Oracle® Enterprise Manager

Event Test Reference Manual

Release 9.0.1

July 2001

Part No. A89872-02

ORACLE®

Oracle Enterprise Manager Event Test Reference Manual, Release 9.0.1

Part No. A89872-02

Primary Authors: Jacqueline Gosselin and Leo Cloutier

Contributors: Gang Chen, Ana Hernandez, Dennis Lee, George Lavash, and Xin Xu

Contents

2 Oracle Database Event Tests

3 Compaq Tru64 Event Tests

4 HP-UX Event Tests

5 IBM AIX Event Tests

7 Windows NT Event Tests

8 Management Pack for Oracle Applications Event Tests

Send Us Your Comments

Oracle Enterprise Manager Event Test Reference Manual, Release 9.0.1

Part No. A89872-02

Oracle Corporation welcomes your comments and suggestions on the quality and usefulness of this document. Your input is an important part of the information used for revision.

- Did you find any errors?
- Is the information clearly presented?
- Do you need more information? If so, where?
- Are the examples correct? Do you need more examples?
- What features did you like most?

If you find any errors or have any other suggestions for improvement, please indicate the document title and part number, and the chapter, section, and page number (if available). You can send comments to us in the following ways:

- Electronic mail: nedc-doc_us@oracle.com
- FAX: 603-897-3317 Attn: Oracle System Management Products
- Postal service:
  Oracle Corporation
  Oracle System Management Products Documentation Manager
  1 Oracle Drive
  Nashua, NH 03062
  U.S.A.

If you would like a reply, please give your name, address, telephone number, and (optionally) electronic mail address.

If you have problems with the software, please contact your local Oracle Support Services.

Preface

This section describes the purpose and organization of this manual: *Oracle Enterprise Manager Event Test Reference Manual*. Specifically, it covers the following topics:

Purpose of This Manual

This manual provides a detailed description of all the event tests available in the Oracle Enterprise Manager Event System. In addition to the general description of each event, event information includes data source, parameters, output, recommended frequency, and user action.

Audience

This manual is written for those who need detailed information about an event used in the Oracle Enterprise Manager Event System.

This manual assumes that you are familiar with the Oracle Enterprise Manager console and base applications. If you are not, please read *Oracle Enterprise Manager Concepts Guide* and *Oracle Enterprise Manager Administrator's Guide*.

How This Manual Is Organized

This manual is organized as follows:

Chapter 1, "Overview"

Introduces the information contained in this manual. It also provides detail information about the base event tests and the common node event tests.

Chapter 2, "Oracle Database Event Tests"

Provides a summary description of all the database event tests as well as, detailed information for each event test.

Chapter 3, "Compaq Tru64 Event Tests"

Provides detailed information for all the Compaq Tru64 event tests.

Chapter 4, "HP-UX Event Tests"

Provides detailed information for all the HP-UX event tests.

Chapter 5, "IBM AIX Event Tests"

Provides detailed information for all the IBM AIX event tests.

Chapter 6, "Solaris Event Tests"

Provides detailed information for all the Solaris event tests.

Chapter 7, "Windows NT Event Tests"

Provides detailed information for all the Windows NT event tests.

Chapter 8, "Management Pack for Oracle Applications Event Tests"

Provides detailed information for all the Oracle Applications event tests.

Chapter 9, "SAP Event Tests"

Provides detailed information for all the SAP R/3 event tests.

Chapter 10, "e-Business Event Tests"

Provides detailed information for all the e-Business event tests.

Oracle Enterprise Manager Pack Information

The Oracle Enterprise Manager product family includes the following packs: Oracle Change Management Pack, Oracle Diagnostics Pack, Oracle Tuning Pack, Oracle Management Pack for SAP R/3, and Oracle Management Pack for Oracle Applications. Each pack is fully integrated into the Oracle Enterprise Manager framework.

Oracle Change Management Pack

- Includes Create Baseline, Baseline Viewer, Comparison Viewer, Compare Database Objects, DB Alter, DB Propagate, DB Quick Change, Plan Editor, and Change Manager.
- Tracks metadata changes in databases.
- Eliminates errors and loss of data when upgrading databases to support new applications.
- Analyzes the impact and complex dependencies associated with application change and automatically performs database upgrades.
- Initiates change with easy-to-use wizards that teach systematic steps necessary to upgrade databases.

Oracle Diagnostics Pack

- Includes Oracle Performance Manager, Oracle Capacity Planner, Oracle Data Viewer, Oracle TopSessions, and Oracle Advanced Event Tests.
- Monitors, diagnoses, and maintains the stability of databases, operating systems, and applications. Both historical and real-time analysis are used to automatically avoid problems before they occur.
- Provides powerful capacity planning features that enable users to easily plan and track future system resource requirements.

Oracle Tuning Pack

- Includes Oracle SQL Analyze, Oracle Expert, SQL Explain Plan, Oracle Index Tuning Wizard, Tablespace Map, Reorg Wizard, Outline Management, and the Outline Editor.
- Optimizes system performance by identifying and tuning major database and application bottlenecks such as inefficient SQL coding, poor data structures, and improper use of system resources.

- Discovers tuning opportunities and automatically generates the analysis and required changes to tune the system. Inherent in the product are powerful teaching tools that help DBAs learn to tune the system as they work.
- Helps increase the productivity of developers and DBAs.

Oracle Management Pack for SAP R/3

- Includes Oracle Performance Manager, Oracle Capacity Planner, and Oracle Event Tests that are specific to monitoring your SAP R/3 environment.
- Monitors, diagnoses, and maintains the health of a SAP R/3 system. Both historical and real-time analysis are used to automatically avoid problems before they occur.
- Provides powerful capacity planning features that enable users to easily plan and track future system resource requirements.

Oracle Management Pack for Oracle Applications

- Includes Oracle Performance Manager, Oracle Capacity Planner, Concurrent Processing Tuning Assistant, and Oracle Applications Event Tests that are specific to monitoring your Oracle Applications environment.
- Enables you to monitor all aspects of your system, including databases and concurrent managers.
- Enables the monitoring, diagnosing, and capacity planning of the Oracle Applications environment.

Oracle Enterprise Manager Documentation

Oracle Enterprise Manager Event Test Reference Manual is one of several Oracle Enterprise Manager documents.

Oracle Enterprise Manager Base Documentation

- *Oracle Enterprise Manager Readme* provides important notes regarding the online documentation, updates to the software, and other late-breaking information for Oracle Enterprise Manager and the Oracle Management Packs.
- *Oracle Enterprise Manager Administrator's Guide* explains how to use Oracle Enterprise Manager, the Oracle Enterprise Manager console, common services, and integrated platform tools.
- *Oracle Enterprise Manager Concepts Guide* provides an overview of Oracle Enterprise Manager.

- *Oracle Enterprise Manager Configuration Guide* explains how to configure Oracle Enterprise Manager.
- *Oracle Enterprise Manager Messages Manual* describes Oracle Enterprise Manager error messages and methods for diagnosing those errors.
- *Oracle Intelligent Agent User's Guide* provides configuration information and answers to crucial troubleshooting questions pertaining to the Oracle Intelligent Agent.
- *Oracle Enterprise Manager Event Test Reference Manual* describes Oracle Event Tests which allow you to implement automatic problem detection and correction on concurrent managers, databases, listeners, nodes, and SAP R/3 systems.

Oracle Management Pack Installation documentation

- The *Oracle9i Installation Guide Release 9.0.1* for your particular platform provides important information for installing the Oracle Enterprise Manager console and the management packs. This manual also contains information such as hardware and software requirements, installable components, and deinstallation procedures. The *Oracle9i Installation Guide Release 9.0.1* is available as a free download from the Oracle Documentation Center at http://docs.oracle.com

Oracle Change Management Pack Documentation

- *Getting Started with Oracle Change Management Pack* provides an overview of the concepts and features of Oracle Change Management Pack applications.

Oracle Diagnostics Pack Documentation

- *Getting Started with the Oracle Diagnostics Pack* provides an overview of the concepts and features of Oracle Performance Manager, Oracle Capacity Planner, and Oracle TopSessions applications.

Oracle Tuning Pack Documentation

- *Database Tuning with the Oracle Tuning Pack* provides an overview of the concepts and features of each of the applications included in the Oracle Tuning Pack. The applications include Oracle SQL Analyze, Oracle Expert, Oracle Index Tuning Wizard, Reorg Wizard, Tablespace Map, Outline Management, and the Outline Editor. A description of how these applications can work together to tune an Oracle database is also provided.

Oracle Management Pack for Oracle Applications Documentation

- *Getting Started with Oracle Management Pack for Oracle Applications* provides an overview of the concepts and features of Oracle Performance Manager, Oracle Capacity Planner, and Concurrent Processing Tuning Assistant. It also describes Oracle Applications Event Tests and Jobs that are specific to monitoring your Oracle Applications environment.

Oracle Management Pack for SAP/R3 Documentation

- *Oracle Management Pack for SAP R/3 Readme* provides important notes regarding Oracle Management Pack for SAP R/3 online documentation, updates to the software, and other late-breaking information.
- *Getting Started with Oracle Management Pack for SAP R/3* provides an overview of the concepts and features of Oracle Performance Manager and Oracle Capacity Planner. It also describes Oracle Event Tests that are provided with the Oracle Management Pack for SAP/R3.
- The *Oracle Management Pack for SAP R/3 Installation* provides important information for installing the Oracle Enterprise Manager console and the Oracle Management Pack for SAP R/3. This manual also contains information such as hardware and software requirements, installable components, and deinstallation procedures.

How to Find Oracle Documentation Online

To download free release notes or installation documentation, please visit the Oracle Documentation Center at http://docs.oracle.com/

Printed documentation is available for sale in the Oracle Store at http://oraclestore.oracle.com/

Oracle Support

The Oracle MetaLink (www.oracle.com/support/metalink/index.html) site provides access to information that will aid you in using Oracle products such as: hot topics, product reference, installation assistance materials, white papers, problem/solution articles, and more. To use this site you must be a licensed Oracle user with an active support service contract.

Contact your Oracle sales representative for more information.

Documentation Accessibility

Oracle's goal is to make our products, services, and supporting documentation accessible to the disabled community with good usability. 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. 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 additional information, visit the Oracle Accessibility Program web site at http://www.oracle.com/accessibility/.

JAWS, a Windows screen reader, 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, JAWS may not always read a line of text that consists solely of a bracket or brace.

1

Overview

The Event System within Oracle Enterprise Manager assists the DBA with automatic problem detection and correction. Using the Event System, the DBA can establish boundary thresholds for warning and critical conditions within the network environment for problem monitoring.

The Enterprise Manager base product comes with a set of event tests called Base Event Tests. These event tests consist of UpDown event tests that check whether a database, listener, or node is available. "Base Event Tests" on page 1-2 gives a brief description of these UpDown event tests.

More comprehensive monitoring is available through Advanced Event Tests. This manual provides a complete description of all the events available through Oracle Enterprise Manager. The sub-categories of events are:

Base event tests are included as part of the Enterprise Manager base product and do not require an additional license. To use all the other event tests, you must have licensed the Oracle Diagnostics Pack, the Oracle Management Pack for Oracle Applications (for the Concurrent Manager events), or the Oracle Management Pack for SAP R/3 (for the SAP R/3 events).

Note: For information on using the Oracle Enterprise Manager Event System, see the *Oracle Enterprise Manager Administrator's Guide*.

Base Event Tests

The Base Event Tests are provided with the Enterprise Manager base product and consist of the UpDown event tests. These event tests check whether a database, listener, or node is available. With the UpDown event for databases or listeners, you can use the Startup Database or Startup Listener task as a fixit job to restart the database or listener. See Descriptions of Base and Common Node Event Tests on page 1-6 for a full description of these events.

Table 1–1 Base Event Tests

UpDown Event Test	Description
Database UpDown	This event test checks whether the database being monitored is running. If this test is triggered, other database events are not ignored. **Note:** If the listener serving a database is down, this event may be triggered because the Intelligent Agent uses the listener to communicate with the database. This note applies to Intelligent Agents released before 8.0.5. (See UpDown Database on page 2-142 for additional information.)
Node UpDown	This event test checks the status of the target node as well as the agent. If the agent is down or communication between the node and the Management Server is lost, this test is triggered. The node up/down event test differs from other event tests because this test is initiated by the Management Server, not the Agent. By default, this check is performed every 2 minutes and is NOT controlled by the event's polling schedule.

Table 1–1 Base Event Tests (Cont.)

UpDown Event Test	Description
Listener Oracle Net UpDown	This event test checks whether the listener on the node being monitored is available. This test is a listener fault management event test. **Note:** The Startup Listener job task can be set up as a fixit job for automatically correcting the problem.
Data Gatherer UpDown	This event test checks whether the Intelligent Agent data gathering service on a node can be accessed from the Console. If the Intelligent Agent data gathering service is down, this test is triggered. **Note:** This event test is valid only for releases of the Intelligent Agent prior to release 9*i*.
HTTP Server UpDown	This event test checks whether the HTTP server being monitored is running.

User-Defined Event Test

This event test allows you to define your own script.

Table 1–2 User-Defined Event Test

Event Test	Description
User-Defined Event Test	User-Defined Event tests allow you to define events based on your own monitoring scripts. The monitoring scripts can be written in any language, as long as the monitored node has the appropriate runtime requirements for the script. User-Defined Event tests thus allow administrators to extend the Event system to monitor any type of service or condition specific to their environments. Refer to the *Oracle Enterprise Manager Administrator's Guide* for more information on setting up User-Defined Event tests.

User-Defined SQL Event Test

This event test allows you to define your own SQL script.

Table 1–3 User-Defined SQL Event Test

Event Test	Description
User-Defined SQL Event Test	The User-Defined SQL event test allows you to define your own SQL script that evaluates an event test. The event tests you define should be written as queries (i.e. SELECT statements) that return condition values for which you are monitoring. These values are checked against the Critical and Warning threshold limits you specify, and trigger the event if the threshold limits are reached. **Example:** You have a custom application that runs against the Oracle database. Each time it finds an application error, it creates an entry into a table called "error_log". Using the “User-Defined SQL Test”, you can write an event test that notifies you when it finds at least 50 errors. Specifically, you define the following SQL statement: select count(*) from error_log This returns the number of rows in the error_log table. Since you want a critical alert raised when it reaches at least 50, you specify the Operator ">=", a Critical value of 50, and perhaps a Warning value of 30. If your query for the event condition requires more complex processing than is allowed in a single SELECT statement, you can first create a pl/sql function that contains the extra processing steps, and then use the pl/sql function with the User-Defined SQL event test. (See User-Defined SQL Event Test on page 2-148 for additional information.)

Microsoft® SQL Server Event Test

This test checks whether the Microsoft SQL Server being monitored is running.

Table 1–4 Microsoft SQL Server Event Test

Event Test	Description
UpDown (SQL Server)	This test checks whether the Microsoft SQL Server being monitored is running. SQL server is installed as a service on Windows NT platforms. You can either start the server from the NT service manager or using SQL Server Enterprise Manager. This service can also be started from the command line using the "net start mssqlsever" command. On Windows95 and Windows 98 environments where services are not available, SQL server can be started by executing the following command: `C:\> sqlservr -c -dc <full path name of master database> -ec <location of the log file>` Master database is one of the SQL server system databases which holds its dictionary information. This master database is similar to the Oracle SYSTEM tablespace except that it is shared across all SQL Server databases on a node. This command can also be used to start SQL Server as a foreground process on Windows NT. (See UpDown (SQL Server) on page 1-12 for additional information.)

Common Node Event Tests

The Common Node Event Tests apply to all operating system platforms that can run the Oracle Intelligent Agent. The Node event tests are divided into the following categories:

- Node Fault Management Event Tests (See Table 1–5)
- Node Performance Management Event Tests (See Table 1–6)
- Node Space Management Event Tests (See Table 1–7)

See Descriptions of Base and Common Node Event Tests on page 1-6 for a full description of these events.

Table 1–5 Node Fault Management Event Test

Event Test	Description
Data Gatherer Alert	This event test signifies that the Data Gatherer has generated errors to the Data Gatherer alert file since the last sample time. The Data Gatherer alert file is a special trace file containing a chronological log of messages and errors. Note that the Data Gatherer alert log file is different than the Database alert log file. An alert is displayed when Data Gatherer (ODG-xxxxx) messages are written to the Data Gatherer alert file.
Data Gatherer UpDown	This test checks whether the Intelligent Agent data gathering service on a node can be accessed from the Console. If the Intelligent Agent data gathering service is down, this test is triggered.
Node UpDown	This event test checks the status of the target node as well as the agent. If the agent is down or communication between the node and the Management Server is lost, this test is triggered. The node up/down event test differs from other event tests because this test is initiated by the Management Server, not the Agent. By default, this check is performed every 2 minutes and is NOT controlled by the event's polling schedule.

Table 1–6 Node Performance Management Event Tests

Event Test	Description
CPU Paging	This test checks the CPU paging rate (kilobytes/second paged in/out) against the threshold values specified by the threshold arguments. If the number of occurrences exceeds the values specified, then a warning or critical alert is generated.
CPU Utilization	This test checks for the CPU utilization (percentage used) against the threshold values specified by the threshold arguments. If the number of occurrences exceeds the values specified, then a warning or critical alert is generated.

Table 1–7 Node Space Management Event Tests

Event Test	Description
Disk Full	This test checks for available space on the disk specified by the disk name parameter, such as c: (Windows) or /tmp (UNIX). If the space available is less than the values specified in the threshold arguments, then a warning or critical alert is generated.
Disk Full (%)	This event test monitors the same file systems as the Disk Full event test. The Disk Full (%) event test, however, returns the percentage of space remaining on the disk destinations.
Swap Full	This test checks for available swap space. If the space available falls below the values specified in the threshold arguments, then a warning or critical alert is generated.

Descriptions of Base and Common Node Event Tests

Alert (Data Gatherer)

This event test signifies that the Data Gatherer has generated errors to the Data Gatherer alert file since the last sample time. The Data Gatherer alert file is a special trace file containing a chronological log of messages and errors. Note that the Data Gatherer alert log file is different than the Database alert log file. An alert is displayed when Data Gatherer (ODG-xxxxx) messages are written to the Data Gatherer alert file.

Parameters

None

Output

Alert log error messages since the last sample time.

Recommended Frequency

60 seconds

User Action

Examine the Data Gatherer alert log file (alert_dg.log) for additional information. The alert log file can be found in the ORACLE_HOME/odg/log directory for the Intelligent Agent.

Note: This event test is valid only for releases of the Intelligent Agent prior to 9*i*.

CPU Paging

This event test checks the CPU paging rate (kilobytes/second paged in/out) against the threshold values specified by the threshold arguments. If the number of

occurrences exceeds the values specified, then a warning or critical alert is generated.

Parameters

- Number of occurrences: Number of consecutive occurrences before a warning or critical alert is generated.
- Critical threshold: Threshold for critical alert (kilobytes/second).
- Warning threshold: Threshold for warning alert (kilobytes/second).

Output

Current rate

CPU Utilization

This event test checks for the CPU utilization (percentage used) against the threshold values specified by the threshold arguments. If the number of occurrences exceeds the values specified, then a warning or critical alert is generated.

Parameters

- Number of occurrences: Number of consecutive occurrences before a warning or critical alert is generated.
- Critical threshold: Threshold for critical alert (%).
- Warning threshold: Threshold for warning alert (%).

Output

Current value

Disk Full

This event test checks for available space on the disk specified by the disk name parameter, such as c: (Windows) or /tmp (UNIX). If the space available is less than the values specified in the threshold arguments, then a warning or critical alert is generated.

Parameters

- Disk name: Name of the disk to be monitored. No default is provided. **Note:** "*" is not a supported disk name.
- Critical threshold: Free space in kilobytes below which a critical alert will be generated. No default is provided.

- Warning threshold: Free space in kilobytes below which a warning alert will be generated. No default is provided.

Output
Disk name and space available in kilobytes on the disk.

Disk Full (%)

This event test monitors the same file systems as the Disk Full event test. The Disk Full (%) event test, however, returns the percentage of space remaining on the disk destinations.

Parameters
- Disk name: Name of the disk to be monitored. No default is provided. **Note:** "*" is not a supported disk name.
- Critical threshold: Percentage of free space below which a critical alert will be generated. Default is 30%.
- Warning threshold: Percentage of free space below which a warning alert will be generated. Default is 50%.

Output
Disk name and percentage of space available on the disk.

HTTP Server UpDown

This event test checks whether the HTTP server being monitored is running.

Parameters
None

Oracle Net UpDown

This event test checks whether the listener on the node being monitored is available. This event test is a listener fault management event test.

Parameters
None

User Action

The Startup Listener job task can be set up as a fixit job for automatically correcting the problem. To avoid the fixit job executing when the listener was brought down intentionally, turn off the fixit job option.

Swap Full

This event test checks for available swap space. If the space available falls below the values specified in the threshold arguments, then a warning or critical alert is generated.

Parameters

- Critical threshold: Percentage of free swap space below which a critical alert will be generated. No default is provided.
- Warning threshold: Percentage of free swap space below which a warning alert will be generated. No default is provided.

Output

Percentage of available space.

UpDown (Data Gatherer)

This event test checks whether the Intelligent Agent data gathering service on a node can be accessed from the Console. If the Intelligent Agent data gathering service is down, this test is triggered.

Parameters

None

Output

None

Recommended Frequency

60 seconds

User Action

Restart the Oracle Data Gatherer.

Note: This event test is valid only for releases of the Intelligent Agent prior to 9*i*.

UpDown (Node)

This event test checks the status of the target node as well as the agent. If the agent is down or communication between the node and the Management Server is lost, this test is triggered.

The node up / down event test differs from other event tests because this test is initiated by the Management Server, not the Agent. By default, this check is performed every 2 minutes and is NOT controlled by the event's polling schedule.

Parameters

None

Possible Error Messages and User Actions

If the node Up / Down event test identifies a problem, one of the following messages may be generated:

VNI-4009: Cannot contact agent on the node -- agent may be down or network communication to the node has failed.

Cause: There may be network congestion or problems with the hardware / software on the node.

Action: Check the node and make sure it operational. Check the network connection by pinging the node. For network problems, contact your network administrator.

