is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: the specific instances of the Telephony Monitor Service, the Voicemail and Fax Application that this Telephony Monitor Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

97.3.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the service. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 97–8 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	After Every Sample	>	80	90	2	Memory utilization of Telephony Monitor Service, %target%, is %value%%%

User Action

You can use this metric to determine if the Telephony Monitor Service is using the most memory on your system and leading to high end-user response times. If the

Telephony Monitor Service is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: the Telephony Monitor Service instances, the Voicemail and Fax Application that this Telephony Monitor Service is a member of (check the status of dependent components - Oracle Internet Directory, Telephony Server), or the host computer.

97.3.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the service.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Telephony Monitor Service.

97.3.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.3.5 Status

This metric provides information about the Up/Down status of the Telephony Monitor Service. The Telephony Monitor Service shows a status of Down when all configured instances for this service are down.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Telephony Monitor Service by selecting the Telephony Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Telephony Monitor Service, specific instances of the Telephony Monitor Service, the Voicemail and Fax Application that this Telephony Monitor Service is a member of (check the dependent component status - Oracle

Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

97.3.6 Total Instances

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.3.7 Up Time (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

97.4 Telephony Monitor Service Response

This category includes metrics that provide information about the Up/Down status of the Telephony Monitor Service.

97.4.1 Status

This metric provides information about the Up/Down status of the Telephony Monitor Service and alerts you when the Telephony Monitor Service is down. The Telephony Monitor Service shows a status of Down when all configured instances for this service are down. By default, a critical threshold value is set for this metric. Alerts are 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 97–9 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	After Every Sample	=	Not Defined	0	1	Telephony Monitor Service, %target%, Is Down

User Action

You can restart the Telephony Monitor Service by selecting the Telephony Monitor Service target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by the following: the Telephony Monitor Service, specific instances of the Telephony Monitor Service, the Voicemail and Fax Application that this Telephony Monitor Service is a member of (check the dependent component status - Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

97.5 Telephony Service Performance Metrics

This category includes a set of metrics that provides summary information about the status of the Telephony Server instances as well as the number of current and total telephony calls serviced by the Telephony Server instances.

97.5.1 Current Number of Calls

The current number of calls is the number of concurrent telephony calls handled by all the Telephony Server instances over the time period specified in the View Data field.

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 97–10 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Current Calls overload

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Telephony Monitor Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

97.5.2 Telephony Server Service Status

This metric provides information about the Up/Down status of the Telephony Server Service. The Telephony Server Service shows a status of Down when all configured instances for this service are down.

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 97–11 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 5 Minutes	After Every Sample	=	Not Defined	0	1	Telephony Server Service Is Down

97.5.3 Total Number of Calls

The total number of calls is the total number of telephony calls handled by all the Telephony Server instances, since the instances were started, over the time period specified in the View Data field.

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 97–12 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Total Calls overload

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Telephony Monitor Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

98

Voicemail and Fax

This target represents the Voicemail and Fax component. The Voicemail and Fax Component is the highest level of the Oracle Voicemail and Fax deployment. An Oracle Collaboration Suite (OCS) deployment has one Voicemail and Fax component. There may be multiple OCS deployments and, therefore, multiple Voicemail and Fax components being managed by Enterprise Manager Grid Control. Each component would be configured against a separate Oracle Internet Directory. An example of this is an ISP deployment with multiple versions of Oracle Voicemail and Fax running. The components in the hierarchy are rolled up into the Voicemail and Fax component. It is an abstraction of the Voicemail and Fax system and related Oracle Collaboration Suite dependencies such as the Collaboration Suite Databases and Oracle Internet Directory.

From the Voicemail and Fax component level, you can drill down to each of the following levels in the hierarchy:

- PBX-Application Clusters that define a relationship between a Voicemail and Fax Application and one or more PBXes
- Voicemail and Fax Applications that support a PBX-Application Cluster
- Each of the 11 services that comprise a Voicemail and Fax Application

From the Voicemail and Fax component level, you can get an overview of the system and how it is performing. For example, you can see which PBX-Applications Clusters are performing poorly. You can find out if the Oracle Collaboration Suite dependencies such as the Collaboration Suite Databases or the Oracle Internet Directory are up or down. You can start at the component level and identify trouble areas, then drill down into the hierarchy to identify more specifically where the problem lies. You perform system-level tasks such as managing users, creating groups and sites, and setting system-wide defaults. You can manage any of the subcomponents of the Voicemail and Fax component, including starting, stopping, restarting, and reloading.