VNI-4038: Out of memory! Large job outputs could cause this.

Cause: There is a problem allocating memory on the Management Server node.

Action: Free up more memory on the node running the Management Server.

VNI-4040: Agent state is corrupted.

Cause: The Oracle Management Server repository is out of sync with the agent's queue files. The queue files of the agent may have been corrupted or deleted. This could be caused in one of three ways:

Situation 1: A new agent was installed into a new Oracle home but the "*.q" files were not migrated over from the old Oracle home.

Action: Bring the agent down, copy over the new "*.q" files, and bring the agent back up. Refresh the node from within the Oracle Enterprise Manager console. Ping the node to see if the Oracle Management Server and agent are now synchronized.

Situation 2: The "*.q" files were deleted.

Action: Remove the node from the Oracle Enterprise Manager console navigator. This will prompt you to remove existing jobs/events. Once the jobs and events have been removed, collapse and expand the console navigator to refresh the tree and see that the node is removed.

Situation 3: Two or more agents are on the same node. At some point, jobs and events were submitted against one agent. That agent was brought down and another agent was brought up. Jobs and events were then submitted against the second agent.

Action: Bring up the correct agent and refresh the node from the Oracle Enterprise Manager console navigator.

VNI-4044: Cannot contact agent. Node may be down, or the network may be down or slow.

Cause: There are problems contacting the node itself.

Action: Check the node and make sure it is up and running. Check the physical network connections to the node. Try doing a "ping" and make sure the node is responding. If there are network problems, contact your network administrator.

VNI-4045: Cannot contact agent. Agent is not running on the node.

Cause: The node is accessible, but the agent is not running.

Action: Start the agent.

Windows NT: Start the agent service from the Control Panel Services

UNIX: For releases of the Intelligent Agent prior to 9*i*, use: lsnrctl dbsnmp_start. For release 9*i* of the Intelligent Agent use: agentctl start [agent].

VNI-4046: Agent is not responding. Agent may be busy or in an invalid state.

Cause: The agent is not able to respond in a timely manner. This is most likely due to internal communication problems with the agent.

Action: Restart the agent. If this error occurs repeatedly, turn on agent tracing and contact Oracle Worldwide Support.

VNI-4047: Error accessing queue files on the Agent node.

Cause: There are problems accessing .q files on the agent node.

Action: Check the $ORACLE_HOME/network/agent directory, where $ORACLE_HOME is the directory where the agent is installed. Make sure there is disk space available and permissions are set such that the agent executable (dbsnmp) has read/write permissions on that directory and its files.

VNI-4048: Agent internal error (For example, Out of memory, Operating system error)

Cause: This is an internal problem.

Action: Try restarting the agent. If the problem occurs again, turn on agent tracing and contact Oracle Worldwide Support.

VNI-4049: Communications error. (e.g., oms communications software error)

Cause: This is usually a transient type of error.

Action: Check the network connection between the OMS node and the agent node.

UpDown (SQL Server)

This event test checks whether the Microsoft ® SQL Server being monitored is running.

Parameters

None

User Action

SQL server is installed as a service on Windows NT platforms. You can either start the server from the NT service manager or using SQL Server Enterprise Manager. This service can also be started from the command line using the "net start mssqlsever" command.

Use the following command to start SQL Server as a foreground process on Windows NT:

C:/> sqlservr -c -dc <full path name of master database> -ec <location of the log file>

Master database is one of the SQL server system databases which holds its dictionary information. This master database is similar to the Oracle SYSTEM tablespace except that it is shared across all SQL Server databases on a node.

2

Oracle Database Event Tests

The Oracle Enterprise Manager Advanced Event Tests for the Oracle Database are divided into a series of categories that enable you to find the event test you want to register.

Summary of Database Event Tests

The Oracle Advanced Event Tests for the database service type are grouped into the following categories:

- User-Defined SQL Event Test

  This event test allows you to define your own SQL script that evaluates an event condition. See User-Defined SQL Event Test on page 2-148.

- Database Audit Management Event Test

  The database Audit Event test (User Audit) allows you to monitor specific database user connections. See Table 2–1.

- Database Fault Management Event Tests

  This category of event tests monitors for server problems that require immediate action. See Table 2–2.

- Database Performance Management Event Tests

  This category of event tests monitors the system for performance problems. The Performance Management event tests are divided into the following activities:

  - Application - See Table 2–3.
  - Instance - See Table 2–4.
  - Transaction - See Table 2–5.

- Wait - See Table 2–6.

- Database Resource Management Event Tests

  This category of event tests tracks possible resource problems. See Table 2–7.

- Database Space Management Event Tests

  This category of event tests tracks possible space problems within the database. See Table 2–8.

- Database Specialized Management Event Tests

  This category of event tests monitors the following specific database capabilities:

  - Advanced Queuing - See Table 2–9.
  - Cluster Databases - See Table 2–10.
  - Data Guard - See Table 2–11.

The full descriptions of the individual event tests follow the tables. The event tests are in alphabetical order.

Table 2–1 Database Audit Management Event Test

Event Test	Description
User Audit	This test monitors specified database user connections. For example, an alert is displayed when a particular database user connection, specified by the User name argument, has been detected.

Table 2–2 Database Fault Management Event Tests

Event Test	Description
Alert	This event test signifies that the database being monitored has generated errors to the ALERT log file since the last sample time. The ALERT log file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when Oracle Exception (ORA-006xx), deadlock detected (ORA-00060), or data block corrupted (ORA-01578) messages are written to the ALERT log file. A warning is displayed when other ORA messages are written to the ALERT log file.
Archiver Hung	This event test signifies that the archiver of the database being monitored has been temporarily suspended since the last sample time. If the database is running in ARCHIVELOG mode, an alert is displayed when archiving is hung (ORA-00257) messages are written to the ALERT file. The ALERT file is a special trace file containing a chronological log of messages and errors. If the database is not running in ARCHIVELOG mode, this test will not register.

Table 2–2 Database Fault Management Event Tests (Cont.)

Event Test	Description
Broken Jobs	The Oracle server job queue is a database table that stores information about local jobs such as the PL/SQL call to execute for a job such as when to run a job. Database replication is also managed by using Oracle's job queue mechanism using jobs to push deferred transactions to remote master sites, to purge applied transactions from the deferred transaction queue or to refresh snapshot refresh groups. A job can be broken in two ways: ■ Oracle has failed to successfully execute the job after sixteen attempts. ■ The job has been explicitly marked as broken by using the procedure DBMS_ JOB.BROKEN This event test checks for broken DBMS jobs. An alert is generated if the number of broken jobs exceeds the value specified by the threshold argument.
Data Block Corruption	This event test signifies that the database being monitored has generated a corrupted block error to the ALERT file since the last sample time. The ALERT file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages (ORA-01578, ORA-27048, and ORA-01157) are written to the ALERT file.
Deferred Transactions	Oracle uses deferred transactions to propagate data-level changes asynchronously among master sites in an advanced replication system as well as from an updatable snapshot to its master table. This event test checks for the number of deferred transactions. An alert is generated if the number of deferred transactions exceeds the value specified by the threshold argument.
Error Transactions	Oracle uses deferred transactions to propagate data-level changes asynchronously among master sites in an advanced replication system as well as from an updatable snapshot to its master table. If a transaction is not successfully propagated to the remote site, Oracle rolls back the transaction, logs the transaction in the SYS.DEFERROR view in the remote destination database. This test checks for the number of transactions in SYS.DEFERROR view and raises an alert if it exceeds the value specified by the threshold argument.
Failed Jobs	The Oracle server job queue is a database table that stores information about local jobs such as the PL/SQL call to execute for a job such as when to run a job. Database replication is also managed by using the Oracle job queue mechanism using jobs to push deferred transactions to remote master sites, to purge applied transactions from the deferred transaction queue or to refresh snapshot refresh groups. If a job returns an error while Oracle is attempting to execute it, the job fails. Oracle repeatedly tries to execute the job doubling the interval of each attempt. If the job fails sixteen times, Oracle automatically marks the job as broken and no longer tries to execute it.This test checks for failed DBMS jobs. An alert is generated if the number of failed jobs exceeds the value specified by the threshold argument.
Probe	This event test checks whether a new connection can be established to a database. If the maximum number of users is exceeded or the listener is down, this test is triggered. **Note:** The choice of user credentials for the Probe event test should be considered. If the preferred user has the RESTRICTED SESSION privilege, the user will be able to connect to a database even if the LICENSE_MAX_SESSIONS limit is reached.
Session Terminated	This test signifies that a session terminated unexpectedly since the last sample time. The ALERT file is a special trace file containing a chronological log of messages and errors. An alert is displayed when session unexpectedly terminated (ORA-00603) messages are written to the ALERT file.

Table 2–2 Database Fault Management Event Tests (Cont.)

Event Test	Description
Unscheduled Jobs	The Oracle server job queue is a database table that stores information about local jobs. This event test checks for unscheduled DBMS jobs. An alert is generated when the number of jobs, whose execution time has exceeded the value specified by the Job Completion Time argument, exceeds the value specified in the Critical Threshold. A job's completion date / time is calculated by using the NEXT_DATE value in the SYS.DBA_JOBS view plus the approximate time it takes to complete a job as specified by the job completion time argument.
User Blocks	This event test signifies that a database user is blocking at least one other user from performing an action, such as updating a table. An alert is generated if the number of consecutive blocking occurrences reaches the specified value. **Note:** The catblock.sql script needs to be run on the managed database prior to using the User Blocks test. This script creates some additional tables, views, and public synonyms that are required by the User Blocks test.

Table 2–3 Database Performance Management Event Tests - Application Activity

Event Test	Description
Average File Read Time	This data item represents the average time spent performing a read from this datafile during the sample period. This value will always be 0 unless the TIMED_STATISTICS parameter is TRUE. The value of this item is reported in 100ths of a second. Therefore a value of 100 would mean on average that one second of time was spent per physical read to this file during the last sample period. There is a drilldown chart available from this chart called Timed Statistics Chart. This chart shows the current value for the TIMED_STATISTICS parameter. Use the Turn On Timed Statistics drilldown to turn on timed statistics for the instance. This test checks the average time spent performing a read for a file specified by File Name(s) parameter during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Average File Write Time	This data item represents the average time spent performing a write to this datafile during the sample period. This value will always be 0 unless the TIMED_STATISTICS parameter is TRUE. The value of this item is reported in 100ths of a second. Therefore a value of 100 would indicate on average that one second of time was spent per physical write to this file during the last sample period. There is a drilldown chart available from this chart called Timed Statistics Chart. This chart shows the current value for the TIMED_STATISTICS parameter. Use the Turn On Timed Statistics drilldown to turn on timed statistics for the instance. This test checks the average time spent performing a write for a file specified by File Name(s) parameter during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–3 Database Performance Management Event Tests - Application Activity (Cont.)

Event Test	Description
Average Redo Write Size Per Second	This data item represents the amount of redo, in bytes, generated per second during this sample period. The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries can be used for database recovery if necessary. This test checks the amount of redo in bytes generated per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Average Rows Per Sort	This data item represents the average number of rows per sort during this sample period. This test checks the average number of rows per sort during sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Commits Per Second	This data item represents the number of user commits performed, per second during the sample period. When a user commits a transaction, the redo generated that reflects the changes made to database blocks must be written to disk. Commits often represent the closest thing to a user transaction rate. This test checks the number of user commits per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Disk I/O	This event test monitors the real time database physical I/O rate (requests/seconds) against the values specified by the threshold arguments. If the Disk I/O rate exceeds the threshold values entered for the specified number of occurrences, then a warning or critical alert is generated. **Note:** The Disk I/O event test is provided for backward compatibility. Oracle recommends that you use the File Read Rate and File Write Rate event tests.
Disk Sorts Per Second	This data item represents the number of sorts going to disk per second for this sample period. For best performance, most sorts should occur in memory, because sorts to disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption. This test checks the number of sorts performed to disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–3 Database Performance Management Event Tests - Application Activity (Cont.)

Event Test	Description
Executes without Parses %	This data item represents the percentage of statement executions that do not require a corresponding parse. A perfect system would parse all statements once and then execute the parsed statement over and over without reparsing. This ratio provides an indication as to how often the application is parsing statements as compared to their overall execution rate. A higher number is better. This test checks the percentage of executes that do not require parses. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Logical Reads Per Second	This data item represents the number of logical reads per second during the sample period. A logical read is a read request for a data block from the SGA. Logical reads may result in a physical read if the requested block does not reside with the buffer cache. This test checks the logical (db block gets + consistent gets) reads per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Logons Per Second	This data item represents the number of logons per second during the sample period. This test checks the number of logons that occurred per second during the sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Network Bytes Per Second	This data item represents the total number of bytes sent and received through the SQL Net layer to and from the database. This test checks the network read/write per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Parses (Hard) Per Second	This data item represents the number of hard parses per second during this sample period. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor. This test checks the number of parses of statements that were not already in the cache. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–3 Database Performance Management Event Tests - Application Activity (Cont.)

Event Test	Description
Parses (Total) Per Second	This number reflects the total number of parses per second, both hard and soft. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse. Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor. This test checks the number of parse calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Physical Reads Per Second	This data item represents the number of data blocks read from disk per second during this sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then searches the disk if it is not already in memory. Reading data blocks from disk is much more inefficient than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization. This test checks the data blocks read from disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Physical Writes Per Second	This data item represents the number of disk writes per second during the sample period. This statistic represents the rate of database blocks written from the SGA buffer cached to disk by the DBWR background process, and from the PGA by processes performing direct writes. This test checks the data blocks written disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–3 Database Performance Management Event Tests - Application Activity (Cont.)

Event Test	Description
Recursive Calls Per Second	This data item represents the number of recursive calls, per second during the sample period. Sometimes, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated: ■ when data dictionary information is not available in the data dictionary cache and must be retrieved from disk ■ in the firing of database triggers ■ in the execution of DDL statements ■ in the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks ■ in the enforcement of referential integrity constraints This test checks the number of recursive SQL calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Redo Writes Per Second	This data item represents the number redo write operations per second during this sample period. The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries can be used for database recovery if necessary. The log writer processes (LGWR) is responsible for redo log buffer management; that is, writing the redo log buffer to a redo log file on disk. This test checks the number of writes by LGWR to the redo log files per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Response Time Per Execution	Using only statistics available within the database, this data item gives the best approximation of response time, in seconds, per SQL statement execution. This statistic may be more valid than response time per transaction as it shows accurate values even for read-only access. This test checks the response time, in seconds, per SQL statement execution during sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Rollbacks Per Second	This data item represents the number of times, per second during the sample period, that users manually issue the ROLLBACK statement or an error occurred during a user's transactions. This test checks the number of rollbacks per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–3 Database Performance Management Event Tests - Application Activity (Cont.)

Event Test	Description
Soft Parse %	A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse. This data item represents the percentage of parse requests where the cursor was already in the cursor cache compared to the number of total parses. This ratio provides an indication as to how often the application is parsing statements that already reside in the cache as compared to hard parses of statements that are not in the cache. This test checks the percentage of soft parse requests to total parse requests. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Table Scans (Long) Per Second	This data item represents the number of long table scans per second during sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks. This test checks the long table scans per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Table Scans (Total) Per Second	This data item represents the number of long and short table scans per second during the sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.
User Call %	This data item represents the percentage of user calls to recursive calls. Occasionally, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated: ■ When data dictionary information is not available in the data dictionary cache and must be retrieved from disk ■ In the firing of database triggers ■ In the execution of DDL statements ■ In the execution of SQL statements within stored procedures, functions, packages and anonymous PL / SQL blocks ■ In the enforcement of referential integrity constraints This test checks the percentage of user calls to recursive calls. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
User Calls Per Second	This data item represents the number of logins, parses, or execute calls per second during the sample period. This test checks the number of logins, parses, or execute calls. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–4 Database Performance Management Event Tests - Instance Activity

Event Test	Description
% CPU Time	Data item that represents the percentage of time, instance-wide, spent executing instructions by the CPU during this sample period. This test checks the percentage time spent executing instructions by the CPU, instance-wide, for resources or objects during this sample period. If the % CPU Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Shared Pool Free	This data item represents the percentage of the Shared Pool that is currently marked as free. This test checks the percentage of Shared Pool that is currently free. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Wait Time	Data item representing the percentage of time spent waiting, instance-wide, for resources or objects during this sample period. This test checks the percentage time spent waiting, instance-wide, for resources or objects during this sample period. If the % Wait Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Buffer Cache Hit %	The data block buffer cache efficiency, as measured by the hit ratio, records the percentage of times the data block requested by the query is in memory. Effective use of the buffer cache can greatly reduce the I/O load on the database. If the buffer cache is too small, frequently accessed data will be flushed from the buffer cache too quickly which forces the information to be re-fetched from disk. Since disk access is much slower than memory access, application performance will suffer. In addition, the extra burden imposed on the I/O subsystem could introduce a bottleneck at one or more devices which would further degrade performance. This event test monitors the buffer cache hit ratio (percentage of success) against the values specified by the threshold arguments. If the number of occurrences is smaller than the values specified, then a warning or critical alert is generated. **Note:** The DB_BLOCK_BUFFERS initialization parameter determines the number of database buffers available in the buffer cache. It is one of the primary parameters which contribute to the total memory requirements of the SGA on the instance. The DB_BLOCK_BUFFERS parameter, together with the DB_BLOCK SIZE parameter, controls the total size of the buffer cache. Since DB_BLOCK_SIZE can only be specified when the database is first created, normally the size of the buffer cache size is controlled using the DB_ BLOCK_BUFFERS parameter.
Commit %	This data item represents the percentage of transactions that ended as commits rather than rollbacks during this sample period. This test checks the percentage of transactions that end as commits, as opposed to rollbacks. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–4 Database Performance Management Event Tests - Instance Activity (Cont.)

Event Test	Description
Data Dictionary Hit %	This data item represents dictionary cache efficiency as measured by the percentage of requests against the dictionary data that were already in memory. It is important to determine whether the misses on the data dictionary are actually affecting the performance of the Oracle Server. The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache, and the other cache structures that are specific to a particular instance configuration. Misses on the data dictionary cache are to be expected in some cases. Upon instance startup, the data dictionary cache contains no data, so any SQL statement issued is likely to result in cache misses. As more data is read into the cache, the likelihood of cache misses should decrease. Eventually the database should reach a steady state in which the most frequently used dictionary data is in the cache. At this point, very few cache misses should occur. To tune the cache, examine its activity only after your application has been running. This test checks the percentage of requests against the data dictionary that were found in the Shared Pool. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Data Dictionary Miss %	The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache and the other cache structures that are specific to a particular instance configuration. The dictionary cache efficiency, as measured by the miss ratio, records the percentage of times the dictionary data was not already in memory. The shared pool mechanism can greatly reduce system resource consumption in at least three ways: ■ Parse time is avoided if the SQL statement is already in the shared pool. ■ Application memory overhead is reduced, since all applications utilize the same pool of shared SQL statements and dictionary resources. ■ I/O resources are saved, since dictionary elements which are in the shared pool do not require access. If the shared pool is too small, users will consume additional resources to complete a database operation. For dictionary cache access, the overhead is primarily the additional I/O since the dictionary cache references that have been displaced from the cache will need to be re-fetched from disk. This event test monitors the data dictionary cache miss ratio (percentage of failures) against the values specified by the threshold arguments. If the number of occurrences exceeds the values specified, then a warning or critical alert is generated. **Note:** The Data Dictionary Miss % event test is provided for backward compatibility. Oracle recommends that you use the Data Dictionary Hit % event test.

Table 2–4 Database Performance Management Event Tests - Instance Activity (Cont.)

Event Test	Description
DBWR Checkpoints Per Second	This data item represents the number of times, per second, during this sample period DBWn was asked to scan the cache and write all blocks marked for a checkpoint. The database writer process (DBWn) writes the contents of buffers to datafiles. The DBWn processes are responsible for writing modified (dirty) buffers in the database buffer cache to disk. When a buffer in the database buffer cache is modified, it is marked dirty. The primary job of the DBWn process is to keep the buffer cache clean by writing dirty buffers to disk. As buffers are dirtied by user processes, the number of free buffers diminishes. If the number of free buffers drops too low, user processes that must read blocks from disk into the cache are not able to find free buffers. DBWn manages the buffer cache so that user processes can always find free buffers. When the Oracle Server process cannot find a clean reusable buffer after scanning a threshold of buffers, it signals DBWn to write. When this request to make free buffers is received, DBWn writes the least recently used (LRU) buffers to disk. By writing the least recently used dirty buffers to disk, DBWn improves the performance of finding free buffers while keeping recently used buffers resident in memory. For example, blocks that are part of frequently accessed small tables or indexes are kept in the cache so that they do not need to be read in again from disk. The LRU algorithm keeps more frequently accessed blocks in the buffer cache so that when a buffer is written to disk, it is unlikely to contain data that may be useful soon. Additionally, DBWn periodically writes buffers to advance the checkpoint which is the position in the redo log from which crash or instance recovery would need to begin. This test checks the number of times DBWR was asked to advance the checkpoint. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Free Buffer Waits	Database writer process (DBWR) bottlenecks can be detected by monitoring occurrences of the free buffer waits test over time. If the database environment is in a steady state, there should not be any free buffer waits. However, an occasional absolute increase in free buffer waits is not a problem. Only consistent occurrences of an increase should be of concern. As a result, this test maintains a history of free buffer waits samples, specified by the number of samples parameter, and monitors for a percentage of these samples where an increase was detected. This percentage is then compared against the values specified by the threshold arguments. If the percentage of samples (where an increase in free buffer waits is detected) exceeds the threshold arguments, then a warning or critical alert is generated. **Example:** If 10 has been specified for the number of samples, then during the first 9 times the test condition is checked, the test is merely building up the history of free buffer waits samples. On the 10 interval and from that point on, the test monitors how many of those samples showed and increase in free buffer waits. Assume 2 samples showed an increase, then the percentage of samples showing an increase is 20%.

Table 2–4 Database Performance Management Event Tests - Instance Activity (Cont.)

Event Test	Description
In Memory Sort %	The sort efficiency is measured by the percentage of times sorts were performed in memory as opposed to going to disk. For best performance, most sorts should occur in memory as sorts to disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption. This event test monitors the in memory sort hit ratio. The ratio equals the number of sorts performed in memory divided by the total number of sorts performed. If the number of occurrences is smaller that the values specified, then a warning or critical alert is generated.
Library Cache Hit %	This data item represents the library cache efficiency, as measured by the percentage of times the fully parsed or compiled representation of PL/SQL blocks and SQL statements are already in memory. The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache and the other cache structures that are specific to a particular instance configuration. The shared pool mechanism can greatly reduce system resource consumption in at least three ways: ■ Parse time is avoided if the SQL statement is already in the shared pool. ■ Application memory overhead is reduced, since all applications use the same pool of shared SQL statements and dictionary resources. ■ I/O resources are saved, since dictionary elements which are in the shared pool do not require access. If the shared pool is too small, users will consume additional resources to complete a database operation. For library cache access, the overhead is primarily the additional CPU resources required to re-parse the SQL statement. This test checks the percentage of parse requests where cursor already in cache If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–4 Database Performance Management Event Tests - Instance Activity (Cont.)

Event Test	Description
Library Cache Miss %	The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache and the other cache structures that are specific to a particular instance configuration. The library cache efficiency, as measured by the miss ratio, records the percentage of times the fully parsed or compiled representation of PL/SQL blocks and SQL statements are not already in memory. The shared pool mechanism can greatly reduce system resource consumption in at least three ways: ▪ Parse time is avoided if the SQL statement is already in the shared pool. ▪ Application memory overhead is reduced, since all applications utilize the same pool of shared SQL statements and dictionary resources. ▪ I/O resources are saved, since dictionary elements which are in the shared pool do not require access. If the shared pool is too small, users will consume additional resources to complete a database operation. For library cache access, the overhead is primarily the additional CPU resources required to re-parse the SQL statement. This event test monitors the library cache miss ratio (percentage of failures) against the values specified by the threshold arguments. If the number of occurrences exceeds the values specified, then a warning or critical alert is generated. **Note:** The Library Cache Miss % event test is provided for backward compatibility. Oracle recommends that you use the Library Cache Hit % event test.
Redo Log Allocation Hit	Redo log entries contain a record of changes that have been made to the database block buffers. The log writer (LGWR) process writes redo log entries from the log buffer to a redo log file. The log buffer should be sized so that space is available in the log buffer for new entries, even when access to the redo log is heavy. When the log buffer is undersized, user process will be delayed as they wait for the LGWR to free space in the redo log buffer. The redo log buffer efficiency, as measured by the hit ratio, records the percentage of times users did not have to wait for the log writer to free space in the redo log buffer. This event test monitors the redo log buffer hit ratio (percentage of success) against the values specified by the threshold arguments. If the number of occurrences is smaller than the values specified, then a warning or critical alert is generated. **Note:** The Redo Log Allocation Hit event test is provided for backward compatibility. Oracle recommends that you use the Redo NoWait Ratio event test.
Redo No Wait %	Redo log entries contain a record of changes that have been made to the database block buffers. The log writer (LGWR) process writes redo log entries from the log buffer to a redo log file. The log buffer should be sized so that space is available in the log buffer for new entries, even when access to the redo log is heavy. When the log buffer is undersized, user process will be delayed as they wait for the LGWR to free space in the redo log buffer. This data item represents the redo log buffer efficiency, as measured by the percentage of times users did not have to wait for the log writer to free space in the redo log buffer. This test checks the percentage of times redo entries are allocated without having to wait. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–4 Database Performance Management Event Tests - Instance Activity (Cont.)

Event Test	Description
Rollback Contention	Rollback segments are portions of the database that record the actions of transactions in case a transaction is rolled back. Rollback segments are used to provide read consistency, support rollback transactions, and recover a database. Proper allocation of rollback segments make for optimal database performance. Using a sufficient number of rollback segments distributes rollback segment contention across many segments and improves performance. Contention for rollback segments is reflected by contention for buffers that contain rollback segment blocks. This event test monitors rollback segment missing ratio (percentage) against the values specified by the threshold arguments. If the missing ratio is greater than the values specified, then a warning or critical alert is generated.
SysStat Table	You can monitor any system statistic available in the database with this event test. A warning or critical alert will be generated if the value of the selected V$SYSSTAT parameter exceeds the values specified by the threshold arguments. To view the V$SYSSTAT parameter names and values, connect to the database with SQL Worksheet and execute SELECT NAME, VALUE FROM V$SYSSTAT.
SysStat Table Delta	You can monitor any system statistic available in the database with this event test. The threshold values are compared to the difference between the last sample point and the current sample point of the V$SYSSTAT parameter. A warning or critical alert is generated if the calculated difference exceeds the values specified by the threshold arguments. To view the V$SYSSTAT parameter names and values, connect to the database with SQL Worksheet and execute SELECT NAME, VALUE FROM V$SYSSTAT.
Transactions Per Second	This data item represents the total number of commits and rollbacks performed during this sample period. This test checks the number of commits and rollbacks performed during sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–5 Database Performance Management Event Tests - Transaction Activity

Event Test	Description
Average Redo Write Size Per Transaction	This data item represents the amount of redo, in bytes, generated per transaction during this sample period. The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries are used for database recovery, if necessary. The value of this statistic is zero if there have been no write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the amount of redo in bytes generated per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Commits Per Transaction	This data item represents the number of user commits performed, per transaction during the sample period. When a user commits a transaction, the redo generated that reflects the changes made to database blocks must be written to disk. Commits often represent the closest thing to a user transaction rate. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the number of user commits per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Disk Sorts Per Transaction	This data item represents the number of sorts going to disk per transactions for this sample period. For best performance, most sorts should occur in memory, because sorts to disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the number of sorts performed to disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–5 Database Performance Management Event Tests - Transaction Activity (Cont.)

Event Test	Description
Logical Reads Per Transaction	This data item represents the number of logical reads per transaction during the sample period. The value of this statistic is zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding per second data item of the same name will be a better indicator of current performance. This test checks the logical (db block gets + consistent gets) reads per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Logons Per Transaction	This data item represents the number of logons per transaction during the sample period. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the number of logons that occurred per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Parses (Hard) Per Transaction	This data item represents the number of hard parses per second during this sample period. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the number of hard parses per second during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–5 Database Performance Management Event Tests - Transaction Activity (Cont.)

Event Test	Description
Parses (Total) Per Transaction	This number reflects the total number of parses per transaction, both hard and soft. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse. Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor. This test checks the number of parse calls per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Physical Reads Per Transaction	This data item represents the number of disk reads per transaction during the sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then goes to disk if it is not in memory already. Reading data blocks from disk is much more expensive than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the data blocks read from disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Physical Writes Per Transaction	This data item represents the number of disk writes per transaction during the sample period. The value of this statistic is zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name is a better indicator of current performance. This test checks the data blocks written disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–5 Database Performance Management Event Tests - Transaction Activity (Cont.)

Event Test	Description
Recursive Calls Per Transaction	This data item represents the number of recursive calls, per second during the sample period. Sometimes, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated: ■ when data dictionary information is not available in the data dictionary cache and must be retrieved from disk ■ in the firing of database triggers ■ in the execution of DDL statements ■ in the execution of SQL statements within stored procedures, functions, packages and anonymous PL / SQL blocks ■ in the enforcement of referential integrity constraints The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the number of calls that result in changes to internal tables. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Redo Writes Per Transaction	This data item represents the number of redo write operations per second during this sample period. The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries are used for database recovery, if necessary. The log writer process (LGWR) is responsible for redo log buffer management; that is, writing the redo log buffer to a redo log file on disk. This test checks the number of writes by LGWR to the redo log files per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Response Time Per Transaction	Using only statistics available within the database, this data item gives the best approximation of response time, in seconds, per transaction during this sample period. This test checks the response time in seconds, per transaction during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–5 Database Performance Management Event Tests - Transaction Activity (Cont.)

Event Test	Description
Rollbacks Per Transaction	This data item represents the number of times, per transaction during the sample period, that users manually issue the ROLLBACK statement or an error occurred during a user's transactions. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the Number of rollbacks per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Table Scan (Long) Per Transaction	This data item represents the number of long table scans per transaction during sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the number of long table scans per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Table Scans (Total) Per Transaction	This data item represents the number of long and short table scans per transaction during the sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks. This test checks the number of long and short table scans per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
User Calls Per Transaction	This data item represents the number of logins, parses, or execute calls per transaction during the sample period. The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance. This test checks the number of logins, parses, or execute calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–6 Database Performance Management Event Tests - Wait Activity

Event Test	Description
Wait by Session Count	This data item represents the number of sessions currently waiting on this event. This test checks the number of sessions currently waiting for the event specified by the Wait Event(s) parameter. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Wait by Time	This data item represents the length of time, in seconds, spent waiting for the event during the last sample period. This value will always be 0 unless the TIMED_STATISTICS parameter is TRUE. This test checks the length of time, in seconds, spent waiting for the event specified by the Wait Event(s) parameter during the last sample period If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–7 Database Resource Management Event Tests

Event Test	Description
Datafile Limit	The DB_FILES initialization parameter specifies the maximum number of database files that can be opened for this database. This event test checks for the utilization of the datafile resource against the values (percentages) specified by the threshold arguments. If the percentage of data files currently used to the limit set in the DB_FILES initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated. **Example:** If 30 data files are used and the value of DB_FILES is 40, the percentage is 75% (30 / 40 x 100). This value is compared against the specified thresholds.
Lock Limit	The DML_LOCKS initialization parameter specifies the maximum number of DML locks. The purpose of DML locks is to guarantee the integrity of data being accessed concurrently by multiple users. DML locks prevent destructive interference of simultaneous conflicting DML and / or DDL operations. This event test checks for the utilization of the lock resource against the values (percentage) specified by the threshold arguments. If the percentage of all active DML locks to the limit set in the DML_LOCKS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated. If DML_LOCKS is 0, this test fails to register. A value of 0 indicates that enqueues are disabled. **Example:** If 40 DML locks are active and the value of DML_LOCKS is 60, the percentage is 67% (40 / 60 x 100). This value is compared against the specified thresholds.

Table 2–7 Database Resource Management Event Tests (Cont.)

Event Test	Description
Process Limit	The PROCESSES initialization parameter specifies the maximum number of operating system user processes that can simultaneously connect to a database at the same time. This number also includes background processes utilized by the instance. This event test checks for the utilization of the process resource against the values (percentage) specified by the threshold arguments. If the percentage of all current processes to the limit set in the PROCESSES initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated. **Example:** If 40 processes are currently connected and the value of PROCESSES is 50, the percentage is 80% (40 / 50 x 100). This value is compared against the specified thresholds.
Session Limit	The SESSIONS initialization parameter specifies the maximum number of concurrent connections that the database will allow. This event test checks for the utilization of the session resource against the values (percentage) specified by the threshold arguments. If the percentage of the number of sessions, including background processes, to the limit set in the SESSIONS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated. **Example:** If there are 20 sessions and the value of SESSIONS is 25, the percentage is 80% (20 / 25 x 100). This value is compared against the specified thresholds.
User Limit	The LICENSE_MAX_SESSIONS initialization parameter specifies the maximum number of concurrent user sessions allowed simultaneously. This event test checks whether the number of users logged on is reaching the license limit. If the percentage of the number of concurrent user sessions to the limit set in the LICENSE_MAX_ SESSIONS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated. If LICENSE_MAX_SESSIONS is not explicitly set to a value, the test does not trigger. **Example:** If there are 15 concurrent user sessions and the value of LICENSE_MAX_SESSIONS is 20, the percentage is 75% (15 / 20 x 100). This value is compared against the specified thresholds. **Note:** This test is most useful when session licensing is enabled. Refer to the Oracle Server Reference Manual for more information on LICENSE_MAX_SESSIONS and LICENSE_MAX_ USERS parameters.

Table 2–8 Database Space Management Event Tests

Event Test	Description
Alert File Large	The ALERT file is a special trace file containing a chronological log of messages and errors. Oracle always appends to the file. To control the size of an ALERT file you must manually delete the file when you no longer need it. This event test checks for file size of the ALERT file. If the file is greater than the values specified in the threshold arguments, then a warning or critical alert is generated. **Note:** The ALERT file can be safely deleted while the instance is running, although you might want to make an archived copy of it first.

Table 2–8 Database Space Management Event Tests (Cont.)

Event Test	Description
Archive Full	When running a database in ARCHIVELOG mode, the archiving of the online redo log is enabled. Filled groups of the online redo log are archived, by default, to the destination specified by the LOG_ARCHIVE_DEST initialization parameter. If this destination device becomes full, the database operation is temporarily suspended until disk space is available. If the database is running in ARCHIVELOG mode, this test checks for available redo log destination devices. If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated. If the database is not running in ARCHIVELOG mode, or all archive destinations are standby databases for Oracle8*i*, this test fails to register. **Note:** If you have more than one number for the amount of free space available, this means you have more than one destination. Check the amount of free space for **all** destinations.
Archive Full (%)	The Archive Full (%) event test monitors the same destination device as the Archive Full event test. The Archive Full (%) event test, however, returns the percentage of free space remaining on the log destination. If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated. If the database is not running in ARCHIVELOG mode or all archive destinations are standby databases for Oracle8*i*, this test fails to register. **Note:** If you have more than one number for the amount of free space available, this means you have more than one destination. Check the amount of free space for **all** destinations.
Chained / Migrated Row	In two circumstances the data for a row in a table may be too large to fit into a single data block. This results in row fragmentation. In the first case, the row is too large to fit into one data block when it is first inserted. In this case, the Oracle Server stores the data for the row in a chain of data blocks reserved for that segment. Row chaining (or continuation) most often occurs with large rows, such as rows that contain a column of data type LONG or LONG RAW. Row chaining in these cases is unavoidable without using a DB_BLOCK_SIZE. In the second case, however, a row that originally fit into one data block is updated so that the overall row length increases and the block's free space is already completely filled. In this case, Oracle migrates the data for the entire row to a new data block, assuming the entire row can fit into a new block. Oracle preserves the original row piece of a migrated row to point to the new block containing the migrated row. When a row is chained or migrated, I/O performance associated with this row decreases because Oracle must scan more than one data block to retrieve the information for the row. This event test monitors whether continued rows are found in the segments specified by the Segment name, Segment owner, and Segment type parameters. If continued rows are found, an alert is generated. **Note:** This test is CPU-intensive. You may want to schedule the test for once a day at non-business hours.

Table 2–8 Database Space Management Event Tests (Cont.)

Event Test	Description
Chunk Small	The Oracle Server allocates space for segments in units of one extent. When the existing extents of a segment are full, the Oracle Server allocates another extent for that segment. In order to do so, Oracle searches through the free space in the tablespace containing the segment for the first free, contiguous set of data blocks sufficient to meet the required extent's size. If sufficient space is not found, an error is returned by the Oracle Server. This event test checks for the largest chunk free space in the tablespace specified by the Tablespace name, Segment name, and Segment type parameters. If any table, index, cluster or rollback segments within the tablespace cannot allocate the additional number of extents specified in the thresholds, then a warning or critical alert is generated. **Example:** If the largest chunk of free space in the specified tablespace can only contain 2 extents, then 2 are compared to the threshold values. If 3 are specified for an alert, the alert test is triggered because 3 extents cannot be allocated in the tablespace.
Dump Full	Each server and background process can write to an associated trace file in order to log messages and errors. Background processes and the ALERT file are written to the destination specified by BACKGROUND_DUMP_DEST. Trace files for server processes are written to the destination specified by USER_ DUMP_DEST. This event test checks for available free space on these dump destination devices. If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated.
Dump Full (%)	This event test monitors the same dump destinations as the Dump Full event test. The Dump Full (%) event test, however, returns the percentage of free space remaining on the dump destinations. If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated.
Fast Segment Growth	A segment collection is a group of extents that make up a single table, index, temporary or rollback segment. The Oracle Server offers a practical method of space allocation to segments as they are required to grow. Oracle allows a segment to have multiple extents, which the server allocates automatically when they are needed. For any segment that grows continuously, it is important to carefully monitor that segment's growth pattern. Storage values for the database should be chosen to ensure new extents are not frequently allocated. This event test checks whether any of the segments specified by the Tablespace name, Segment name, and Segment type parameters are allocating extents too quickly. If, for any segment, the number of extents allocated since the event check is greater than the threshold values specified in the threshold arguments, then a warning or critical alert is generated.
Index Rebuild	When an indexed value is updated in the table, the old value is deleted from the index and the new value is inserted into a separate part of the index. The space released by the old value can never be used again. As indexed values are updated or deleted, the amount of unusable space within the index increases, a condition called index stagnation. Because a stagnated index contains a mixture of data and empty areas, scans of the index will be less efficient. This event test monitors whether indexes specified by the Index name, Index owner, Indexed object name, and Indexed object owner parameters suffer from index stagnation. If an index has stagnation, an alert is generated.

Table 2–8 Database Space Management Event Tests (Cont.)

Event Test	Description
Maximum Extents	A segment is a collection of extents that make up a single table, cluster, index, temporary or rollback segment. The MAXEXTENTS segment storage parameter specifies the maximum number of extents that can be allocated to the segment. Once a segment has filled the maximum number of extents, any row insertion will fail with an ORA-01631 error message. This event test checks whether any of the segments specified by the Tablespace name, Segment name, and the Segment type parameters are approaching their maximum extents. If for any segment the maximum number of extents minus the number of existing extents is less than the threshold values specified in the threshold arguments, then a warning or critical alert is generated. **Example:** If the maximum number of extents for a segment is 20 and the number of existing extents is 16, then 4 is compared against the specified threshold values. If 3 is specified for a critical alert and 5 is specified for a warning, a warning is triggered because only 4 extents are available.
Multiple Extents	A segment is a collection of extents that make up a single table, cluster, index, temporary or rollback segment. The Oracle Server allows a segment to have multiple extents, which the server allocates automatically when additional space is required. There is no performance degradation for a segment having multiple extents that are never full-scanned (table and temporary segments only) where the extents are the same size and are also an integral multiple of the multiblock read batch size. No performance degradation is found where extents are 100 or more times larger that the read batch size. Oracle administrators may, however, choose to monitor the number of extents in a segment. This event test checks whether any of the segments specified by the Tablespace name, Segment name, and Segment type parameters have multiple extents. If the number of extents is greater than the threshold values specified in the threshold arguments, then a warning or critical alert is generated. **Note:** The only time multiple extents may cause a performance problem is when a segment is fully scanned and that segment's extent size is **not** a multiple of the multiblock read size.
Snapshot Log Full	A master table's snapshot log keeps track of fast refresh data for all corresponding snapshots. When a snapshot log is created for a master table, Oracle creates an underlying table to support the snapshot log. Oracle automatically tracks which rows in a snapshot log have been used during the refreshes of snapshots, and purges those rows from the log. Oracle does not delete rows from the log until all snapshots have used them. As a result, in certain situations a snapshot log can grow indefinitely when multiple snapshots are based on the same master table. It is best to always try to keep a snapshot log as small as possible to minimize the database space that it uses. This event test checks whether a snapshot log is too large. In order to do this, the test determines the number of snapshot log tables containing more rows than specified by the Snapshot log's table size parameter. If this number is greater than the threshold value specified in the threshold argument, then an alert is generated.
Tablespace Full	As segments within a tablespace grow, the free space within that tablespace decreases. Should free space become insufficient, the creation of new segments or the extension of existing segments will fail. This event test checks for the total free space in the tablespace specified by the Tablespace name. If the percentage of used space is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

Table 2–9 Database Specialized Management Event Tests - Advanced Queuing

Event Test	Description
AQ Expired Messages Count	This data item contains the number of messages for the current queue that are in the 'EXPIRED' state
	This test checks the number of messages in the 'EXPIRED' state specified by the Queue Name(s) parameter. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
AQ Ready Messages Count	This data item contains the number of messages for the current queue in the 'READY' state.
	This test checks the number of messages in the 'READY' state specified by the Queue Name(s) parameter. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
AQ Waiting Messages Count	This data item contains the number of messages for the current queue in the 'WAITING' state.
	This test checks the number of messages in the 'WAITING' state specified by the Queue Name(s) parameter. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–10 Database Specialized Management Event Tests - Cluster Databases

Event Test	Description
Global Cache Converts	This data item represents average convert time in seconds during this sample period. This test checks the Global Cache Converts for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Global Cache Convert Timeouts	This data item represents number of times lock converts in the global cache timed out for each Oracle server instance per second during this sample period.
	This test checks the Global Cache Convert Timeouts for an instance per second for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Global Cache CR Request	This data item represents average time CR block was received during this sample period. This test checks the Global Cache CR Request for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–10 Database Specialized Management Event Tests - Cluster Databases (Cont.)

Event Test	Description
Global Cache CR Timeouts	This data item represents the number of times a foreground process requested a consistent-read (CR) block when the request timed out for each cluster database instance per second during this sample period. This test checks the Global Cache CR Timeouts for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Global Cache FreeList Waits	This data item represents number of times foreground has to wait for a lock element for each cluster database instance per second during this sample period. This test checks the Global Cache Freelist Waits for an instance per second for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Global Cache Gets	This data item represents average get time in seconds during this sample period. This test checks the Global Cache Gets for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Block Class Pings	This data item represents the ping count per second for a block class during this sample period. This test checks the Ping count per second for the block class specified by the Class Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Instance Pings	This data item represents the ping ratio during this sample period. This test checks the Ping Ratio for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Total Pings	This data item represents the ping count per second for a cluster database during this sample period. This test checks the total number of pings per second. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 2–11 Database Specialized Management Event Tests - Data Guard

Event Test	Description
Data Guard - Actual Apply Delay	The difference (in number of archived redo logs) between the current log at the primary site and the last log applied on the standby site.
Data Guard - Data Not Applied	The time difference (in minutes) between the last archived redo log received and the last log applied on the standby.
Data Guard - Logs Not Applied	The difference (in number of archived redo logs) between the last log received and the last log applied on the standby.

Table 2–11 Database Specialized Management Event Tests - Data Guard (Cont.)