98.1 Voicemail and Fax Response

This category contains metrics that provide information about the Up/Down status of the Voicemail and Fax component.

98.1.1 Status

This metric provides information about the Up/Down status of the Voicemail and Fax component. It alerts you when the Voicemail and Fax target is down. The Voicemail and Fax target is considered down when any of its member targets, that is, any one of its PBX-Application Cluster targets, is down. The evaluation of this metric is triggered whenever there is a change in the Up/Down status of any of its member targets. The alert message for the status of the Voicemail and Fax target lists the members, followed

by their state. The possible states are: Up, Down, Unreachable, Blackout, Agent Down, Metric Error, and Status Pending.

Metric Summary

The following table shows how this metric is evaluated and the alerts that get generated.

Target Version	Evaluation and Collection Frequency	Alert Text	Alert Example
All Versions	Every time there is a change in the Response Status of its member targets	Members status --> %Non-zero count of members% Up; %Non-zero count of members% Down; %Non-zero count of members% Unreachable; %Non-zero count of members% Blackout; %Non-zero count of members% Agent Down; %Non-zero count of members% Metric Error; %Non-zero count of members% Status Pending;	Members status --> 1 Up; 3 Status Pending;

User Action

The status of the Voicemail and Fax target is dependent on the status of its members. To investigate why the Voicemail and Fax target is down, check for alerts that may have been generated by its member targets, that is, the PBX-Application Clusters.

99

Voicemail and Fax Application

This target represents the Voicemail and Fax Application. A Voicemail and Fax Application is a set of services running on a host. There is one application per Telephony Server. The services are: Routing, Retrieval, Recording, Call Transfer, Message Delivery Monitor, Message Recovery, Telephony Monitor, SMDI (Simplified Message Desk Interface) Monitor, MWI (Message Waiting Indicator), IVR (Interactive Voice Response), and Fax Receiving. You may have multiple Voicemail and Fax Applications associated with a PBX-Application Cluster. You might require more than one Voicemail and Fax Application, for example, if a PBX requires more ports than one Telephony Server can support. From the Voicemail and Fax Application level, you get an overview of the status and performance of this application. The Voicemail and Fax Application inherits its properties from the global process settings set at the Voicemail and Fax component level and passes those settings on to its services. These settings can be overridden at the application level.

99.1 Collaboration Suite Database Availablity

This category includes a set of metrics that provides information about the Up/Down status of the Collaboration Suite Database and the name of the host system where the Voicemail & Fax Application communicating with that database resides.

The Oracle Voicemail & Fax services process incoming calls and store the voice mail and fax messages recorded in each call in the called party's account in the Collaboration Suite Database.

99.1.1 Collaboration Suite Database Status

This metric provides information about the Up/Down status of the Collaboration Suite Database which stores the voice mail and fax messages for users. It alerts you when the Collaboration Suite Database is down.

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 99–1 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	Collaboration Suite Database is inaccessible

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Collaboration Suite Database Name" object.

If warning or critical threshold values are currently set for any "Collaboration Suite Database 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 "Collaboration Suite Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

If the Collaboration Suite Database is down, restart the database. Otherwise, restore connectivity between the Oracle Voicemail & Fax Application host and the Collaboration Suite Database named.

99.1.2 OVF Host Name

Host name of system where the the Voicemail & Fax Application is running. The application stores and retrieves voice mail and fax messages from the Collaboration Suite Database named.

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 99–2 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	=	Not Defined	Not Defined	1	Incorrect Accessing Host Name

Multiple Thresholds

For this metric you can set different warning and critical threshold values for each "Collaboration Suite Database Name" object.

If warning or critical threshold values are currently set for any "Collaboration Suite 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 "Collaboration Suite Name" object, use the Edit Thresholds page. See Editing Thresholds for information on accessing the Edit Thresholds page.

User Action

If the Oracle Voicemail & Fax Application host is down, bring up the host.

99.2 Voicemail and Fax Application Availability Metrics

This category includes a set of metrics that provides the availability status of key features supported by the Oracle Voicemail & Fax Applications and its key dependent components in the Oracle Collaboration Suite.

This category provides information on the ability of Oracle Voicemail & Fax Applications to accept inbound faxes and to handle the recording and retrieval of voice mail and fax messages. In addition, the status of key dependent compoments in the Oracle Collaboration Suite (Collaboration Suite Database and Oracle Internet Directory) are also provided.