Event Test	Description
Data Guard - Logs Not Shipped	The difference (in number of archived redo logs) between the current log on the primary site and the last log shipped to the standby site.
Data Guard - Potential Data Loss	The time difference (in minutes) between the current redo log on the primary site and the last log received on the standby site.
Data Guard - Status	This event test checks the status of the Data Guard configuration. **Note:** If the status is not SUCCESS, then this event test is triggered.

Descriptions of Database Event Tests

The Oracle Database Event Tests are listed in alphabetical order.

% CPU Time

Description

Data item that represents the percentage of time, instance-wide, spent executing instructions by the CPU during this sample period.

This test checks the percentage time spent executing instructions by the CPU, instance-wide, for resources or objects during this sample period. If the % CPU Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaCpuTime / (DeltaTotalWait + DeltaCpuTime)
where:

- DeltaTotalWait: difference of 'sum of time waited for all wait events in v$system_event' between sample end and start
- DeltaCpuTime: difference of 'select value from v$sysstat where name='CPU used by this session' between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: Default is 3

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and percentage of time spent by CPU.

Recommended Frequency
5 minutes

User Action
When CPU is the largest contributor to total response time, it must be broken down to properly understand the problem further. CPU Time is broken down into the following categories:

- Parse CPU time: Amount of CPU used for parsing SQL statements.
- Recursive CPU: Amount of CPU used for parsing row cache statements such as lookups in the data dictionary, executing triggers, PL/SQL, etc.
- Other CPU: Amount of CPU used for tasks such as looking up buffers, fetching rows or index keys, etc.

Selecting this resource and drilling down leads to the CPU Breakdown Chart which shows the breakdown of database CPU usage into its various components.

% Shared Pool Free

Description
This data item represents the percentage of the Shared Pool that is currently marked as free.

This test checks the percentage of Shared Pool that is currently free. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
((Free / Total)*100)
where:

- free: select sum(decode(name,'free memory',bytes)) from v$sgastat
- total: select sum(bytes) from v$sgastat

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and shared pool free percentage.

Recommended Frequency

5 minutes

User Action

If the percentage of Free Memory in the Shared Pool rises above 50%, too much memory has been allocated to the shared pool. This extra memory could be better utilized by other applications on the machine. In this case the size of the Shared Pool should be decreased. This can be accomplished by modifying the shared_pool_size initialization parameter.

To view the current shared pool statistics use the SGA Overview Chart. This chart shows the current SGA parameter settings as well as the size of various components of the SGA.

% Wait Time

Description

Data item representing the percentage of time spent waiting, instance-wide, for resources or objects during this sample period.

This test checks the percentage time spent waiting, instance-wide, for resources or objects during this sample period. If the % Wait Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaTotalWait / (DeltaTotalWait + DeltaCpuTime)
where:

- DeltaTotalWait: difference of 'sum of time waited for all wait events in v$system_event' between sample end and start
- DeltaCpuTime: difference of 'select value from v$sysstat where name='CPU used by this session' between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: Default is 3

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and percentage of time spent waiting.

Recommended Frequency

5 minutes

User Action

Investigate further into which specific wait events are responsible for the bulk of the wait time. Individual wait events may identify unique problems within the database. Diagnosis will be tailored where appropriate through drilldowns specific to individual wait events. Selecting this resource and drilling down will identify the Wait Analysis Overview Chart which shows the breakdown of wait time into specific wait events.

Alert File Large

Description

The ALERT file is a special trace file containing a chronological log of messages and errors. Oracle always appends to the file. To control the size of an ALERT file you must manually delete the file when you no longer need it.

This event test checks for file size of the ALERT file. If the file is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

Parameters

- Critical threshold: File size in kilobytes for critical alert. Default 100,000 kilobytes.
- Warning threshold: File size in kilobytes for warning alert. Default 50,000 kilobytes.

Output

Current size of ALERT file in kilobytes

Recommended Frequency

10 minutes

User Action

Delete the ALERT file to recover disk space. Note this file can be safely deleted while the instance is running, although you might want to make an archived copy of it first.

AQ Expired Messages Count

Description

This data item contains the number of messages for the current queue that are in the 'EXPIRED' state.

This test checks the number of messages in the 'EXPIRED' state specified by the Queue Name(s) parameter. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Select name, expired from gv$aq g ,all_queues d where g.qid = d.qid order by name

Parameters

- Queue Name(s): Name of the queue.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Queue name and number of messages in the 'EXPIRED' state.

Recommended Frequency
5 minutes

User Action
The threshold for the Expired Queue may have been reached because the dequeuing process is not fast enough to process the messages within the specified time. In case of propagation, the propagation process may die. If that is the case the message expires before it gets propagated.

AQ Ready Messages Count

Description
This data item contains the number of messages for the current queue in the 'READY' state.

This test checks the number of messages in the 'READY' state specified by the Queue Name(s) parameter. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
select name, ready from gv$aq g ,all_queues d where g.qid = d.qid order by name

Parameters
- Queue Name(s): Name of the queue.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Queue name and number of messages in the 'READY' state.

Recommended Frequency
5 minutes

User Action

Reaching the threshold of the Ready Queue indicates the process dequeuing the messages is slower than the rate by which messages are put in. Consider increasing the processing speed of the dequeuer processes. This can be done by giving more resource to the dequeuing process or by spawning more dequeuing processes.

AQ Waiting Messages Count

Description

This data item contains the number of messages for the current queue in the 'WAITING' state.

This test checks the number of messages in the 'WAITING' state specified by the Queue Name(s) parameter. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Select name, waiting from gv$aq g ,all_queues d where g.qid = d.qid order by name.

Parameters

- Queue Name(s): Name of the queue.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Queue name and number of messages in the 'WAITING' state.

Recommended Frequency

5 minutes

User Action

This data item reports on the number of messages that are in the queue that are not meant to be processed at this time, but are waiting for certain time period before they are allowed to be processed. When the required waiting period expires, the

messages will be moved into the 'READY' state and will then be available to consumers.

Archive Full

Description

When running a database in ARCHIVELOG mode, the archiving of the online redo log is enabled. Filled groups of the online redo log are archived, by default, to the destination specified by the LOG_ARCHIVE_DEST initialization parameter. If this destination device becomes full, the database operation is temporarily suspended until disk space is available.

If the database is running in ARCHIVELOG mode, this event test checks for available redo log destination devices. If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated.

If the database is not running in ARCHIVELOG mode, or all archive destinations are standby databases for Oracle8*i*, this event test fails to register.

Parameters

- Critical threshold: Free space threshold in kilobytes for critical alert.
- Warning threshold: Free space threshold in kilobytes for warning alert.

Output

- For releases of the Intelligent Agent prior to 9*i*: Space available on the destination drive in kilobytes. **Note:** If you have more than one number for the amount of free space available, this means you have more than one destination. Check the amount of free space for all destinations.
- For the 9*i* release of the Intelligent Agent: Destination and its current used space in kilobytes

Recommended Frequency

10 minutes

User Action

Verify the device specified in the initialization parameter LOG_ARCHIVE_DEST is set up properly for archiving.

- For Oracle7, verify that the LOG_ARCHIVE_DEST initialization parameter is set up properly for archiving.

- For Oracle8, verify that the LOG_ARCHIVE_DEST and LOG_ARCHIVE_DUPLEX_DEST initialization parameters are set up properly for archiving.
- For Oracle8*i*, there are two methods you can use to specify archive destinations. The first method is to use the LOG_ARCHIVE_DEST_n parameter (where n is an integer from 1 to 5) to specify from one to five different destinations for archival. Each numerically-suffixed parameter uniquely identifies an individual destination, for example, LOG_ARCHIVE_DEST_1, LOG_ARCHIVE_DEST_2, and so on. The second method, which allows you to specify a maximum of two locations, is to use the LOG_ARCHIVE_DEST parameter to specify a primary archive destination and the LOG_ARCHIVE_DUPLEX_DEST parameter to determine an optional secondary location.

If the LOG_ARCHIVE_DEST initialization parameter is set up correctly and this event test triggers, then free up more space in the destination specified by the archive destination parameters.

Archive Full (%)

Description

The Archive Full (%) event test monitors the same destination device as the Archive Full event test. The Archive Full (%) event test, however, returns the percentage of free space remaining on the log destination.

If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated.

If the database is not running in ARCHIVELOG mode or all archive destinations are standby databases for Oracle8*i*, this event test fails to register.

Parameters

- Critical threshold: Percentage of free space threshold for critical alert. Default is 30%.
- Warning threshold: Percentage of free space threshold for warning alert. Default is 50%.

Output

For releases of the Intelligent Agent prior to 9*i*: Percentage of free space available on the destination drive. **Note:** If you have more than one number for the percentage of free space available, this means you have more than one destination. Check the percentage of free space for all destinations.

For the 9*i* release of the Intelligent Agent: Destination and its current used space in percentage

Recommended Frequency
10 minutes

User Action
Verify the device specified in the initialization parameter LOG_ARCHIVE_DEST is set up properly for archiving.

For Oracle7, verify that the LOG_ARCHIVE_DEST initialization parameter is set up properly for archiving.

For Oracle8, verify that the LOG_ARCHIVE_DEST and LOG_ARCHIVE_DUPLEX_DEST initialization parameters are set up properly for archiving.

For Oracle8*i*, there are two methods you can use to specify archive destinations. The first method is to use the LOG_ARCHIVE_DEST_n parameter (where n is an integer from 1 to 5) to specify from one to five different destinations for archival. Each numerically-suffixed parameter uniquely identifies an individual destination, for example, LOG_ARCHIVE_DEST_1, LOG_ARCHIVE_DEST_2, and so on. The second method, which allows you to specify a maximum of two locations, is to use the LOG_ARCHIVE_DEST parameter to specify a primary archive destination and the LOG_ARCHIVE_DUPLEX_DEST parameter to determine an optional secondary location.

If the LOG_ARCHIVE_DEST initialization parameter is set up correctly and this event test triggers, then free up more space in the destination specified by the archive destination parameters.

Archiver Hung

Description
This event test signifies that the archiver of the database being monitored has been temporarily suspended since the last sample time.

If the database is running in ARCHIVELOG mode, an alert is displayed when archiving is hung (ORA-00257) messages are written to the ALERT file. The ALERT file is a special trace file containing a chronological log of messages and errors.

If the database is not running in ARCHIVELOG mode, this test will not register.

Parameters
None

Output
ALERT log error messages since last sample time

Recommended Frequency
30 seconds

User Action
Examine ALERT log and archiver trace file for additional information; however, the most likely cause of this message is that the destination device is out of space to store the redo log file. Verify the device specified in the initialization parameter ARCHIVE_LOG_DEST is set up properly for archiving. **Note:** This event does not automatically clear since there is no automatic way of determining when the problem has been resolved. Hence, you need to manually clear the event once the problem is fixed.

Average File Read Time

Description
This data item represents the average time spent performing a read from this datafile during the sample period. This value will always be 0 unless the TIMED_ STATISTICS parameter is TRUE.

The value of this item is reported in 100ths of a second. Therefore a value of 100 would mean on average that one second of time was spent per physical read to this file during the last sample period.

There is a drilldown chart available from this chart called Timed Statistics Chart. This chart shows the current value for the TIMED_STATISTICS parameter. Use the Turn On Timed Statistics drilldown to turn on timed statistics for the instance.

This test checks the average time spent performing a read for a file specified by File Name(s) parameter during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
DeltaReadTime / DeltaPhysicalReads
where:

- DeltaReadTime: difference in 'select readtim from v$filestat' between sample end and start

- DeltaPhysicalReads: difference in 'select phyrds from v$filestat' between sample end and start

Parameters

- File Name(s): Name of the file.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

File name and average file read time in 100ths of a second.

Recommended Frequency

5 minutes

User Action

This statistic shows the average read time which is the average amount of time spent for each read against the datafile. This number may be as important as the number of reads against the file. Comparing read times across multiple datafiles shows you which datafiles are slower than others. Read times may be improved if contention is reduced on the datafile, although read times may be high due to the file residing on a slow disk. You need to identify whether the SQL accessing the file can be tuned, as well as the underlying characteristics of the hardware device.

Use SQL tuning to first reduce the IO rates to this file. Often high physical read rates are attributed to queries that are performing full table scans. Full table scans, especially of large tables, should be avoided whenever possible. To identify the SQL statements that are causing the most physical reads use the Top SQL (Physical Reads) Chart. This quickly identifies the SQL statements that are prime candidates for tuning.

If your SQL statements are already adequately tuned for I/O, you can use the information in this chart to determine whether some tablespaces within the file must be separated in order to spread the I/O load more evenly across the available disks.

Average File Write Time

Description

This data item represents the average time spent performing a write to this datafile during the sample period. This value will always be 0 unless the TIMED_ STATISTICS parameter is TRUE.

The value of this item is reported in 100ths of a second. Therefore a value of 100 would indicate on average that one second of time was spent per physical write to this file during the last sample period.

There is a drilldown chart available from this chart called Timed Statistics Chart. This chart shows the current value for the TIMED_STATISTICS parameter. Use the Turn On Timed Statistics drilldown to turn on timed statistics for the instance.

This test checks the average time spent performing a write for a file specified by File Name(s) parameter during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaWriteTime / DeltaPhysicalWrites
where:

- DeltaWriteTime: difference in 'select writetim from v$filestat' between sample end and start
- DeltaPhysicalWrites: difference in 'select phywrts from v$filestat' between sample end and start

Parameters

- File Name(s): Name of the file.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

File name and average file write time in 100ths of a second.

Recommended Frequency

5 minutes

User Action

A large value for average write time to a particular file might suggest that either the underlying hardware is slow or that there is enough contention on the disk to slow it down. If a particular datafile is experiencing a slow average write time, you can further determine what tablespaces are located within the file.

If the file contains the TEMP tablespace, you can view the Top Sessions by Disk Sorts Chart to determine which sessions are performing the most sorts. The SQL statements being executed by these sessions should be examined to see if their sorting can be tuned or reduced. Increasing the SORT_AREA_SIZE initialization parameter may help move more of these sorts into memory and off the disk.

If the physical writes are caused by inserts or modifications into multiple tables within the file you may want to further investigate separating the tables into individual datafiles. Ideally these datafiles would reside on separate disks.

Average Redo Write Size Per Second

Description

This data item represents the amount of redo, in bytes, generated per second during this sample period.

The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries can be used for database recovery if necessary.

This test checks the amount of redo in bytes generated per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaRedoSize / Seconds
where:

- DeltaRedoSize: difference in 'select value from v$sysstat where name='redo size'' between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and redo size in bytes per second.

Recommended Frequency

5 minutes

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when redo entries are buffered to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer should waiting be a problem. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

Average Redo Write Size Per Transaction

Description

This data item represents the amount of redo, in bytes, generated per transaction during this sample period.

The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries are used for database recovery, if necessary.

The value of this statistic is zero if there have been no write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the amount of redo in bytes generated per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaRedoSize / DeltaTransactions
where:

- DeltaRedoSize: difference in 'select value from v$sysstat where name='redo size'' between end and start of sample period
- Transactions: difference in 'select value from v$sysstat where name = 'user commits'' between end and start of sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and amount of redo in bytes generated per transaction.

Recommended Frequency

5 minutes

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when buffering redo entries to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer should waiting be a problem. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

Average Rows Per Sort

Description

This data item represents the average number of rows per sort during this sample period.

This test checks the average number of rows per sort during sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

(DeltaSortRows / (DeltaDiskSorts + DeltaMemorySorts)) * 100
where:

- DeltaSortRows: difference in 'select value from v$sysstat where name='sorts (rows)" between sample end and start
- DeltaMemorySorts: difference in 'select value from v$sysstat where name='sorts (memory)" between sample end and start
- DeltaDiskSorts: difference in 'select value from v$sysstat where name='sorts (disk)" between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and the number of rows per sort.

Recommended Frequency

5 minutes

User Action

This statistic displays the average number of rows that are being processed per sort. The size provides information about the sort size of the database. This can help you to determine the SORT_AREA_SIZE appropriately. If the rows per sort are high,

you should investigate the sessions and SQL performing the most sorts to see if those SQL statements can be tuned to reduce the size of the sort sample set.

The sessions that are performing the most sorts should be identified, such that the SQL they are executing can be further identified. The sort area sizes for the database may be sized correctly and the application SQL may be performing unwanted or excessive sorts. The sessions performing the most sorts are available through the Top Sessions by Disk Sorts drilldown.

Further drilldown into the session performing the most disk sorts with the Current SQL Chart displays the SQL statement responsible for the disk sorts. Further investigation on how to best tune a particular SQL statement can be done by using the Explain Plan drilldown, or if you are on NT, the Tune SQL Statement drilldown as well.

The Top SQL (Sorts) Chart provides a mechanism to quickly display the SQL statements in the cache presented in sorted order by their number of sort operations. This is an alternative to viewing the sort of current sessions. It allows you to view sort activity via SQL statements and contains cumulative statistics for all executions of that statement.

If the top sessions and their associated SQL statements seem to be okay, you can drill down to see a more complete breakdown of sort statistics and initialization parameters with the Sort Statistics At A Glance Chart.

If excessive sorts are taking place on disk and the queries are correct, consider increasing the SORT_AREA_SIZE initialization parameter to increase the size of the sort area. A larger sort area allows the Oracle Server to keep sorts in memory, reducing the number of I/O operations required to do an equivalent amount of work using the current sort area size.

Block Class Pings

Description

This data item represents the ping count per second for a block class during this sample period.

This test checks the Ping count per second for the block class specified by the Class Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Parameters

- Class Name(s): The name of the class.
- Warning Threshold: Default is 1.
- Critical Threshold: Default is 5.
- Number of Occurrences: Default is 1.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Class name and pings per second.

Recommended Frequency

5 minutes

Broken Jobs

Description

The Oracle server job queue is a database table that stores information about local jobs such as the PL / SQL call to execute for a job such as when to run a job. Database replication is also managed by using Oracle's job queue mechanism using jobs to push deferred transactions to remote master sites, to purge applied transactions from the deferred transaction queue or to refresh snapshot refresh groups.

A job can be broken in two ways:

Oracle has failed to successfully execute the job after sixteen attempts

The job has been explicitly marked as broken by using the procedure DBMS_ JOB.BROKEN

This event test checks for broken DBMS jobs. A critical alert is generated if the number of broken jobs exceeds the value specified by the threshold argument.

Parameters

Critical threshold: Threshold for critical alert (number of jobs). Default is 0 jobs.

Output

Job identifiers of broken DBMS jobs

Recommended Frequency
60 seconds

User Action
Check the ALERT log and trace files for error information. Correct the problem that is preventing the job from running. Force immediate re-execution of the job by calling DBMS_JOB.RUN.

Buffer Cache Hit %

Description
This data item represents the data block buffer cache efficiency, as measured by the percentage of times the data block requested by the query is in memory.

Effective use of the buffer cache can greatly reduce the I/O load on the database. If the buffer cache is too small, frequently accessed data will be flushed from the buffer cache too quickly which forces the information to be re-fetched from disk. Since disk access is much slower than memory access, application performance will suffer. In addition, the extra burden imposed on the I/O subsystem could introduce a bottleneck at one or more devices which would further degrade performance.

This test checks the percentage of buffer requests that were already in buffer cache. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
((DeltaLogicalGets - (DeltaPhysicalReads - DeltaPhysicalReadsDirect)) / DeltaLogicalGets) * 100
where:

- DeltaLogicalGets: difference in 'select value from v$sysstat where name='session logical reads'' between sample end and start
- DeltaPhysicalReads: difference in 'select value from v$sysstat where name='physical reads'' between sample end and start
- DeltaPhysicalReadsDirect: difference in 'select value from v$sysstat where name='physical reads direct'' between sample end and start (Oracle 8*i*)

Parameters
- Warning Threshold: Default is 80. The value can be between 0.0 and 100.0.
- Critical Threshold: Default is 70. The value can be between 0.0 and 100.0.

- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance Name and buffer cache hit percentage.

Recommended Frequency
5 minutes

User Action
A low buffer cache hit ratio means that the server must often go to disk to retrieve the buffers required to satisfy a query. The queries that perform the most physical reads lower the numerical value of this statistic. Typically queries that perform full table scans force large amounts of buffers into the cache, aging out other buffers that may be required by other queries later. The Top Sessions by Physical Reads Chart will show the sessions performing the most reads and through further drilldown their associated queries can be identified. Similarly, the Top SQL (Physical Reads) Chart shows which SQL statements are performing the most physical reads. The statements performing the most I/O should be looked at for tuning.

The difference between the two is that the Top Sessions chart shows the sessions that are responsible for the physical reads at any given moment. The Top SQL view shows all SQL that is still in the cache. The top statement may not be executing currently, and thus not responsible for the current poor buffer cache hit ratio.

If the queries seem to be well tuned, the size of the buffer cache also determines how often buffers need to be fetched from disk. The DB_BLOCK_BUFFERS initialization parameter determines the number of database buffers available in the buffer cache. It is one of the primary parameters which contribute to the total memory requirements of the SGA on the instance. The DB_BLOCK_BUFFERS parameter, together with the DB_BLOCK_SIZE parameter, controls the total size of the buffer cache. Since DB_BLOCK_SIZE can only be specified when the database is first created, normally the size of the buffer cache size is controlled using the DB_BLOCK_BUFFERS parameter.

Consider increasing the DB_BLOCK_BUFFERS initialization parameter to increase the size of the buffer cache. This increase allows the Oracle Server to keep more information in memory, thus reducing the number of I/O operations required to do an equivalent amount of work using the current cache size.

Chained/Migrated Row

Description

In two circumstances the data for a row in a table may be too large to fit into a single data block. This results in row fragmentation.

In the first case, the row is too large to fit into one data block when it is first inserted. In this case, the Oracle Server stores the data for the row in a chain of data blocks reserved for that segment. Row chaining (or continuation) most often occurs with large rows, such as rows that contain a column of data type LONG or LONG RAW. Row chaining in these cases is unavoidable without increasing the DB_ BLOCK_SIZE.

In the second case, however, a row that originally fit into one data block is updated so that the overall row length increases and the block's free space is already completely filled. In this case, Oracle migrates the data for the entire row to a new data block, assuming the entire row can fit into a new block. Oracle preserves the original row piece of a migrated row to point to the new block containing the migrated row.

When a row is chained or migrated, I/O performance associated with this row decreases because Oracle must scan more than one data block to retrieve the information for the row.

This event test monitors whether continued rows are found in the segments specified by the Segment name, Segment owner, and Segment type parameters. If continued rows are found, an alert is generated.

Parameters

- Segment name: Filter of the segment names to be monitored, or * for all segments. Default is *.
- Segment owner: Filter of the segment owners to be monitored, or * for all owners. Default is *. Owners SYS and SYSTEM are excluded.
- Segment type: Filter of the segment types to be monitored, or * for all segment types. Default is *. Only segment type TABLE and CLUSTER are allowed.

Note: All filters must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'. There are higher resource requirements if there is a large number of objects being monitored at high frequencies, for example, checking the space for all 200 segments every 2 minutes. Where possible, Oracle recommends that you use the filters to narrow the scope of the objects being monitored. Also, set the polling schedule to a value that is appropriate to your environment. For example, segments

that do not grow rapidly in size may be checked every 2 days instead of every 5 minutes.

Output
Names of segments containing chained or migrated rows.

Recommended Frequency
1 day

Note: This event test is CPU-intensive. You may want to schedule the test for once a day at non-business hours.

User Action
If a segment containing fragmented rows has been detected, there are two ways to solve the problem. If rows are not likely to continue growing, rebuild the table. Row fragmentation is eliminated as rows are tightly packed into each database block during re-creation.

If rows are likely to continue growing through updates, consider increasing the segment's PCTFREE value to reduce the likelihood of future row fragmentation.

Note: To determine what needs to be done, the Chained / Migrated Row event test gathers statistics using the ANALYZE command. Running this command may be a resource-intensive operation. Therefore, Oracle recommends running the Chained / Migrated Row event test during off-peak periods.

Chunk Small

Description
The Oracle Server allocates space for segments in units of one extent. When the existing extents of a segment are full, the Oracle Server allocates another extent for that segment. In order to do so, Oracle searches through the free space in the tablespace containing the segment for the first free, contiguous set of data blocks sufficient to meet the required extent's size. If sufficient space is not found, an error is returned by the Oracle Server.

This event test checks for the largest chunk free space in the tablespace specified by the Tablespace name, Segment name, and Segment type parameters. If any table, index, cluster or rollback segments within the tablespace cannot allocate the additional number of extents specified in the thresholds, then a warning or critical alert is generated.

Example

If the largest chunk of free space in the specified tablespace can only contain 2 extents, then 2 is compared to the threshold values. If 3 extents are specified for a critical alert, the critical test is triggered because 3 extents cannot be allocated in the tablespace.

Parameters

- Tablespace name filter: Filter of the tablespace names to be monitored, or * for all tablespaces. Tablespaces that are either temporary, read-only, or off-line are excluded. For Oracle Server release 8*i* or higher, tablespaces with allocation_type='SYSTEM' are excluded. Default is *.
- Segment name filter: Filter of the segments to be monitored, or * for all segments. Default is *.
- Segment type filter: Filter of the segment types to be monitored, or * for all segment types. Segment type CACHE and DEFERRED ROLLBACK are excluded.
- Critical threshold: Threshold for critical alert (number of extents). Default extent is 1.
- Warning threshold: Threshold for warning alert (number of extents). Default is 2 extents.

Note: All filters must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'. There are higher resource requirements if there is a large number of objects being monitored at high frequencies, for example, checking the space for all 200 segments every 2 minutes. Where possible, Oracle recommends that you use the filters to narrow the scope of the objects being monitored. Also, set the polling schedule to a value that is appropriate to your environment. For example, segments that do not grow rapidly in size may be checked every 2 days instead of every 5 minutes.

Output

- Segment name where the additional extents cannot be allocated.
- Tablespace name containing the segment.
- Maximum size of contiguous free space in bytes for the tablespace.

Recommended Frequency

10 minutes

User Action

Increase the size of the tablespace by enabling automatic extension for one of its existing data files, manually resizing one of its existing data files or adding a new datafile.

Or if the tablespace is suffering from tablespace free space fragmentation problems, consider reorganizing the entire tablespace by dropping and recreating all segments within that tablespace. When reorganizing a tablespace, consider making the extents to be sized as integral divisors of the usable size of the data files in which they reside. Try to limit the extent sizes used in the tablespace to be no more than 2 or 3 different extent sizes. Ensure extents within a segment are the same size or a multiple of each other by specifying STORAGE parameters where NEXT=INITIAL and PCTINCREASE = 0. For segments that are linearly scanned, chose an extent size is a multiple of the number of blocks read during each multiblock read.

Note: Running the Chunk Small event test may be a resource-intensive operation. Therefore, Oracle recommends running the Chunk Small event test during off-peak periods.

Commit %

Description

This data item represents the percentage of transactions that ended as commits rather than rollbacks during this sample period.

This test checks the percentage of transactions that end as commits, as opposed to rollbacks. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

(DeltaCommits / (DeltaCommits + DeltaRollbacks)) * 100.0
where:

- DeltaCommits: difference of 'select value from v$sysstat where name='user commits'' between sample end and start
- DeltaRollbacks: difference of 'select value from v$sysstat where name='user rollbacks'' between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and commit percentage.

Recommended Frequency
5 minutes

User Action
This statistic is an indication of how often transactions are completing successfully. A low percentage means that users are issuing the ROLLBACK statement or encountering errors in their transactions. You should investigate further to determine whether the rollbacks are part of some faulty application logic or due to errors occurring through database access.

Commits Per Second

Description
This data item represents the number of user commits performed, per second during the sample period. When a user commits a transaction, the redo generated that reflects the changes made to database blocks must be written to disk. Commits often represent the closest thing to a user transaction rate.

This test checks the number of user commits per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
DeltaCommits / Seconds
where:

- DeltaCommits: difference in 'select value from v$sysstat where name='user commits'' between end and start of sample period
- Seconds: number of seconds in sample period

Parameters
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and the number of commits per second.

Recommended Frequency
5 minutes

User Action
This statistic is an indication of how much work is being accomplished within the database. A spike in the transaction rate may not necessarily be bad. If response times stay close to normal, it means your system can handle the added load. Actually, a drop in transaction rates and an increase in response time may be indicators of problems. Depending upon the application, transaction loads may vary widely across different times of the day.

Commits Per Transaction

Description
This data item represents the number of user commits performed, per transaction during the sample period. When a user commits a transaction, the redo generated that reflects the changes made to database blocks must be written to disk. Commits often represent the closest thing to a user transaction rate.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the number of user commits per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
DeltaCommits / Transactions
where:

- DeltaCommits: difference in 'select value from v$sysstat where name='user commits'' between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and the number of commits per transaction.

Recommended Frequency

5 minutes

User Action

This statistic is an indication of how much work is being accomplished within the database. A spike in the transaction rate may not necessarily be bad. If response times stay close to normal, it means your system can handle the added load. Actually, a drop in transaction rates and an increase in response time may be indicators of problems. Depending upon the application, transaction loads may vary widely across different times of the day.

Data Block Corruption

Description

This event test signifies that the database being monitored has generated a corrupted block error to the ALERT file since the last sample time. The ALERT file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when data block corrupted messages are written to the ALERT file.

Parameters

None

Output

- For Agents prior to release 8.1.7: Segment name containing the data block specified by the file ID and block number in the ORA-01578 message.
- For Agent release 8.1.7 or higher: Alert log error messages (ORA-01157, ORA-27048) indicate a data block is corrupted.

Recommended Frequency

30 seconds

User Action

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

Data Dictionary Hit %

Description

This data item represents dictionary cache efficiency as measured by the percentage of requests against the dictionary data that were already in memory. It is important to determine whether the misses on the data dictionary are actually affecting the performance of the Oracle Server.

The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache, and the other cache structures that are specific to a particular instance configuration.

Misses on the data dictionary cache are to be expected in some cases. Upon instance startup, the data dictionary cache contains no data, so any SQL statement issued is likely to result in cache misses. As more data is read into the cache, the likelihood of cache misses should decrease. Eventually the database should reach a steady state in which the most frequently used dictionary data is in the cache. At this point, very few cache misses should occur. To tune the cache, examine its activity only after your application has been running.

This test checks the percentage of requests against the data dictionary that were found in the Shared Pool. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

(Gets / Misses) * 100
where:

- Misses: select sum(getmisses) from v$rowcache
- Gets: select sum(gets) from v$rowcache

Parameters

- Warning Threshold: Default is 90.0. The value can be between 0.0 and 100.0.
- Critical Threshold: Default is 85.0. The value can be between 0.0 and 100.0.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and data dictionary hit percentage.

Recommended Frequency

5 minutes

User Action

If the percentage of gets is below %90 to %85, consider increasing SHARED_POOL_SIZE to decrease the frequency in which dictionary data is being flushed from the shared pool to make room for new data. To increase the memory available to the cache, increase the value of the initialization parameter SHARED_POOL_SIZE.

Data Dictionary Miss Ratio

Description

The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache and the other cache structures that are specific to a particular instance configuration.

The dictionary cache efficiency, as measured by the miss ratio, records the percentage of times the dictionary data was not already in memory.

The shared pool mechanism can greatly reduce system resource consumption in at least three ways:

- Parse time is avoided if the SQL statement is already in the shared pool.

- Application memory overhead is reduced, since all applications utilize the same pool of shared SQL statements and dictionary resources.
- I/O resources are saved, since dictionary elements which are in the shared pool do not require access.

If the shared pool is too small, users will consume additional resources to complete a database operation. For dictionary cache access, the overhead is primarily the additional I/O since the dictionary cache references that have been displaced from the cache will need to be re-fetched from disk.

This event test monitors the data dictionary cache miss ratio (percentage of failures) against the values specified by the threshold arguments. If the number of occurrences exceeds the values specified, then a warning or critical alert is generated.

Parameters

- Number of occurrences: Number of consecutive occurrences that the data dictionary cache miss ratio is greater than or equal to the thresholds before a warning or critical alert is generated. Default is 3.
- Critical threshold: Threshold for critical alert (%). Default is 15%.
- Warning threshold: Threshold for warning alert (%). Default is 10%.

Output

Current ratio

Recommended Frequency

30 seconds

User Action

The SHARED_POOL_SIZE initialization parameters controls the total size of the shared pool. Consider increasing SHARED_POOL_SIZE in order to decrease the frequency in which dictionary data is being flushed from the shared pool in order to make room for new data.

Note: For Oracle Intelligent Agent release 9*i*, this event test has been obsoleted. It is recommended that you use the Data Dictionary Hit Ratio event test. This event test is kept for backward compatibility with older versions of the Intelligent Agent.

Database Alert

Description

This event test signifies that the database being monitored has generated errors to the ALERT log file since the last sample time. The ALERT log file is a special trace file containing a chronological log of messages and errors. An alert event is triggered when Oracle Exception (ORA-006xx), deadlock detected (ORA-00060), or data block corrupted (ORA-01578) messages are written to the ALERT log file. A warning is displayed when other ORA messages are written to the ALERT log file.

Parameters

None

Output

Alert log error messages since last sample time

Recommended Frequency

60 seconds

User Action

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

Note: This event is valid only for releases of the Intelligent Agent prior to 9*i*.

Datafile Limit

Description

The DB_FILES initialization parameter specifies the maximum number of database files that can be opened for this database.

This event test checks for the utilization of the datafile resource against the values (percentages) specified by the threshold arguments. If the percentage of data files currently used to the limit set in the DB_FILES initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated.

Example

If 30 data files are used and the value of DB_FILES is 40, the percentage is 75% (30 / 40 x 100). This value is compared against the specified thresholds.

Parameters

- Critical threshold: Threshold value for critical alert (%). Default is 90%.
- Warning threshold: Threshold value for warning alert (%). Default is 80%.

Output

Current value and the limit specified by DB_FILES

User Action

Verify the current number of data files in use by the database. Increase the DB_FILES instance parameter, if the current value for DB_FILES is less than MAXDATAFILES.

DBWR Checkpoints

Description

This data item represents the number of times, per second, during this sample period DBWn was asked to scan the cache and write all blocks marked for a checkpoint.

The database writer process (DBWn) writes the contents of buffers to datafiles. The DBWn processes are responsible for writing modified (dirty) buffers in the database buffer cache to disk.

When a buffer in the database buffer cache is modified, it is marked dirty. The primary job of the DBWn process is to keep the buffer cache clean by writing dirty buffers to disk. As buffers are dirtied by user processes, the number of free buffers diminishes. If the number of free buffers drops too low, user processes that must read blocks from disk into the cache are not able to find free buffers. DBWn manages the buffer cache so that user processes can always find free buffers.

When the Oracle Server process cannot find a clean reusable buffer after scanning a threshold of buffers, it signals DBWn to write. When this request to make free buffers is received, DBWn writes the least recently used (LRU) buffers to disk. By writing the least recently used dirty buffers to disk, DBWn improves the performance of finding free buffers while keeping recently used buffers resident in memory. For example, blocks that are part of frequently accessed small tables or indexes are kept in the cache so that they do not need to be read in again from disk. The LRU algorithm keeps more frequently accessed blocks in the buffer cache so that when a buffer is written to disk, it is unlikely to contain data that may be useful soon.

Additionally, DBWn periodically writes buffers to advance the checkpoint which is the position in the redo log from which crash or instance recovery would need to begin.

This test checks the number of times DBWR was asked to advance the checkpoint. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaCheckpoints / Seconds
where:

- DeltaCheckpoints: difference in 'select value from v$sysstat where name='DBWR checkpoints" between sample end and start
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and DBWR checkpoints per second.

Recommended Frequency

5 minutes

User Action

A checkpoint tells the DBWR to write out modified buffers to disk. This write operation is different from the make free request in that the modified buffers are not marked as free by the DBWR process. Dirty buffers may also be written to disk at this time and freed.

The write size is dictated by the _db_block_checkpoint_batch parameter. If writing, and subsequently waiting for checkpoints to complete is a problem, the checkpoint completed event displays in the Top Waits by Time Waited Chart or the Sessions Waiting for this Event Chart.

If the database is often waiting for checkpoints to complete you may want to increase the time between checkpoints by checking the init.ora parameter db_block_checkpoint_batch: select name, value, isdefault from v$parameter where name = 'db_block_checkpoint_batch' The value should be large enough to take advantage of parallel writes. The DBWR uses a write batch that is calculated like this: ('db_files' * 'db_file_simultaneous_writes')/2 The write_batch is also limited by two other factors:

- A port specific limit on the numbers of I/Os (compile time constant).
- 1/4 of the number of buffers in the SGA.

The db_block_checkpoint_batch is always smaller or equal to the _db_block_write_batch. You can also consider enabling the check point process.

Deferred Transactions

Description

Oracle uses deferred transactions to propagate data-level changes asynchronously among master sites in an advanced replication system as well as from an updatable snapshot to its master table.

This event test checks for the number of deferred transactions. An alert is generated if the number of deferred transactions exceeds the value specified by the threshold argument.

Parameters

Threshold for alert (number of transactions). Default is 100 transactions.

Output

Number of deferred transactions

Recommended Frequency

30 seconds

User Action

When the advanced replication facility pushes a deferred transaction to a remote site, it uses a distributed transaction to ensure that the transaction has been properly committed at the remote site before the transaction is removed for the queue at the local site. If transactions are not being pushed to a given remote site, verify that the destination for the transaction was correctly specified. If you specify a destination database when calling DBMS_DEFER_SYS.SCHEDULE_EXECUTION using the

DBLINK parameter or DBMS_DEFER_SYS.EXECUTE using the DESTINATION parameter, make sure the full database link is provided.

Wrong view destinations can lead to erroneous deferred transaction behavior. Verify the DEFCALLEST and DEFTRANDEST views are the definitions from the CATREPC.SQL not the ones from CATDEFER.SQL.

Disk I/O

Description

This event test monitors the real time database physical I/O rate (requests/seconds) against the values specified by the threshold arguments. If the Disk I/O rate exceeds the threshold values entered for the specified number of occurrences, then a warning or critical alert is generated.

Parameters

- Number of occurrences: Number of consecutive occurrences that I/O rate exceeds thresholds before a warning or critical alert is generated. Default is 3.
- Critical threshold: Threshold for critical alert (requests/seconds). No default provided.
- Warning threshold: Threshold for warning alert (requests/seconds). No default provided.

Output

Current rate in requests/second

Recommended Frequency

30 seconds

User Action

Determine whether the I/O rate is having a negative impact to performance by investigating the disk queue lengths for high I/O devices. It may be necessary to move data files around to balance any identified bottlenecks. Other tuning efforts such as adjusting indexes to reduce the number of full table scans can also reduce I/O load.

If no bottlenecks are evident, increase the I/O rate threshold values.

Note: For Oracle Intelligent Agent release 9*i*, this event test has been obsoleted. It is recommended that you use the File Read Rate and File Write Rate event tests. This event test is kept for backward compatibility with older versions of the Intelligent Agent.

Disk Sorts Per Second

Description

This data item represents the number of sorts going to disk per second for this sample period.

For best performance, most sorts should occur in memory, because sorts to disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption.

This test checks the number of sorts performed to disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaDiskSorts / Seconds
where:

- DeltaDiskSorts: difference in 'select value from v$sysstat where name='sorts (disk)" between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and disk sorts per second.

Recommended Frequency

5 minutes

User Action

The sessions that are performing the most sorts should be identified, such that the SQL they are executing can be further identified. The sort area sizes for the database may be sized correctly, the application SQL may be performing unwanted or

excessive sorts. The sessions performing the most sorts are available through the Top Sessions by Disk Sorts drilldown.

Further drilldown into the session performing the most disk sorts with the Current SQL Chart will show you the SQL statement responsible for the disk sorts. Further investigation on how to best tune a particular SQL statement can be done by using the Explain Plan drilldown, or if you are on NT, the Tune SQL Statement drilldown as well.

The Top SQL (Sorts) Chart provides a mechanism to quickly display the SQL statements in the cache, presented in sorted order by their number sort operations. This is an alternative to viewing sort of current sessions, it allows you to view sort activity via SQL statements, and will contain cumulative statistics for all executions of that statement.

If the top sessions and their associated SQL statements seem to be okay, you can drilldown to see a more complete breakdown of sort statistics and initialization parameters with the Sort Statistics At A Glance Chart.

If excessive sorts are taking place on disk, and the query's are correct, consider increasing the SORT_AREA_SIZE initialization parameter to increase the size of the sort area. A larger sort area will allow the Oracle Server to keep sorts in memory, reducing the number of I/O operations required to do an equivalent amount of work using the current sort area size.

Disk Sorts Per Transaction

Description

This data item represents the number of sorts going to disk per transactions for this sample period.

For best performance, most sorts should occur in memory, because sorts to disks are expensive to perform. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the number of sorts performed to disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
DeltaDiskSorts / Transactions
where:

- DeltaDiskSorts: difference in 'select value from v$sysstat where name='sorts (disk)" between end and start of sample period
- Transactions: number of transactions in sample period

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and disk sorts per transaction.

Recommended Frequency
5 minutes

User Action
The sessions that are performing the most sorts should be identified, such that the SQL they are executing can be further identified. The sort area sizes for the database may be sized correctly, the application SQL may be performing unwanted or excessive sorts. The sessions performing the most sorts are available through the Top Sessions by Disk Sorts drilldown.

Further drilldown into the session performing the most disk sorts with the Current SQL Chart will show you the SQL statement responsible for the disk sorts. Further investigation on how to best tune a particular SQL statement can be done by using the Explain Plan drilldown, or if you are on NT, the Tune SQL Statement drilldown as well.

The Top SQL (Sorts) Chart provides a mechanism to quickly display the SQL statements in the cache, presented in sorted order by their number sort operations. This is an alternative to viewing sort of current sessions, it allows you to view sort activity via SQL statements, and will contain cumulative statistics for all executions of that statement.

If the top sessions and their associated SQL statements seem to be okay, you can drilldown to see a more complete breakdown of sort statistics and initialization parameters with the Sort Statistics At A Glance Chart.

If excessive sorts are taking place on disk, and the query's are correct, consider increasing the SORT_AREA_SIZE initialization parameter to increase the size of the sort area. A larger sort area will allow the Oracle Server to keep sorts in memory, reducing the number of I/O operations required to do an equivalent amount of work using the current sort area size.

Dump Full

Description

Each server and background process can write to an associated trace file in order to log messages and errors. Background processes and the ALERT file are written to the destination specified by BACKGROUND_DUMP_DEST.

Trace files for server processes are written to the destination specified by USER_ DUMP_DEST.

This event test checks for available free space on these dump destination devices. If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated.

Parameters

- Critical threshold: Free space threshold in kilobytes for a critical alert. Default 2000 kilobytes.
- Warning threshold: Free space threshold in kilobytes for a warning alert. Default 5000 kilobytes.

Output

Dump destination device and space available in kilobytes

Recommended Frequency

10 minutes

User Action

Verify the device specified in the initialization parameters BACKGROUND_ DUMP_DEST and USER_DUMP_DEST are set up properly for archiving. If the BACKGROUND_ DUMP_DEST and USER_DUMP_DEST initialization parameters are set up correctly and this event test triggers, then free up more space in the destination specified by the dump destination parameters.

Dump Full (%)

Description

This event test monitors the same dump destinations as the Dump Full event test. The Dump Full (%) event test, however, returns the percentage of free space remaining on the dump destinations.

If the space available is less than the threshold value given in the threshold arguments, then a warning or critical alert is generated.

Parameters

- Critical threshold: Percentage of free space threshold for critical alert. Default 30%.
- Warning threshold: Percentage of free space threshold for warning alert. Default 50%.

Output

Dump destination device and percentage of free space available

Recommended Frequency

10 minutes

User Action

Verify the device specified in the initialization parameters BACKGROUND_ DUMP_DEST and USER_DUMP_DEST are set up properly for archiving. If the BACKGROUND_ DUMP_DEST and USER_DUMP_DEST initialization parameters are set up correctly and this event test triggers, then free up more space in the destination specified by the dump destination parameters.