The Oracle Voicemail & Fax services process incoming calls based on profile and context information stored in the Oracle Internet Directory and stores the voice mail and fax messages recorded in each call in the called party's account in the Collaboration Suite Database.

The status of the Telephony Server is reported on the Voicemail & Fax Application Home page. Details on the status over various periods of time is reported in the All Metrics page of the Telephony Monitor Service.

99.2.1 Collaboration Suite Database Accessible

This metric provides information about the Up/Down status of the Collaboration Suite Database which stores the voice mail and fax messages for users. It alerts you when the Collaboration Suite Database is down.

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 99–3 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	=	Not Defined	0	1	Not all Collaboration Suite Database(s) accessible

User Action

If the Collaboration Suite Database is down, restart the database. Otherwise, restore connectivity between the Oracle Voicemail & Fax Application host and the Collaboration Suite Database named.

99.2.2 Inbound Fax Feature Available

The inbound fax feature is reported as available (status is Up) on the All Metrics page if at least one instance of each of the key Voicemail & Fax Application Services (Fax Receiving, Telephony Monitor, Routing) is Up. It is assumed that Oracle Internet

Directory and all Collaboration Suite Databases used by the Application Services are Up.

Note that for the retrieval feature to be reported as available (status is Up) on the Oracle Voicemail & Fax Application home page, all the above conditions in the All Metrics page must hold. In addition, if SMDI is enabled, at least one instance of SMDI Monitor Service in each PBX-Application Cluster must be up.

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 99–4 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	=	Not Defined	0	1	Inbound Fax Feature is unavailable

User Action

Check to see that at least one instance of each of the key Voicemail & Fax Application Services (Fax Receiving, Telephony Monitor, Routing) is Up. It is assumed that Oracle Internet Directory and all Collaboration Suite Databases used by the Application Services are Up.

You can restart a particular service by selecting that service target and clicking Restart on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by that service or specific instances of the service, by the Voicemail & Fax Application that this Fax Receiving Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), by the central agent on the host computer, or by the host computer.

99.2.3 Oracle Internet Directory Accessible

This metric provides information about the Up/Down status of the Oracle Internet Directory. It alerts you when the Oracle Internet Directory is down.

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 99–5 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	=	Not Defined	0	1	Oracle Internet Directory inaccessible

User Action

If the Oracle Internet Directory is down, restart the Oracle Internet Directory database and its services. Otherwise, restore accessibility of Oracle Internet Directory service for the Oracle Voicemail & Fax Application.

99.2.4 Recording Feature Available

The recording feature is reported as available (status is Up) on the All Metrics page if at least one instance of each of the key Voicemail & Fax Application services (Recording, Telephony Monitor, Routing) is Up. It is assumed that Oracle Internet Directory and all Collaboration Suite Databases used by the Application Services are Up.

Note that for the recording feature to be reported as available (status is Up) on the Oracle Voicemail & Fax Application home page, all the above conditions in the All Metrics page must hold. In addition, if SMDI is enabled, at least one instance of SMDI Monitor Service in each PBX-Application Cluster must be up.

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 99–6 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	=	Not Defined	0	1	Recording Feature is unavailable

User Action

Check to see that at least one instance of each of the key Voicemail & Fax Application services (Recording, Telephony Monitor, Routing) is Up. If SMDI is enabled, check to see that at least one instance of SMDI Monitor Service is Up.

You can restart a particular service by selecting that service target and clicking Restart on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by that service or specific instances of the service, by the Voicemail & Fax Application that this Recording Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), by the central agent on the host computer, or by the host computer.

99.2.5 Retrieval Feature Available

The retrieval feature is reported as available (status is Up) on the All Metrics page if at least one instance of each of the key Voicemail & Fax Application Services (Retrieval, Telephony Monitor, Routing) is Up, and Oracle Internet Directory and all Collaboration Suite Databases used by the Application Services are Up.

Note that for the retrieval feature to be reported as available (status is Up) on the Oracle Voicemail & Fax Application home page, all the above conditions for All

Metrics page must be true. In addition, if SMDI is enabled, at least one instance of SMDI Monitor Service in each PBX-Application Cluster must be up.

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 99–7 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 5 Minutes	After Every Sample	=	Not Defined	0	1	Retrieval Feature is unavailable

User Action

Check to see that at least one instance of each of the key Voicemail & Fax Application Services (Retrieval, Telephony Monitor, Routing) is Up, and Oracle Internet Directory and all Collaboration Suite Databases used by the Application Services are Up.