Error Transactions

Description

Oracle uses deferred transactions to propagate data-level changes asynchronously among master sites in an advanced replication system as well as from an updatable snapshot to its master table. If a transaction is not successfully propagated to the remote site, Oracle rolls back the transaction, logs the transaction in the SYS.DEFERROR view in the remote destination database.

This event test checks for the number of transactions in SYS.DEFERROR view and raises an alert if it exceeds the value specified by the threshold argument.

Parameters
Threshold for alert (number of error transactions). Default is 0 transactions.

Output
Number of transactions that could not be applied

Recommended Frequency
30 seconds

User Action
An error in applying a deferred transaction may be the result of a database problem, such as a lack of available space in the table is to be updated or may be the result of an unresolved insert, update or delete conflict. The SYS.DEFERROR view provides the ID of the transaction that could not be applied. Use this ID to locate the queued calls associated with the transaction. These calls are stored in the SYS.DEFCALL view. You can use the procedures in the DBMS_DEFER_QUERY package to determine the arguments to the procedures listed in the SYS.DEFCALL view.

Executes without Parses %

Description
This data item represents the percentage of statement executions that do not require a corresponding parse. A perfect system would parse all statements once and then execute the parsed statement over and over without reparsing. This ratio provides an indication as to how often the application is parsing statements as compared to their overall execution rate. A higher number is better.

This test checks the percentage of executes that do not require parses. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
((DeltaExecuteCount - (DeltaParseCountTotal)) / DeltaExecuteCount) * 100
where:

- DeltaParseCountTotal: difference in 'select value from v$sysstat where name='parse count (total)'' between sample end and start
- DeltaExecuteCount: difference in 'select value from v$sysstat where name='execute count'' between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and executes without parses percentage.

Recommended Frequency

5 minutes

User Action

An execute to parse ratio of less than 70% indicates that the application may be parsing statements more often than it should. Reparsing the statement, even if it is a soft parse, requires a network round trip from the application to the database, as well as requiring the processing time to locate the previously compiled statement in the cache. Reducing network round trips and unnecessary processing improves application performance.

Use the Top Sessions by Total Parse Count to identify the sessions responsible for the bulk of the parse activity within the database. Start with these sessions to determine whether the application could be modified to make more efficient use of its cursors.

To see the actual values of the underlying statistics used to compute this resource, you can use the Parse Statistics Chart. This chart shows the Parse, Execute and Hard Parse rates per second.

Failed Job

Description

The Oracle server job queue is a database table that stores information about local jobs such as the PL / SQL call to execute for a job such as when to run a job. Database replication is also managed by using the Oracle job queue mechanism using jobs to push deferred transactions to remote master sites, to purge applied transactions from the deferred transaction queue or to refresh snapshot refresh groups.

If a job returns an error while Oracle is attempting to execute it, the job fails. Oracle repeatedly tries to execute the job doubling the interval of each attempt. If the job fails sixteen times, Oracle automatically marks the job as broken and no longer tries to execute it.

This event test checks for failed DBMS jobs. An alert is generated if the number of failed job exceeds the value specified by the threshold argument.

Parameters

Critical threshold: Threshold for critical alert (number of jobs). Default is 0 jobs.

Output

- Job identifiers of failed DBMS jobs.
- Number of failures since last successful execution.

Recommended Frequency

30 seconds

User Action

Check the ALERT log and trace files for error information. Correct the problem that is preventing the job from running.

Fast Segment Growth

Description

A segment collection is a group of extents that make up a single table, index, temporary or rollback segment. The Oracle Server offers a practical method of space allocation to segments as they are required to grow. Oracle allows a segment to have multiple extents, which the server allocates automatically when they are needed. For any segment that grows continuously, it is important to carefully monitor that segment's growth pattern. Storage values for the database should be chosen to ensure new extents are not frequently allocated.

This event test checks whether any of the segments specified by the Tablespace name, Segment name, and Segment type parameters are allocating extents too quickly. If, for any segment, the number of extents allocated since the event check is greater than the threshold values specified in the threshold arguments, then a warning or critical alert is generated.

Parameters

- Tablespace name filter: Filter of the tablespace names to be monitored, or * for all tablespaces. Tablespaces that are either temporary, read-only or off-line are excluded. Default is *.
- Segment name filter: Filter of the segments to be monitored, or * for all segments. Default is *.
- Segment type filter: Filter of the segment types to be monitored, or * for all segment types. Segment types CACHE and DEFERRED ROLLBACK are excluded. Default is *.
- Critical threshold: Threshold for critical alert or number of extents. Default is 3 extents.
- Warning threshold: Threshold for warning alert or number of extents. Default is 2 extents.

Note: All filters must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'. There are higher resource requirements if there is a large number of objects being monitored at high frequencies, for example, checking the space for all 200 segments every 2 minutes. Where possible, Oracle recommends that you use the filters to narrow the scope of the objects being monitored. Also, set the polling schedule to a value that is appropriate to your environment. For example, segments that do not grow rapidly in size may be checked every 2 days instead of every 5 minutes.

Output

- Name of segment growing too quickly.
- Tablespace name containing segment.
- Number of extents segment grew since last event condition check.

Recommended Frequency

1 day

User Action

Consider increasing the value of the segment's NEXT storage parameter value so that extents are allocated less frequently.

Note: Running the Fast Segment Growth event test may be a resource-intensive operation. Therefore, Oracle recommends running the Fast Segment Growth event test during off-peak periods.

Free Buffer Waits

Description

Database writer process (DBWR) bottlenecks can be detected by monitoring occurrences of the free buffer waits test over time. If the database environment is in a steady state, there should not be any free buffer waits. However, an occasional absolute increase in free buffer waits is not a problem. Only consistent occurrences of an increase should be of concern.

As a result, this event test maintains a history of free buffer waits samples, specified by the number of samples parameter, and monitors for a percentage of these samples where an increase was detected. This percentage is then compared against the values specified by the threshold arguments. If the percentage of samples (where an increase in free buffer waits is detected) is greater than the threshold arguments, then a warning or critical alert is generated.

Example: If 10 has been specified for the number of samples, then during the first 9 times the test condition is checked, the test is merely building up the history of free buffer waits samples. On the 10 interval and from that point on, the test monitors how many of those samples showed and increase in free buffer waits. Assume 2 samples showed an increase, then the percentage of samples showing an increase is 20%.

Parameters

- Number of samples: Number of free buffer waits samples. Default is 10.
- Critical threshold: Threshold for critical alert (%). Default is 20%.
- Warning threshold: Threshold for warning alert (%). Default is 10%.

Output

- Current percentage of samples where an increase in free buffer waits is detected.
- Current DB_FILE_SIMULTANEOUS_WRITES setting

Recommended Frequency

60 seconds

User Action

When users are having to wait for free buffers, then either DB_FILE_ SIMULTANEOUS_WRITES needs to be increased of the number or DBWR processes needs to be increased.

The DB_FILE_SIMULTANEOUS_WRITES initialization parameter determines the number of simultaneous writes to each database file when written by DBWR. This parameter is also used to determine the number of reads per file in the redo read ahead when reading redo during recover. This parameter impacts the number of simultaneous I/Os, not just the number of simultaneous writes.

Consider increasing the DB_FILE_SIMULTANEOUS_WRITES initialization parameter in order to increase the speed at which the DBWR writes dirty buffers which then decreases the number of times sessions needed to wait for free buffers.

The DB_WRITES initialization parameter controls the number of DBWR processes that are activated at instance startup. It is a platform specific parameter which is used to avoid DBWR bottlenecks on operating systems which do not support asynchronous I/O. The DBWR process is responsible for writing dirty buffers in batches from the buffer cache back to the data files.

DBWR bottlenecks are most likely on systems which have a high insert, update or delete rate and a large number of disk devices. Since database writes are not serial, there can be benefit to having multiple DBWR processes, even in a single CPU database environment.

Global Cache Convert Timeouts

Description

This data item represents number of times lock converts in the global cache timed out for each Oracle server instance per second during this sample period.

This test checks the Global Cache Convert Timeouts for an instance per second for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

ConvertTimeout / Seconds
where:

- ConvertTimeout: difference of 'select sum(value) from gv$sysstat where name = 'global cache convert timeouts' group by instance_name between sample end and start

Parameters

- Instance Name(s): Cluster database instance name.

- Critical Threshold: Default is 0.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and convert timeouts per second.

Recommended Frequency
5 minutes

Global Cache Converts

Description
This data item represents average convert time in milliseconds during this sample period.

This test checks the Global Cache Converts for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
ConvertTime * 10 / Converts
where:

- ConvertTime: difference of 'select sum(value) from gv$sysstat where name = 'global cache convert time' group by instance_name between sample end and start
- Converts:difference of 'select sum(value) from gv$sysstat where name = 'global cache converts' group by instance_name between sample end and start

Parameters
- Instance Name(s): Cluster database instance name.
- Warning Threshold: Default is 80 milliseconds.
- Critical Threshold: Default is 100 milliseconds.
- Number of Occurrences: Default is 1.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and global cache converts time in milliseconds.

Recommended Frequency
5 minutes

Global Cache CR Request

Description
This data item represents average time in milliseconds that CR block was received during this sample period.

This test checks the Global Cache CR Request for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
BlockReceiveTime * 10 / BlocksReceived
where:

- BlockReceiveTime: difference of 'select sum(value) from gv$sysstat where name = 'global cache CR block receive time' group by instance_name between sample end and start
- BlocksReceived:difference of 'select sum(value) from gv$sysstat where name = 'global cache current blocks received' group by instance_name between sample end and start

Parameters
- Instance Name(s): Cluster database instance name.
- Warning Threshold: Default is 30 milliseconds.
- Critical Threshold: Default is 50 milliseconds.
- Number of Occurrences: Default is 1.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and global cache CR request time in milliseconds.

Recommended Frequency
5 minutes

Global Cache CR Timeouts

Description
This data item represents the number of times a foreground process requested a consistent-read (CR) block when the request timed out for each Oracle cluster database instance per second during this sample period.

This test checks the Global Cache CR Timeouts for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
CR_Timeout / Seconds
where:

- CR_Timeout: difference of 'select sum(value) from gv$sysstat where name = 'global cache CR timeouts' group by instance_name between sample end and start

Parameters
- Instance Name(s): Cluster database instance name.
- Critical Threshold: Default is 0.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and CR timeout per second.

Recommended Frequency
5 minutes

Global Cache FreeList Waits

Description

This data item represents number of times foreground has to wait for a lock element for each cluster database instance per second during this sample period.

This test checks the Global Cache FreeList Waits for an instance per second for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

FreelistWait / Seconds
where:

- FreelistWait: difference of 'select sum(value) from gv$sysstat where name = 'global cache freelist waits' group by instance_name between sample end and start

Parameters

- Instance Name(s): Cluster database instance name.
- Critical Threshold: Default is 0.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and freelist waits per second.

Recommended Frequency

5 minutes

Global Cache Gets

Description

This data item represents average get time in milliseconds during this sample period.

This test checks the Global Cache Gets for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the

threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

GetTime * 10 / Gets
where:

- GetTime: difference of 'select sum(value) from gv$sysstat where name = 'global cache get time' group by instance_name between sample end and start
- Gets:difference of 'select sum(value) from gv$sysstat where name = 'global cache gets' group by instance_name between sample end and start

Parameters

- Instance Name(s): Cluster database instance name.
- Warning Threshold: Default is 30 milliseconds.
- Critical Threshold: Default is 60 milliseconds.
- Number of Occurrences: Default is 1.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and global cache gets time in milliseconds.

Recommended Frequency

5 minutes

In Memory Sort %

Description

This data item represents the sort efficiency as measured by the percentage of times sorts were performed in memory as opposed to going to disk.

For best performance, most sorts should occur in memory because sorts to disks are less efficient. If the sort area is too small, extra sort runs will be required during the sort operation. This increases CPU and I/O resource consumption.

This test checks the percentage of sorts performed in memory rather than to disk. If the value is less than or equal to the threshold values specified by the threshold

arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
(DeltaMemorySorts / (DeltaDiskSorts + DeltaMemorySorts)) * 100
where:

- DeltaMemorySorts: difference in 'select value from v$sysstat where name='sorts (memory)" between sample end and start
- DeltaDiskSorts: difference in 'select value from v$sysstat where name='sorts (disk)" between sample end and start

Parameters
- Warning Threshold: Default is 99.0. The value can be between 0.0 and 100.0.
- Critical Threshold: Default is 90.0. The value can be between 0.0 and 100.0.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and in memory sort percentage.

Recommended Frequency
5 minutes

User Action
The sessions that are performing the most sorts should be identified such that the SQL they are executing can be further identified. The sort area sizes for the database may be sized correctly, and the application SQL may be performing unwanted or excessive sorts. The sessions performing the most sorts are available through the Top Sessions by Disk Sorts drilldown.

Further drilldown into the session performing the most disk sorts with the Current SQL Chart shows you the SQL statement responsible for the disk sorts. Further investigation on how to best tune a particular SQL statement can be done by using the Explain Plan drilldown, or if you are on NT, the Tune SQL Statement drilldown as well.

The Top SQL (Sorts) Chart provides a mechanism to quickly display the SQL statements in the cache, presented in sorted order by their number sort operations. This is an alternative to viewing a sort of current sessions. It allows you to view sort

activity via SQL statements and contains cumulative statistics for all executions of that statement.

If the top sessions and their associated SQL statements seem to be okay, you can drill down to see a more complete breakdown of sort statistics and initialization parameters with the Sort Statistics At A Glance Chart.

If excessive sorts are taking place on disk and the queries are correct, consider increasing the SORT_AREA_SIZE initialization parameter to increase the size of the sort area. A larger sort area allows the Oracle Server to maintain sorts in memory, reducing the number of I/O operations required to do an equivalent amount of work using the current sort area size.

For more detailed sort statistics, the Sort Statistics At A Glance Chart is available which displays the current sort-related initialization parameter values as well as a breakdown of the individual sort statistics.

Index Rebuild

Description

When an indexed value is updated in the table, the old value is deleted from the index and the new value is inserted into a separate part of the index. The space released by the old value can never be used again. As indexed values are updated or deleted, the amount of unusable space within the index increases, a condition called index stagnation. Because a stagnated index contains a mixture of data and empty areas, scans of the index will be less efficient.

This event test monitors whether indexes specified by the Index name, Index owner, Indexed object name, and Indexed object owner parameters suffer from index stagnation. If an index has stagnation, an alert is generated.

Parameters

- Index name filter: Filter of the index names to be monitored, or * for all indexes. Default is *.
- Index owner filter: Filter of the index owners to be monitored, or * for all owners. Owners SYS and SYSTEM are excluded. Default is *.
- Index object name filter: Filter of the indexed object name to be monitored, or * for all objects. Default is *.
- Indexed object owner name filter: Filter of the indexed object owner name to be monitored, or * for all owners. Default is *. The filter must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'.

Note: All filters must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'. There are higher resource requirements if there is a large number of objects being monitored at high frequencies, for example, checking the space for all 200 indexes every 2 minutes. Where possible, Oracle recommends that you use the filters to narrow the scope of the objects being monitored. Also, set the polling schedule to a value that is appropriate to your environment. For example, indexes that do not grow rapidly in size may be checked every 2 days instead of every 5 minutes.

Output
Index name where index stagnation is detected.

Recommended Frequency
1 day

User Action
Consider rebuilding the index to enhance performance. An index rebuild can be accomplished by using either the ALTER INDEX REBUILD statement or the CREATE INDEX statement.

Note: To determine whether or not an index should be rebuilt, the Index Rebuild event test gathers statistics using the ANALYZE...INDEX VALIDATE STRUCTURE command. Running this command may be a resource-intensive operation. Therefore, Oracle recommends running the Index Rebuild event test during off-peak periods.

Instance Pings

Description
This data item represents the ping ratio during this sample period.

This test checks the Ping Ratio for the instance specified by the Instance Name(s) parameter. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Pings / Writes
where:

- Pings: difference of 'select sum(value) from gv$sysstat where name = 'DBWR cross instance writes' group by instance_name between sample end and start

- Writes: difference of 'select sum(value) from gv$sysstat where name = 'physical writes' group by instance_name between sample end and start

Parameters

- Instance Name(s): cluster database instance name.
- Warning Threshold: Default is 20.
- Critical Threshold: Default is 35.
- Number of Occurrences: Default is 1.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and ping ratio.

Recommended Frequency

5 minutes

Library Cache Hit %

Description

This data item represents the library cache efficiency, as measured by the percentage of times the fully parsed or compiled representation of PL/SQL blocks and SQL statements are already in memory.

The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache and the other cache structures that are specific to a particular instance configuration.

The shared pool mechanism can greatly reduce system resource consumption in at least three ways:

Parse time is avoided if the SQL statement is already in the shared pool.

Application memory overhead is reduced, since all applications use the same pool of shared SQL statements and dictionary resources.

I/O resources are saved, since dictionary elements which are in the shared pool do not require access.

If the shared pool is too small, users will consume additional resources to complete a database operation. For library cache access, the overhead is primarily the additional CPU resources required to re-parse the SQL statement.

This test checks the percentage of parse requests where cursor already in cache If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

(DeltaPinHits / DeltaPins) * 100
where:

- DeltaPinHits: difference in 'select sum(pinhits) from v$librarycache' between sample end and start
- DeltaPins: difference in 'select sum(pins) from v$librarycache' between sample end and start

Parameters

- Warning Threshold: Default is 99.5. The value can be between 0.0 and 100.0.
- Critical Threshold: Default is 99.0. The value can be between 0.0 and 100.0.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and library cache hit percentage.

Recommended Frequency

5 minutes

User Action

The Top Sessions by Hard Parse Count chart lists the sessions incurring the most hard parses. Hard parses occur when the server parses a query and cannot find an exact match for the query in the library cache. You can avoid hard parses by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this chart can identify the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

To identify potential similar SQL statements use the Similar SQL Statements Chart. This shows you which statements are similar in the first 'n' characters and how many versions of that statement segment are in the cache. Hard parses can also be forced by aging of SQL statements out of the cache due to an insufficient size of the shared pool area. The shared pool sizes allows you to see your current shared pool allocation and potentially increase it.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

Library Cache Miss %

Description

The shared pool is an area in the SGA that contains the library cache of shared SQL requests, the dictionary cache and the other cache structures that are specific to a particular instance configuration.

The library cache efficiency, as measured by the miss ratio, records the percentage of times the fully parsed or compiled representation of PL/SQL blocks and SQL statements are not already in memory.

The shared pool mechanism can greatly reduce system resource consumption in at least three ways:

- Parse time is avoided if the SQL statement is already in the shared pool.
- Application memory overhead is reduced, since all applications utilize the same pool of shared SQL statements and dictionary resources.
- I/O resources are saved, since dictionary elements which are in the shared pool do not require access.

If the shared pool is too small, users will consume additional resources to complete a database operation. For library cache access, the overhead is primarily the additional CPU resources required to re-parse the SQL statement.

This event test monitors the library cache miss ratio (percentage of failures) against the values specified by the threshold arguments. If the number of occurrences exceeds the values specified, then a warning or critical alert is generated.

Parameters

- Number of occurrences: Number of consecutive occurrences that library cache miss ratio exceeds thresholds before a warning or critical alert is generated. Default is 3.
- Critical threshold: Threshold for critical alert (%). Default is 1%.
- Warning threshold: Threshold for warning alert (%). Default is 0.5%.

Output

Current ratio

Recommended Frequency

30 seconds

User Action

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE in order to decrease the frequency in which SQL requests are being flushed from the shared pool in order to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

Also examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. Consider using bind variables rather than explicitly specified constants in your statements whenever possible.

Note: For Oracle Intelligent Agent release 9*i*, this event test has been obsoleted. It is recommended that you use the Library Cache Hit Ratio event test. This event test is kept for backward compatibility with older versions of the Intelligent Agent.

Lock Limit

Description

The DML_LOCKS initialization parameter specifies the maximum number of DML locks. The purpose of DML locks is to guarantee the integrity of data being accessed concurrently by multiple users. DML locks prevent destructive interference of simultaneous conflicting DML and / or DDL operations.

This event test checks for the utilization of the lock resource against the values (percentage) specified by the threshold arguments. If the percentage of all active DML locks to the limit set in the DML_LOCKS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated.

If DML_LOCKS is 0, this test fails to register. A value of 0 indicates that enqueues are disabled.

Example

If 40 DML locks are active and the value of DML_LOCKS is 60, the percentage is 67% (40 / 60 x 100). This value is compared against the specified thresholds.

Parameters

- Critical threshold: Threshold value for critical alert (%). Default is 90%.
- Warning threshold: Threshold value for warning alert (%). Default is 80%.

Output

Current value and the limit specified by DML_LOCKS

Recommended Frequency

30 seconds

User Action

Increase the DML_LOCKS instance parameter by 10%.

Logical Reads Per Second

Description

This data item represents the number of logical reads per second during the sample period. A logical read is a read request for a data block from the SGA. Logical reads may result in a physical read if the requested block does not reside with the buffer cache.

This test checks the logical(db block gets + consistent gets) reads per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
LogicalReads / Seconds
where:

- LogicalReads: difference in 'select value from v$sysstat where name='session logical reads'' between end and start of sample period
- Seconds: number of seconds in sample period

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and logical reads per second.

Recommended Frequency
5 minutes

User Action
Excessive logical reads, even if they do not result in physical reads, can still represent an area that should be considered for performance tuning. Typically large values for this statistic indicate that full table scans are being performed. To identify the SQL that is performing the most logical reads (buffer gets), use the Top SQL (Buffer Gets) chart. This quickly identifies the SQL responsible for the bulk of the logical reads. You can further investigate these SQL statements via drilldowns. Tuning these SQL statements will reduce your buffer cache access.

Logical Reads Per Transaction

Description
This data item represents the number of logical reads per transaction during the sample period.

The value of this statistic is zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding per second data item of the same name will be a better indicator of current performance.

This test checks the logical (db block gets + consistent gets) reads per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaReads / Transactions
where:

- DeltaReads: difference in 'select value from v$sysstat where name='session logical reads" between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and logical reads per transaction.

Recommended Frequency

5 minutes

User Action

Excessive logical reads, even if they do not result in physical reads, can still represent an area that should be considered for performance tuning. Typically large values for this statistic indicate that full table scans are being performed. To identify the SQL that is performing the most logical reads (buffer gets) use the Top SQL (Buffer Gets) chart. This quickly identifies the SQL responsible for the bulk of the logical reads. Further investigation on how to best tune a particular SQL statement can be done by using the Explain Plan drilldown, or if you are on NT, the Tune SQL Statement drilldown as well.

Logons Per Second

Description

This data item represents the number of logons per second during the sample period.

This test checks the number of logons that occurred per second during the sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaLogons / Seconds
where:

- DeltaLogons: difference in 'select value from v$sysstat where name='logons cumulative'' between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and logons per second.

Recommended Frequency

5 minutes

User Action

A high logon rate may indicate that an application is inefficiently accessing the database. Database logon's are a costly operation. If an application is performing a logon for every SQL access, that application will experience poor performance as well as affect the performance of other applications on the database. If there is a high logon rate try to identify the application that is performing the logons to determine if it could be redesigned such that session connections could be pooled, reused or shared.

The Transaction Based Execution Rates Chart will allow you to quickly determine the ratio of logons to transactions to determine the average amount of transactional work being done per logon.

Quick analysis of the database's CPU consumption can be done by using the CPU Breakdown Chart. This chart breaks the database CPU consumption into 3 parts, and further analysis into the largest portion of the CPU time will lead you towards reducing your CPU consumption.

Logons Per Transaction

Description

This data item represents the number of logons per transaction during the sample period.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the number of logons that occurred per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaLogons / Transactions
where:

- DeltaLogons: difference in 'select value from v$sysstat where name='logons cumulative'' between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and logons per transaction.

Recommended Frequency
5 minutes

User Action
A high logon rate may indicate that an application is inefficiently accessing the database. Database logon's are a costly operation. If an application is performing a logon for every SQL access, that application will experience poor performance as well as affect the performance of other applications on the database. If there is a high logon rate try to identify the application that is performing the logons to determine if it could be redesigned such that session connections could be pooled, reused or shared.

Maximum Extents

Description
A segment is a collection of extents that make up a single table, cluster, index, temporary or rollback segment. The MAXEXTENTS segment storage parameter specifies the maximum number of extents that can be allocated to the segment. Once a segment has filled the maximum number of extents, any row insertion will fail with an ORA-01631 error message.

This event test checks whether any of the segments specified by the Tablespace name, Segment name, and the Segment type parameters are approaching their maximum extents. If for any segment the maximum number of extents minus the number of existing extents is less than the threshold values specified in the threshold arguments, then a warning or critical alert is generated.

Example

If the maximum number of extents for a segment is 20 and the number of existing extents is 16, then 4 is compared against the specified threshold values. If 3 is specified for a critical alert and 5 is specified for a warning alert, a warning alert is triggered because only 4 extents are available.

Parameters
- Tablespace name filter: Filter of the tablespace names to be monitored, or * for all tablespaces. Tablespaces that are either temporary, read-only or off-line are excluded. Default is *.

- Segment name filter: Filter of the segments to be monitored, or * for all segments. Default is *.
- Segment type filter: Filter of the segment types to be monitored, or * for all segment types. Segment type CACHE is excluded. Default is *.
- Critical threshold: Threshold for critical alert (number of extents). Default is 1 extent.
- Warning threshold: Threshold for warning alert (number of extents). Default is 2 extents.

Note: All filters must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'. There are higher resource requirements if there is a large number of objects being monitored at high frequencies, for example, checking the space for all 200 segments every 2 minutes. Where possible, Oracle recommends that you use the filters to narrow the scope of the objects being monitored. Also, set the polling schedule to a value that is appropriate to your environment. For example, segments that do not grow rapidly in size may be checked every 2 days instead of every 5 minutes.

Output

- Name of segment approaching its maximum extents.
- Tablespace name containing segment.
- Number of extents that can be allocated before the maximum number of extents is hit.

Recommended Frequency

10 minutes

User Action

If possible, increase the value of the segment's MAXEXTENTS storage parameter. Otherwise, rebuild the segment with a larger extent size ensuring the extents within a segment are the same size by specifying STORAGE parameters where NEXT=INITIAL and PCTINCREASE = 0. For segments that are linearly scanned, choose an extent size that is a multiple of the number of blocks read during each multiblock read. This will ensure that Oracle's multiblock read capability is used efficiently.

Note: Running the Maximum Extents event test may be a resource-intensive operation. Therefore, Oracle recommends running the Maximum Extents event test during off-peak periods.

Multiple Extents

Description

A segment is a collection of extents that make up a single table, cluster, index, temporary or rollback segment. The Oracle Server allows a segment to have multiple extents, which the server allocates automatically when additional space is required.

There is no performance degradation for a segment having multiple extents that are never full-scanned (table and temporary segments only) where the extents are the same size and are also an integral multiple of the multiblock read batch size. No performance degradation is found where extents are 100 or more times larger that the read batch size. Oracle administrators may, however, choose to monitor the number of extents in a segment.

This event test checks whether any of the segments specified by the Tablespace name, Segment name, and Segment type parameters have multiple extents. If the number of extents is greater than the threshold values specified in the threshold arguments, then a warning or critical alert is generated.

Note: The only time multiple extents may cause a performance problem is when a segment is fully scanned and that segment's extent size is not a multiple of the multiblock read size.

Parameters

- Tablespace name filter: Filter of the tablespace names to be monitored, or * for all tablespaces. Tablespaces that are either temporary, read-only or off-line are excluded. Default is *.
- Segment name filter: Filter of the segment names to be monitored, or * for all segments. Default is *.
- Segment type filter: Filter of the segment types to be monitored, or * for all segment types. Segment types CACHE and DEFERRED ROLLBACK are excluded. Default is *.
- Critical threshold: Threshold for critical alert (number of extents). Default is 50 extents.
- Warning threshold: Threshold for warning alert (number of extents). Default is 30 extents.

Note: All filters must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'. There are higher resource requirements if there is a large number of objects being monitored at high frequencies, for example, checking the space for all

200 segments every 2 minutes. Where possible, Oracle recommends that you use the filters to narrow the scope of the objects being monitored. Also, set the polling schedule to a value that is appropriate to your environment. For example, segments that do not grow rapidly in size may be checked every 2 days instead of every 5 minutes.

Output

- Name of segment comprised of multiple extents.
- Name of tablespace containing segment.
- Number of extents currently allocated for the segment.

Recommended Frequency

10 minutes

User Action

If the segment may be linearly scanned, make sure the multiple extents are the same size. The chosen extent size is an integral multiple of the muliblock read batch size or the extents is 100 or more times larger than the read batch size in order to achieve the highest efficiency of the server's multiblock read capability.

For all other segments, no action is required unless the number of extent allocations is approaching the segment's maximum number of extents. In this case, increase the value of the segment's MAXEXTENTS storage parameter if possible.

Otherwise, rebuild the segment with a larger extent size ensuring that the extents within a segment are the same size by specifying STORAGE parameters where NEXT=INITIAL and PCTINCREASE = 0.

Note: Running the Multiple Extents event test may be a resource-intensive operation. Therefore, Oracle recommends running the Multiple Extents event test during off-peak periods.

Network Reads Per Second

Description

This data item represents the total number of bytes sent and received through the SQL Net layer to and from the database.

This test checks the network read / write per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

(DeltaBytesFromClient+DeltaBytesFromDblink+DeltaBytesToClient+DeltaBytesToDblink) / Seconds

where:

- Delta Bytes From Client: difference in 'select s.value from v$sysstat s, visitation n where n.name='bytes received via SQL*Net from client' and n.statistic#=s.statistic#' between end and start of sample period
- DeltaBytesFromClient: difference in 'select s.value from v$sysstat s, v$statname n where n.name='bytes received via SQL*Net from dblink' and n.statistic#=s.statistic#' between end and start of sample period
- DeltaBytesFromClient: difference in 'select s.value from v$sysstat s, v$statname n where n.name='bytes sent via SQL*Net to client' and n.statistic#=s.statistic#' between end and start of sample period
- DeltaBytesFromClient: difference in 'select s.value from v$sysstat s, v$statname n where n.name='bytes sent via SQL*Net to dblink' and n.statistic#=s.statistic#' between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and network bytes per second.

Recommended Frequency

5 minutes

User Action

This data item represents the amount of network traffic in and out of the database. This number may only be useful when compared to historical levels to understand network traffic usage related to a specific database.

Parses (Hard) Per Second

Description

This data item represents the number of hard parses per second during this sample period. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement.

Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor.

This test checks the number of parses of statements that were not already in the cache. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaParses / Seconds
where:

- DeltaParses: difference in 'select value from v$sysstat where name='parse count (hard)" between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and hard parses per second.

Recommended Frequency

5 minutes

User Action

If there appears to be excessive time spent parsing, evaluate SQL statements to determine which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The Top Sessions by Hard Parse Count chart will show you which sessions are incurring the most hard parses. Hard parses happen when the server parses a query and cannot find an exact match for the query in the library cache. Hard parses can be avoided by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this chart may lead you to the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

To identify potential similar SQL statements use the Similar SQL Statements Chart. This will show you which statements are similar in the first 'n' characters and how many versions of that statement segment are in the cache. Hard parses can also be forced by aging of SQL statements out of the cache due to an insufficient size of the shared pool area. The shared pool sizes allows you to see your current shared pool allocation and potentially increase it.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

Parses (Hard) Per Transaction

Description

This data item represents the number of hard parses per second during this sample period. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement.

Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the number of hard parses per second during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaParses / Transactions
where:

- DeltaParses: difference in 'select value from v$sysstat where name='parse count (hard)" between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and hard parses per second.

Recommended Frequency
5 minutes

User Action
If there appears to be excessive time spent parsing, evaluate SQL statements to determine which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The Top Sessions by Hard Parse Count chart will show you which sessions are incurring the most hard parses. Hard parses happen when the server parses a query and cannot find an exact match for the query in the library cache. Hard parses can be avoided by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this chart may lead you to the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

To identify potential similar SQL statements use the Similar SQL Statements Chart. This will show you which statements are similar in the first 'n' characters and how many versions of that statement segment are in the cache. Hard parses can also be forced by aging of SQL statements out of the cache due to an insufficient size of the shared pool area. The shared pool sizes allows you to see your current shared pool allocation and potentially increase it.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

Parses (Total) Per Second

Description

This number reflects the total number of parses per second, both hard and soft. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.

Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor.

This test checks the number of parse calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaParses / Seconds
where:

- DeltaParses: difference in 'select value from v$sysstat where name='parse count (total)" between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and number of parse calls.

Recommended Frequency

5 minutes

User Action

If there appears to be excessive time spent parsing, evaluate SQL statements to determine which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The Top Sessions by Hard Parse Count chart will show you which sessions are incurring the most hard parses. Hard parses happen when the server parses a query and cannot find an exact match for the query in the library cache. Hard parses can be avoided by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this chart may lead you to the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

To identify potential similar SQL statements use the Similar SQL Statements Chart. This will show you which statements are similar in the first 'n' characters and how many versions of that statement segment are in the cache. Hard parses can also be forced by aging of SQL statements out of the cache due to an insufficient size of the shared pool area. The shared pool sizes allows you to see your current shared pool allocation and potentially increase it.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

Parses (Total) Per Transaction

Description

This number reflects the total number of parses per transaction, both hard and soft. A hard parse occurs when a SQL statement has to be loaded into the shared pool. In this case, the Oracle Server has to allocate memory in the shared pool and parse the statement. A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.

Each time a particular SQL cursor is parsed, this count will increase by one. There are certain operations which will cause a SQL cursor to be parsed. Parsing a SQL statement breaks it down into atomic steps which the optimizer will evaluate when generating an execution plan for the cursor.

This test checks the number of parse calls per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaParses / Transactions
where:

- DeltaParses: difference in 'select value from v$sysstat where name='parse count (total)" between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and number of parse calls per transaction.

Recommended Frequency

5 minutes

User Action

If there appears to be excessive time spent parsing, evaluate SQL statements to determine which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

The Top Sessions by Hard Parse Count chart will show you which sessions are incurring the most hard parses. Hard parses happen when the server parses a query and cannot find an exact match for the query in the library cache. Hard parses can be avoided by sharing SQL statements efficiently. The use of bind variables instead of literals in queries is one method to increase sharing.

By showing you which sessions are incurring the most hard parses, this chart may lead you to the application or programs that are the best candidates for SQL rewrites.

Also, examine SQL statements which can be modified to optimize shared SQL pool memory use and avoid unnecessary statement reparsing. This type of problem is commonly caused when similar SQL statements are written which differ in space, case, or some combination of the two. You may also consider using bind variables rather than explicitly specified constants in your statements whenever possible.

To identify potential similar SQL statements use the Similar SQL Statements Chart. This will show you which statements are similar in the first 'n' characters and how many versions of that statement segment are in the cache. Hard parses can also be forced by aging of SQL statements out of the cache due to an insufficient size of the shared pool area. The shared pool sizes allows you to see your current shared pool allocation and potentially increase it.

The SHARED_POOL_SIZE initialization parameter controls the total size of the shared pool. Consider increasing the SHARED_POOL_SIZE to decrease the frequency in which SQL requests are being flushed from the shared pool to make room for new requests.

To take advantage of the additional memory available for shared SQL areas, you may also need to increase the number of cursors permitted per session. You can increase this limit by increasing the value of the initialization parameter OPEN_CURSORS.

Physical Reads Per Second

Description

This data item represents the number of data blocks read from disk per second during this sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then searches the disk if it is not already in memory. Reading data blocks from disk is much more inefficient than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization.

This test checks the data blocks read from disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaPhysicalReads / Seconds
where:

- DeltaPhysicalReads: difference in 'select s.value from v$sysstat s, v$statname n where n.name='physical reads' and n.statistic#=s.statistic#' between sample end and start
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and physical reads per second.

Recommended Frequency

5 minutes

User Action

Block reads are inevitable so the aim should be to minimize unnecessary IO. This is best achieved by good application design and efficient execution plans. Changes to

execution plans can yield profound changes in performance. Tweaking at system level usually only achieves percentage gains.

To view I/O on a per session basis to determine which sessions are responsible for your physical reads, you should use the Top Sessions by Physical Reads Chart. This approach allows you to identify problematic sessions and then drill down to their current SQL statement and perform tuning from there.

To identify the SQL that is responsible for the largest portion of physical reads, use the Top SQL (Physical Reads) Chart. This chart allows you to quickly determine which SQL statements are the causing your I/O activity. From this chart you can view the full text of the SQL statement. Further investigation on how to best tune a particular SQL statement can be done by using the Explain Plan drilldown, or if you are on NT, the Tune SQL Statement drilldown as well.

The difference between the two methods for identifying problematic SQL is that the Top Sessions view displays sessions that are performing the most physical reads at the moment. The Top SQL view displays the SQL statements that are still in the SQL cache that have performed the most I/O over their lifetime. A SQL statement could show up in the Top SQL view that is not currently being executed.

If the SQL statements are properly tuned and optimized, consider the following suggestions. A larger buffer cache may help - test this by actually increasing DB_ BLOCK_BUFFERS. Do not use DB_BLOCK_LRU_EXTENDED_STATISTICS, as this may introduce other performance issues. Never increase the SGA size if it may induce additional paging or swapping on the system.

A less obvious issue which can affect the IO rates is how well data is clustered physically. For example, assume that you frequently fetch rows from a table where a column is between two values via an index scan. If there are 100 rows in each index block then the two extremes are: 1.Each of the table rows is in a different physical block (100 blocks need to be read for each index block). 2.The table rows are all located in the few adjacent blocks (a handful of blocks need to be read for each index block).

Pre-sorting or reorganizing data can improve this situation in severe situations as well.

To view more detailed I/O statistics, the I/O at a Glance Chart displays some overall I/O statistics as well as a breakdown of the top files being accessed within the database.

For a view of I/O statistics on a per transaction basis, the I/O Rates per Transaction Chart shows you the average amount of I/O incurred by each transaction. These transaction-based rates can provide you with a more consistent view of the I/O

activity within the database. The transaction based statistics may not fluctuate during the day as much as the per second numbers may.

Physical Reads Per Transaction

Description

This data item represents the number of disk reads per transaction during the sample period. When a user performs a SQL query, Oracle tries to retrieve the data from the database buffer cache (memory) first, then goes to disk if it is not in memory already. Reading data blocks from disk is much more expensive than reading the data blocks from memory. The goal with Oracle should always be to maximize memory utilization.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the data blocks read from disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaReads / Transactions
where:

- DeltaReads: difference in 'select value from v$sysstat where name='physical reads'' between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and physical reads per transaction.

Recommended Frequency

5 minutes

User Action

Block reads are inevitable so the aim should be to minimize unnecessary IO. This is best achieved by good application design and efficient execution plans. Changes to execution plans can yield orders of magnitude changes in performance. Tweaking at system level usually only achieves percentage gains.

To identify the SQL that is responsible for the largest portion of physical reads, use the Top SQL (Physical Reads) Chart. This chart will allow you to quickly determine which SQL statements are causing the I/O activity. From this chart you can view the full text of the SQL statement. Further investigation on how to best tune a particular SQL statement can be done by using the Explain Plan drilldown, or if you are on NT, the Tune SQL Statement drilldown as well.

To view I/O on a per session basis to determine which sessions are responsible for your physical reads, you can use the Top Sessions by Physical Reads Chart. This approach allows you to identify problematic sessions and then drill down to their current SQL statement to perform tuning.

If the SQL statements are properly tuned and optimized the following suggestions may help. A larger buffer cache may help - test this by actually increasing DB_BLOCK_BUFFERS and not by using DB_BLOCK_LRU_EXTENDED_STATISTICS. Never increase the SGA size if it will induce additional paging or swapping on the system.

A less obvious issue which can affect the IO rates is how well data is clustered physically. For example, assume that you frequently fetch rows from a table where a column is between two values via an index scan. If there are 100 rows in each index block then the two extremes are: 1. Each of the table rows is in a different physical block (100 blocks need to be read for each index block). 2. The table rows are all located in the few adjacent blocks (a handful of blocks need to be read for each index block).

Pre-sorting or reorganizing data can help to tackle this in severe situations as well.

Physical Writes Per Second

Description

This data item represents the number of disk writes per second during the sample period. This statistic represents the rate of database blocks written from the SGA

buffer cached to disk by the DBWR background process, and from the PGA by processes performing direct writes.

This test checks the data blocks written disk per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaWrites / Seconds
where:

- DeltaWrites: difference in 'select value from v$sysstat where name='physical writes" between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and physical writes per second.

Recommended Frequency

5 minutes

User Action

Because this statistic shows both DBWR writes as well as direct writes by sessions, you should view the physical writes directly to determine where the write activity is actually occurring. If the physical writes direct value comprises a large portion of the writes, then there are probably many sorts or writes to temporary tablespaces occurring. You can investigate further into sort activity by viewing the Top Sessions by Disk Sorts Chart.

If the majority of the writes are not direct, they are being performed by the DBWR writes process. This is only be a problem if log writer or redo waits are showing up in the Sessions Waiting for this Event Chart or the Top Waits by Time Waited Chart. These charts can be found at the bottom of the database overview chart.

You can also view DBWR performance and health in the DBWR Analysis Chart. This chart is comprised of a number of charts that breakdown the DBWR activity into categories that determine whether it is functioning efficiently.

To immediately analyze where the I/O operations are actually taking place, view the File Write Operations Chart. This chart lists the top data files by the number of writes per second. Similarly, to determine which files have the slowest access times use the Average Cost of I/O Chart. This chart lists which files are the slowest to access resulting in bottlenecks in your system.

Lastly, to view Background Process I/O statistics on a per transaction basis the Background Process I/O - Per Transaction Chart displays the amount of I/O attributed to each transaction on average.

Physical Writes Per Transaction

Description

This data item represents the number of disk writes per transaction during the sample period.

The value of this statistic is zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name is a better indicator of current performance.

This test checks the data blocks written disk per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaWrites / Transactions
where:

- DeltaWrites: difference in 'select value from v$sysstat where name='physical writes" between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and physical writes per transaction.

Recommended Frequency
5 minutes

User Action
Because this statistic shows both DBWR writes as well as direct writes by sessions, you should view the physical writes directly to determine where the write activity is really occurring. If the physical writes direct value comprises a large portion of the writes, then there are likely many sorts or writes to temporary tablespaces that are occurring. Further investigation into sort activity can be found with the Top Sessions by Disk Sorts Chart.

If the majority of the writes are not direct, they are being performed by the DBWR writes process. This will typically only be a problem if log writer or redo waits are showing up in the Sessions Waiting for this Event Chart or the Top Waits by Time Waited Chart.

Look for DBWR performance and health in the DBWR Analysis Chart. This chart is comprised of a number of charts that breakdown the DBWR and the statistics that determine if it is functioning efficiently.

Probe

Description
This event test checks whether a new connection can be established to a database. If the maximum number of users is exceeded or the listener is down, this test is triggered.

Parameters
None

Output
None

Recommended Frequency
10 minutes

User Action

Check the status of the listener to make sure it is running on the node where the event was triggered. If the listener is running, check to see if the number of users is at the session limit.

Note: The choice of user credentials for the Probe event test should be considered. If the preferred user has the RESTRICED SESSION privilege, the user will be able to connect to a database even if the LICENSE_MAX_SESSIONS limit is reached.

Process Limit

Description

The PROCESSES initialization parameter specifies the maximum number of operating system user processes that can simultaneously connect to a database at the same time. This number also includes background processes utilized by the instance.

This event test checks for the utilization of the process resource against the values (percentage) specified by the threshold arguments. If the percentage of all current processes to the limit set in the PROCESSES initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated.

Example

If 40 processes are currently connected and the value of PROCESSES is 50, the percentage is 80% (40 / 50 x 100). This value is compared against the specified thresholds.

Parameters

- Critical threshold: Threshold value for critical alert (%). Default is 90%.
- Warning threshold: Threshold value for warning alert (%). Default is 80%.