You can restart a particular service by selecting that service target and clicking Restart on the Oracle Voicemail and Fax home page. To investigate why the service is down, check for alerts that may have been generated by that service or specific instances of the service, by the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), by the central agent on the host computer, or by the host computer.

99.3 Voicemail and Fax Application Performance Metrics

This category includes a set of metrics that provides information on the average performance and capacity of all services in this Voicemail & Fax Application.

In terms of performance, this category reports the average greeting response time for all Recording Service instances, as well as the average login response time, average menu play time, average message play time, and average message delivery time for all Retrieval Service instances in this Voicemail & Fax Application.

In terms of capacity, this category reports the total number of concurrent calls handled by all Retrieval, Recording and Fax Receiving Service instances in this Voicemail & Fax Application. In addition, this category also reports the total number of calls handled by all service instances in this Voicemail & Fax Application since the systems were first started up.

99.3.1 Average Greeting Response Time (ms)

Average Greeting Response Time is the average greeting response time for this Voicemail and Fax Application, over the time period specified in the View Data field. Greeting response time is the length of time, in milliseconds, to hear the voice mail system greeting once the user has successfully logged in.

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 99–8 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	After Every Sample	>	Not Defined	Not Defined	1	Greeting Response Time exceeded

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Recording Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Recording Service instances, and resource shortage among key components in the instances.

To investigate why the greeting response time exceeded the response time value set, check for alerts that may have been generated by the Recording Service or specific instances of the Recording Service, the Routing Service, the Voicemail & Fax Application that this Recording Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific recording instances, you can restart the Recording Service by selecting the Recording Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect resource contention is affecting components, review the resource usages of the Recording Service and its dependent components.

99.3.2 Average Login Response Time (ms)

Average Login Response Time is the average login response time for this Voicemail and Fax Application, over the time period specified in the View Data field. Login response time is the length of time, in milliseconds, between the time the password is accepted and the voice mail system responds with the message count.

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 99–9 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	After Every Sample	>	Not Defined	Not Defined	1	Login Response Time exceeded

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the login response time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent component -- Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

99.3.3 Average Menu Play Time (ms)

Average Menu Play Time is the average length of time it takes to play the Message Menu after the message count is played, for this Voicemail and Fax Application, over the time period specified in the View Data field. The time is measured in milliseconds.

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 99–10 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Menu Play Time exceeded

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more

key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the menu play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or by the host computer.

If you suspect that the cause of the high average response time is due to outages of specific retrieval instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Retrieval Service and its dependent components.

99.3.4 Average Message Delivery Time (s)

Average Message Delivery Time is the average message delivery time for this Voicemail and Fax Application, over the time period specified in the View Data field. Message delivery time is the time, in seconds, it takes to deliver a message to the mail box.

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 99–11 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Message Delivery Time exceeded

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Message Delivery Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Message Delivery Service instances, and resource shortages among key components in the instances.

To investigate why the message delivery time exceeded the response time value set, check for alerts that may have been generated by the Message Delivery Service or specific instances of the Message Delivery Service, by the Voicemail & Fax Application that this Message Delivery Service is a member of (check the status of dependent components -- Oracle Internet Directory, Collaboration Suite Databases, Telephony Server), by the central agent on the host computer, or by the host computer.

If you suspect that the cause of the high average response time is due to outages of specific Message Delivery Service instances, you can restart the Message Delivery Service by selecting the Message Delivery Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect resource contention is affecting the components, review the resource usage of the Message Delivery Service and its dependent components.

99.3.5 Average Message Play Time (ms)

Average Message Play Time is the message play time for this Voicemail and Fax Application over the time period specified in the View Data field. Message Play Time is the length of time between the time the user chooses to hear the message and when the message starts playing. The time is measured in milliseconds.

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 99–12 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 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Message Play Time exceeded

User Action

Performance degradation can result from one or more causes, including but not limited to: outage of one or more Retrieval Service instances, outage of one or more key components in the instances, contention for common resources (for example, Oracle Internet Directory) among Retrieval Service instances, and resource shortage among key components in the instances.

To investigate why the message play time exceeded the response time value set, check for alerts that may have been generated by the Retrieval Service or specific instances of the Retrieval Service, the Routing Service, the Collaboration Suite Databases, the Voicemail & Fax Application that this Retrieval Service is a member of (check the status of dependent components -- Oracle Internet Directory, Telephony Server, Collaboration Suite Databases), the central agent on the host computer, or the host computer.

If you suspect that the cause of the high average response time is due to outages of specific Retrieval Service instances, you can restart the Retrieval Service by selecting the Retrieval Service target and clicking Restart on the Oracle Voicemail & Fax home page.

If you suspect that outages of other key components are affecting performance, navigate to the home pages of those components to view their Up/Down status. If you suspect resource contention is affecting components, review the resource usage of the Retrieval Service and its dependent components.

99.3.6 Number of Active Calls

The current number of calls is the number of concurrent telephony calls handled by all the Telephony Server instances over the time period specified in the View Data field.

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 99–13 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Current Calls overload

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Telephony Monitor Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

99.3.7 Total Number of Calls

The total number of calls is the total number of telephony calls handled by all the Telephony Server instances, since the instances were started, over the time period specified in the View Data field.

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 99–14 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
All Versions	Every 5 Minutes	After Every Sample	>	Not Defined	Not Defined	1	Total Calls overload

User Action

No action is required. If there is evidence that the service cannot keep up with the incoming call demand, return to the Telephony Monitor Service home page, click the *Add One Instance* button to increase the number of service instances that can handle the calls.

99.4 Voicemail and Fax Application Resource Usage

This category includes a set of related metrics that provide you with information about the CPU and memory being used by the Voicemail and Fax Application. It provides a snapshot of how the Voicemail and Fax Application is performing. If a particular metric is empty, it is likely that the Voicemail and Fax Application is down and unavailable. Check the Up/Down status metric for the application, its services, and their instances.

99.4.1 CPU Usage (%)

This metric represents the percentage of the host CPU recorded for the Voicemail and Fax Application. By default, a critical and warning threshold value is set for this metric. Alerts are 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 99–15 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
All Versions	Every 5 Minutes	After Every Sample	>	70	75	2	CPU utilization of Voicemail and Fax Application, %target%, is %value%%%

User Action

You can use this metric to determine if the Voicemail and Fax Application is using the most CPU on your system, thereby leading to high end-user response times. If the Voicemail and Fax Application is consuming a large amount of CPU, consider changing the configuration settings to reduce the CPU consumption. To investigate the cause of the CPU consumption, check for alerts that may have been generated by the following: Voicemail and Fax Application's member services and their instances, the central agent on the host computer, or the host computer. Also, check the status of dependent components - Oracle Internet Directory, Telephony Server.

99.4.2 Memory Usage (%)

This metric shows you the percentage of host memory being used by the Voicemail and Fax Application. By default, a critical and warning threshold value is set for this metric column. Alerts are 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 99–16 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
All Versions	Every 5 Minutes	After Every Sample	>	80	90	2	Memory utilization of Voicemail and Fax Application, %target%, is %value%%%

User Action

You can use this metric to determine if the Voicemail and Fax Application is using the most memory on your system and leading to high end-user response times. If the Voicemail and Fax Application is consuming a large amount of memory, consider changing the configuration settings to reduce memory consumption. To investigate the cause of the memory consumption, check for alerts that may have been generated by the following: Voicemail and Fax Application's member services and their instances, the central agent on the host computer, or the host computer. Also, check the status of dependent components - Oracle Internet Directory, Telephony Server.

99.4.3 Memory Usage (MB)

This metric represents the memory usage (in megabytes) for the Voicemail and Fax Application

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

Compare this metric with Memory Usage (%), which measures the percentage of host memory being used by the Voicemail and Fax Application.

99.4.4 Start Time (ms since epoch)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

99.4.5 Status

This metric provides information about the Up/Down status of the Voicemail and Fax Application and alerts you when the application is down. The Voicemail and Fax Application shows a status of Down when any one of the enabled services for this application is down. If the status is down, it could mean that the services instances configured for this application are in the process of starting up, or they are not responding to process management heartbeat checks. By default, a critical threshold

value is set for this metric. Alerts are 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.

Target Version	Collection Frequency
All Versions	Every 5 Minutes

User Action

You can restart the Voicemail and Fax Application by selecting the Voicemail and Fax Application target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the target is down, check for alerts that may have been generated by the following: Voicemail and Fax Application's member services and their instances, the central agent on the host computer, or the host computer. Also, check the status of dependent components - Oracle Internet Directory, Telephony Server.

99.4.6 Uptime (ms)

This metric is for internal use only.

Metric Summary

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

Target Version	Collection Frequency
All Versions	Every 5 Minutes

99.5 Voicemail and Fax Application Response

This category includes metrics that provide information about the Up/Down status of the Voicemail and Fax Application.

99.5.1 Status

This metric provides information about the Up/Down status of the Voicemail and Fax Application and alerts you when the application is down. The Voicemail and Fax Application shows a status of Down when any one of the enabled services for this application is down. By default, a critical threshold value is set for this metric. Alerts are 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 99–17 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 5 Minutes	After Every Sample	=	Not Defined	0	1	Voicemail and Fax Application, %target%, is down

User Action

You can restart the Voicemail and Fax Application by selecting the Voicemail and Fax Application target and clicking on the Restart button on the Oracle Voicemail and Fax home page. To investigate why the target is down, check for alerts that may have been generated by the following: Voicemail and Fax Application's member services and their instances, the central agent on the host computer, or the host computer. Also, check the status of dependent components - Oracle Internet Directory, Telephony Server.

100

Voicemail and Fax Fax Service

The Voicemail and Fax Fax Service monitors the availability, performance, and usage of the Fax functionality.

100.1 Response

The Response category checks and displays whether or not the Voicemail and Fax Fax Service is available. Its status is based on the status of all Voicemail and Fax Fax Services. The Voicemail and Fax Fax Service is available only when all these services are available.

100.1.1 Status

This metric shows whether or not the Voicemail and Fax Fax Service is available.

User Action

If the Status of Voicemail and Fax Fax Service is not up, then check the results obtained by the Root Cause Analysis on the Voicemail and Fax Fax Service Home Page.

101

Voicemail and Fax Service

The Voicemail and Fax Service target is a grouping of the Fax Service, Recording Service, and Retrieval Service that are accessed by general users.

101.1 Activity Total

The Activity Total Time category includes information about total retrieval calls for the last 5 minutes and total recordings for the last 5 minutes.

101.1.1 Total Recordings (last 5 minutes)

This metric displays information about the number of users performing recording activity for the last five minutes across all the recording servers of the Voicemail and Fax service.

101.1.2 Total Retrieval Calls (last 5 minutes)

This metric displays information about the number of users performing the retrieval activity for the last five minutes across all the retrieval servers of the Voicemail and Fax service.

101.2 Response

The Response category checks and displays whether or not the Voicemail and Fax Service is available. Its status is based on the status of all Voicemail and Fax Services. The Voicemail and Fax Service is available only when all these services are available.

101.2.1 Status

User Action

If the Status of Voicemail and Fax Service is down, then check the results obtained by the Root Cause Analysis on the Voicemail and Fax Service Home Page.

102

Voicemail and Fax Recording Service

The Voicemail and Fax Recording Service monitors the availability, performance, and usage of the recording functionality.

102.1 Activity Total

The Activity Total shows information about total recording activity for the last 5 minutes.

102.1.1 Total Recording Calls (last 5 minutes)

This metric displays information about the number of users performing recording activity for the last five minutes across all the recording servers of the Voicemail and Fax service.

102.2 Response

The Response category checks and displays whether or not the Voicemail and Fax Recording Service is available. Its status is based on the status of all Voicemail and Fax Recording Services. The Voicemail and Fax Recording Service is available only when all these services are available.

102.2.1 Status

This metric shows whether or not the Voicemail and Fax Recording Service is available.

User Action

If the Status of Voicemail and Fax Recording Service is down, then check the results obtained by the Root Cause Analysis on the Voicemail and Fax Recording Service Home Page.

103

Voicemail and Fax Retrieval Service

The Voicemail and Fax Retrieval Service monitors the availability, performance, and usage of the Voicemail and Fax Service.

103.1 Activity Total

The Activity Total shows information about total retrieval calls for the last 5 minutes.

103.1.1 Total Retrieval Calls (last 5 minutes)

This metric displays information about the number of users performing the retrieval activity for the last five minutes across all the retrieval servers of the Voicemail and Fax service.

103.2 Response

The Response category checks and displays whether or not the Voicemail and Fax Retrieval Service is available. Its status is based on the status of all Voicemail and Fax Retrieval Services. The Voicemail and Fax Retrieval Service is available only when all these services are available.

103.2.1 Status

This metric shows whether or not the Voicemail and Fax Retrieval Service is available.

User Action

If the Status of Voicemail and Fax Retrieval Service is down, then check the results obtained by the Root Cause Analysis on the Voicemail and Fax Retrieval Service Home Page.