Output

Current value and the limit specified by PROCESSES

Recommended Frequency

30 seconds

User Action

Verify that the current PROCESSES instance parameter setting has not exceeded the operating system-dependent maximum. Increase the number of processes to be at

least 6 + the maximum number of concurrent users expected to log in to the instance.

Recursive Calls Per Second

Description

This data item represents the number of recursive calls, per second during the sample period.

Sometimes, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:

- when data dictionary information is not available in the data dictionary cache and must be retrieved from disk
- in the firing of database triggers
- in the execution of DDL statements
- in the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- in the enforcement of referential integrity constraints

This test checks the number of recursive SQL calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaRecursiveCalls / Seconds
where:

- DeltaRecursiveCalls: difference in 'select value from v$sysstat where name='recursive calls'' between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.

- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and recursive calls per second.

Recommended Frequency
5 minutes

User Action
If the Oracle Server appears to be making excessive recursive calls while your application is running, determine what activity is causing these recursive calls. If you determine that the recursive calls are caused by dynamic extension, either reduce the frequency of extension by allocating larger extents or, if you are using Oracle 8*i*, considering taking advantage of locally managed tablespaces.

Recursive Calls Per Transaction

Description
This data item represents the number of recursive calls, per second during the sample period.

Sometimes, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:

- when data dictionary information is not available in the data dictionary cache and must be retrieved from disk
- in the firing of database triggers
- in the execution of DDL statements
- in the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- in the enforcement of referential integrity constraints

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of

the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the number of calls that result in changes to internal tables. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaRecursiveCalls / Transactions
where:

- DeltaRecursiveCalls: difference in 'select value from v$sysstat where name='recursive calls'' between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and recursive calls per transaction.

Recommended Frequency

5 minutes

User Action

If the Oracle Server appears to be making excessive recursive calls while your application is running, determine what activity is causing these recursive calls. If you determine that the recursive calls are caused by dynamic extension, either reduce the frequency of extension by allocating larger extents or, if you are using Oracle 8*i*, considering taking advantage of locally managed tablespaces.

Redo Log Allocation Hit

Description

Redo log entries contain a record of changes that have been made to the database block buffers. The log writer (LGWR) process writes redo log entries from the log buffer to a redo log file. The log buffer should be sized so that space is available in the log buffer for new entries, even when access to the redo log is heavy. When the log buffer is undersized, user process will be delayed as they wait for the LGWR to free space in the redo log buffer.

The redo log buffer efficiency, as measured by the hit ratio, records the percentage of times users did not have to wait for the log writer to free space in the redo log buffer.

This event test monitors the redo log buffer hit ratio (percentage of success) against the values specified by the threshold arguments. If the number of occurrences is smaller than the values specified, then a warning or critical alert is generated.

Parameters

- Number of occurrences: Number of consecutive occurrences that redo log buffer hit ratio is below the thresholds before a warning or critical alert is generated. Default is 3.
- Critical threshold: Threshold for critical alert (%). Default is 98%.
- Warning threshold: Threshold of warning alert (%). Default is 100%.

Output

- Current ratio
- Current LOG_BUFFER in kilobytes

Recommended Frequency

30 seconds

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when buffering redo entries to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter in order to increase the size of the redo log buffer. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

Note: For Oracle Intelligent Agent release 9*i*, this event test has been obsoleted. It is recommended that you use the Redo NoWait Ratio event test. This event test is kept for backward compatibility with older versions of the Intelligent Agent.

Redo No Wait %

Description

Redo log entries contain a record of changes that have been made to the database block buffers. The log writer (LGWR) process writes redo log entries from the log buffer to a redo log file. The log buffer should be sized so that space is available in the log buffer for new entries, even when access to the redo log is heavy. When the log buffer is undersized, user process will be delayed as they wait for the LGWR to free space in the redo log buffer.

This data item represents the redo log buffer efficiency, as measured by the percentage of times users did not have to wait for the log writer to free space in the redo log buffer.

This test checks the percentage of times redo entries are allocated without having to wait. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

((DeltaRedoEntries - DeltaRedoLogSpaceRequests) / DeltaRedoEntries) * 100
where:

- DeltaRedoEntries: difference in 'select value from v$sysstat where name='redo entries" between sample end and start
- DeltaRedoLogSpaceRequests: difference in 'select value from v$sysstat where name='redo log space requests" between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and redo no wait percentage.

Recommended Frequency
5 minutes

User Action
The LOG_BUFFER initialization parameter determines the amount of memory that is used when buffering redo entries to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer if waiting is a problem. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

Redo Write Per Second

Description
This data item represents the number redo write operations per second during this sample period.

The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries can be used for database recovery if necessary.

The log writer processes (LGWR) is responsible for redo log buffer management; that is, writing the redo log buffer to a redo log file on disk.

This test checks the number of writes by LGWR to the redo log files per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
DeltaRedoWrites / Seconds
where:

- DeltaRedoWrites: difference in 'select value from v$sysstat where name='redo writes" between end and start of sample period

- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and redo write per second.

Recommended Frequency

5 minutes

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when redo entries are buffered to the redo log file.

Should waiting be a problem, consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

A drilldown is available to the Redo Analysis Chart for further analysis of the LGWR process. This event indicates that the LGWR process needs to be sped up. This is related to the throughput of the disk. Do NOT put redo on raid 5. Raid 5 is not efficient for writes. Use multiplexed redo on different spindles or mirrored disks for redo.

Lastly, if you would like to view Background Process I/O statistics on a per transaction basis the Background Process I/O - Per Transaction Chart displays the amount of I/O attributed to each transaction on average.

Redo Write Per Transaction

Description

This data item represents the number of redo write operations per second during this sample period.

The redo log buffer is a circular buffer in the SGA that holds information about changes made to the database. This information is stored in redo entries. Redo entries contain the information necessary to reconstruct, or redo, changes made to the database by INSERT, UPDATE, DELETE, CREATE, ALTER or DROP operations. Redo entries are used for database recovery, if necessary.

The log writer process (LGWR) is responsible for redo log buffer management; that is, writing the redo log buffer to a redo log file on disk.

This test checks the number of writes by LGWR to the redo log files per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaRedoWrites /(DeltaCommits+DeltaRollbacks)
where:

- DeltaRedoWrites: difference in 'select s.value from v$sysstat s, v$statname n where n.name='redo writes' and n.statistic#=s.statistic#' between sample end and start
- DeltaCommits: difference in 'select s.value from v$sysstat s, v$statname n where n.name='user commits' and n.statistic#=s.statistic#' between sample end and sample start
- DeltaRollbacks: difference in 'select s.value from v$sysstat s, v$statname n where n.name='user commits' and n.statistic#=s.statistic#' between sample end and sample start

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and redo writes per transaction.

Recommended Frequency

5 minutes

User Action

The LOG_BUFFER initialization parameter determines the amount of memory that is used when buffering redo entries to the redo log file.

Consider increasing the LOG_BUFFER initialization parameter to increase the size of the redo log buffer should waiting be a problem. Redo log entries contain a record of the changes that have been made to the database block buffers. The log writer process (LGWR) writes redo log entries from the log buffer to a redo log. The redo log buffer should be sized so space is available in the log buffer for new entries, even when access to the redo log is heavy.

Response Time Per Execute

Description

Using only statistics available within the database, this data item gives the best approximation of response time, in seconds, per SQL statement execution. This statistic may be more valid than response time per transaction as it shows accurate values even for read-only access.

This test checks the response time, in seconds, per SQL statement execution during sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

(DeltaTotalWait + DeltaCpuTime) / (DeltaUserCalls + DeltaRecursiveCalls)
where:

- DeltaTotalWait: difference of 'sum of time waited for all wait events in v$system_event' between sample end and start
- DeltaCpuTime: difference of 'select value from v$sysstat where name='CPU used by this session'' between sample end and start
- DeltaUserCalls: difference of 'select value from v$sysstat where name='user calls'' between sample end and start
- DeltaRecursiveCalls: difference of 'select value from v$sysstat where name='recursive calls'' between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and average response time in seconds per transaction.

Recommended Frequency
5 minutes

User Action
Investigate further into which component, waits or CPU, is responsible for the majority of the response time and then continue diagnosis.

Response Time Per Transaction

Description
Using only statistics available within the database, this data item gives the best approximation of response time, in seconds, per transaction during this sample period.

This test checks the response time in seconds, per transaction during this sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
(DeltaTotalWait + DeltaCpuTime) / (DeltaCommits + DeltaRollbacks)
where:

- DeltaTotalWait: difference of 'sum of time waited for all wait events in v$system_event' between sample end and start
- DeltaCpuTime: difference of 'select value from v$sysstat where name='CPU used by this session" between sample end and start
- DeltaCommits: difference of 'select value from v$sysstat where name='user commits" between sample end and start
- DeltaRollbacks: difference of 'select value from v$sysstat where name='user rollbacks" between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and average response time in seconds per transaction.

Recommended Frequency

5 minutes

User Action

Investigate further into which component, waits or CPU, is responsible for the majority of the response time and then continue diagnosis.

Rollback Contention

Description

Rollback segments are portions of the database that record the actions of transactions in case a transaction is rolled back. Rollback segments are used to provide read consistency, support rollback transactions, and recover a database.

Proper allocation of rollback segments make for optimal database performance. Using a sufficient number of rollback segments distributes rollback segment contention across many segments and improves performance.

Contention for rollback segments is reflected by contention for buffers that contain rollback segment blocks.

This event test monitors rollback segment missing ratio (percentage) against the values specified by the threshold arguments. If the missing ratio is greater than the values specified, then a warning or critical alert is generated.

Parameters

- Number of occurrences: Number of consecutive occurrences that rollback segment missing ratio is above the thresholds before a warning or critical alert is generated. Default is 3.
- Critical threshold: Threshold for critical alert (%). Default is 1.

- Warning threshold: Threshold for warning alert (%). Default is 0.

Output

- Current missing ratio
- Current number of concurrently active transactions
- Current number of online rollback segments

Recommended Frequency

30 seconds

User Action

To reduce contention for buffers containing rollback segment blocks, create additional rollback segments. The general guidelines for choosing how many rollback segments to allocate is based on the number and type of concurrently active transactions on your database. Allocate one rollback segment for each 10 concurrent OLTP (online transaction processing) transactions and one rollback segment for each concurrent batch job.

In addition, when creating a rollback segment keep extents within a rollback the same size by specifying STORAGE parameters where NEXT=INITIAL.

It is also recommended that you set the MINEXTENTS parameter value to 20. Because rollback segments are logically regarded as a circular queue of extents, they are required to have MINEXTENTS value of at least 2. The probability that a rollback segment will require a new extent allocation depends on how likely the next extents are to contain active undo. The more extents the rollback segment has, the less likely it that a rollback segment will require an extent allocation that could be avoided. Administrators should create rollback segments with many extents. Naturally, there is a point of diminishing returns. There is a rapid decline of a rollback segment's probability of extending as the number of extents increases. It has been determined that beyond 20 extents, the incremental decrease in the segment's probability of extending fails to justify the cost of the additional extent.

Rollbacks Per Second

Description

This data item represents the number of times, per second during the sample period, that users manually issue the ROLLBACK statement or an error occurred during a user's transactions.

This test checks the number of rollbacks per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number

of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaRollbacks / Seconds
where:

- DeltaRollbacks: difference in 'select value from v$sysstat where name='user rollbacks" between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and the number of rollbacks per second.

Recommended Frequency

5 minutes

User Action

This value shows how often users are issuing the ROLLBACK statement or encountering errors in their transactions. Further investigation should be made to determine if the rollbacks are part of some faulty application logic or due to errors occurring through database access.

Rollbacks Per Transaction

Description

This data item represents the number of times, per transaction during the sample period, that users manually issue the ROLLBACK statement or an error occurred during a user's transactions.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of

the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the Number of rollbacks per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaRollbacks / Transactions
where:

- DeltaRollbacks: difference in 'select value from v$sysstat where name='user rollbacks" between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and the number of rollbacks per transaction.

Recommended Frequency

5 minutes

User Action

This value shows how often users are issuing the ROLLBACK statement or encountering errors in their transactions. Further investigation should be made to determine if the rollbacks are part of some faulty application logic or due to errors occurring through database access.

Session Limit

Description

The SESSIONS initialization parameter specifies the maximum number of concurrent connections that the database will allow.

This event test checks for the utilization of the session resource against the values (percentage) specified by the threshold arguments. If the percentage of the number of sessions, including background processes, to the limit set in the SESSIONS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated.

Example

If there are 20 sessions and the value of SESSIONS is 25, the percentage is 80% (20 / 25 x 100). This value is compared against the specified thresholds.

Parameters

- Critical threshold: Threshold value for critical alert (%). Default is 90%.
- Warning threshold: Threshold value for warning alert (%). Default is 80%.

Output

Current value and the limit specified by SESSIONS

Recommended Frequency

30 seconds

User Action

Increase the SESSIONS instance parameter. For XA environments, confirm that SESSIONS is at least 2.73 * PROCESSES. For shared server environments, confirm that SESSIONS is at least 1.1 * maximum number of connections.

Session Terminated

Description

This event test signifies that a session terminated unexpectedly since the last sample time. The ALERT file is a special trace file containing a chronological log of messages and errors. An alert is displayed when session unexpectedly terminated (ORA-00603) messages are written to the ALERT file.

Parameters

None

Output

ALERT log error messages since the last sample time

Recommended Frequency

30 seconds

User Action

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

Snapshot Log Full

Description

A master table's snapshot log keeps track of fast refresh data for all corresponding snapshots. When a snapshot log is created for a master table, Oracle creates an underlying table to support the snapshot log. Oracle automatically tracks which rows in a snapshot log have been used during the refreshes of snapshots, and purges those rows from the log. Oracle does not delete rows from the log until all snapshots have used them. As a result, in certain situations a snapshot log can grow indefinitely when multiple snapshots are based on the same master table. It is best to always try to keep a snapshot log as small as possible to minimize the database space that it uses.

This event test checks whether a snapshot log is too large. In order to do this, the test determines the number of snapshot log tables containing more rows than specified by the Snapshot log's table size parameter. If this number is greater than the threshold value specified in the threshold argument, then an alert is generated.

Parameters

- Threshold for alert (number of snapshot log tables). Default is 1 snapshot log table.
- Snapshot log table size (number of rows). Default is 100 rows.

Output

Snapshot log table and its size

Recommended Frequency

30 seconds

User Action

To remove rows from a snapshot log and free up space for newer log records, you can refresh the snapshots associated with the log so that Oracle can purge rows from the snapshot log or manually purge records in the log by deleting the rows required only by the nth least recently refreshed snapshots.

To manually purge rows from a snapshot log, execute the PURGE_LOG stored procedure of the DBMS_SNAPSHOT package at the database that contains the log.

Note: Running the Snapshot Log Full event test may be a resource-intensive operation. Therefore, Oracle recommends running the Snapshot Log Full event test during off-peak periods.

Soft Parse %

Description

A soft parse is recorded when the Oracle Server checks the shared pool for a SQL statement and finds a version of the statement that it can reuse.

This data item represents the percentage of parse requests where the cursor was already in the cursor cache compared to the number of total parses. This ratio provides an indication as to how often the application is parsing statements that already reside in the cache as compared to hard parses of statements that are not in the cache.

This test checks the percentage of soft parse requests to total parse requests. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

((DeltaParseCountTotal - DeltaParseCountHard) / DeltaParseCountTotal) * 100
where:

- DeltaParseCountTotal: difference in 'select value from v$sysstat where name='parse count (total)" between sample end and start
- DeltaParseCountHard: difference in 'select value from v$sysstat where name='parse count (hard)" between sample end and start

Parameters

- Warning Threshold: Default is 50. The value can be between 0.0 and 100.0.
- Critical Threshold: Default is 30. The value can be between 0.0 and 100.0.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance Name and soft parse percentage.

Recommended Frequency
5 minutes

User Action
Soft parses consume less resources than hard parses, so the larger the value for this item, the better. But many soft parses indicate the application is using SQL inefficiently. Reparsing the statement, even if it is a soft parse, requires a network round trip from the application to the database, as well as requiring the processing time to locate the previously compiled statement in the cache. Reducing network round trips and unnecessary processing will improve application performance.

If this data item is below 80% you should look at the Top Sessions by Hard Parse Count Chart. This chart lists the sessions that are currently performing the most hard parses. Starting with these sessions and the SQL statements they are executing will indicate which applications and corresponding SQL statements are being used inefficiently.

A faster way to identify SQL statements that might be candidates for bind variable replacement is the Similar SQL Statements Chart. This identifies which statements are similar in the first 'n' characters and how many versions of that statement segment are in the cache. Further drilldown will show the full text of the SQL statements and allow you to see if the statements are truly viable candidates for re-write.

If the data item is currently showing a high value, the expensive hard parses are not occurring but the application can still be tuned by reducing the amount of soft parses. Use the Top SQL (Parses) Chart to identify the SQL statements that have been most parsed. This will allow you to quickly identify SQL that is being re-parsed unnecessarily. You should investigate these statements first for possible application logic changes such that cursors are opened once, and executed or fetched from many times.

To see the actual values of the underlying statistics used to compute this resource you can use the Parse Statistics Chart. This chart shows the Parse, Execute, and Hard Parse rates per second.

SysStat Table

Description

You can monitor any system statistic available in the database with this event test. A warning or critical alert will be generated if the value of the selected V$SYSSTAT parameter exceeds the values specified by the threshold arguments.

To view the V$SYSSTAT parameter names and values, connect to the database with SQL Worksheet and execute SELECT NAME, VALUE FROM V$SYSSTAT.

Parameters

- Number of occurrences: Number of consecutive occurrences that is greater than or equal to the thresholds before a warning or critical alert is generated. Default is 3.
- Critical threshold: Threshold for critical alert (parameter value). Default is 15.
- Warning threshold: Threshold for warning alert (parameter value). Default is 10.
- Parameter name: The name of the parameter in the V$SYSSTAT table that you want to monitor. Do not use quotes.

Output

Parameter's current value

Recommended Frequency

30 seconds

User Action

The user action for the event is dependent on the statistic that is being monitored.

SysStat Table Delta

Description

You can monitor any system statistic available in the database with this event test. The threshold values are compared to the difference between the last sample point and the current sample point of the V$SYSSTAT parameter. A warning or critical alert is generated if the calculated difference exceeds the values specified by the threshold arguments.

To view the V$SYSSTAT parameter names and values, connect to the database with SQL Worksheet and execute SELECT NAME, VALUE FROM V$SYSSTAT.

Parameters

- Number of occurrences: Number of consecutive occurrences that is greater than or equal to the thresholds before a warning or critical alert is generated. Default is 3.
- Critical threshold: Threshold for critical alert (change in parameter value). Default is 15.
- Warning threshold: Threshold for warning alert (change in parameter value). Default is 10.
- Parameter: The name of the parameter in the V$SYSSTAT table that you want to monitor. Do not use quotes.

Output

Parameter name and change in parameter's value

Recommended Frequency

30 seconds

User Action

The user action for the event is dependent upon the statistic that is being monitored.

Table Scans (Long) Per Second

Description

This data item represents the number of long table scans per second during sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.

This test checks the long table scans per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaScans / Seconds
where:

- DeltaScans: difference in 'select value from v$sysstat where name='table scans (long tables)'' between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and the number of long table scans per second.

Recommended Frequency

5 minutes

User Action

A table scan means that the entire table is being scanned record by record in order to satisfy the query. For small tables that can easily be read into and kept in the buffer cache this may be advantageous. But for larger tables this will force a lot of physical reads and potentially push other needed buffers out of the cache. SQL statements with large physical read and logical read counts are candidates for table scans. They can be identified either through the Top SQL (Physical Reads) Chart, or through the Top Sessions by Physical Reads Chart, with a drilldown to the current SQL for a session.

Table Scans (Long) Per Transaction

Description

This data item represents the number of long table scans per transaction during sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the number of long table scans per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
DeltaScans / Transactions
where:

- DeltaScans: difference in 'select value from v$sysstat where name='table scans (long tables)" between end and start of sample period
- Transactions: number of transactions in sample period

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and the number of long table scans per transaction.

Recommended Frequency
5 minutes

User Action
A table scan means that the entire table is being scanned record by record in order to satisfy the query. For small tables that can easily be read into and kept in the buffer cache this may be advantageous. But for larger tables this will force a lot of physical reads and potentially push other needed buffers out of the cache. SQL statements with large physical read and logical read counts are candidates for table scans. They can be identified either through the Top SQL (Physical Reads) Chart, or through the Top Sessions by Physical Reads Chart, with a drilldown to the current SQL for a session.

Table Scans (Total) Per Second

Description
This data item represents the number of long and short table scans per second during the sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.

Data Source

(DeltaLongScans + DeltaShortScans) / Seconds
where:

- DeltaLongScans: difference in 'select value from v$sysstat where name='table scans (long tables)" between end and start of sample period
- DeltaShortScans: difference in 'select value from v$sysstat where name='table scans (short tables)" between end and start of sample period
- DeltaShortScans: difference in 'select value from v$sysstat where name='table scans (short tables)" between end and start of sample period
- DBA_index_fast_full_scans_full
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and total table scans per second.

Recommended Frequency

5 minutes

User Action

A table scan indicates that the entire table is being scanned record-by-record in order to satisfy the query. For small tables that can easily be read into and kept in the buffer cache, this may be advantageous. But larger tables will force many physical reads and potentially push other required buffers out of the cache. SQL statements with large physical read and logical read counts are candidates for table scans. They can be identified through two different methods. The Top Sessions by Physical Reads Chart displays sessions that are responsible for the current I/O activity. The Top SQL (Physical Reads) Chart lists the SQL statements in the cache by the amount of I/O they have performed. Some of these SQL statements may have high I/O numbers but they may not be attributing to the current I/O load.

The Table Scans per Transaction Chart shows table scan rates on a per-transaction rate. This chart provides an understanding of what type of table scan activity each transaction is performing. The per-transaction figures may be easier to use for comparisons to determine whether application performance has been improved or degraded. While the transaction rate may change from time to time, the amount of work the transactions do may stay the same, thus giving you a more concrete number for comparisons.

Table Scans (Total) Per Transaction

Description

This data item represents the number of long and short table scans per transaction during the sample period. A table is considered 'long' if the table is not cached and if its high-water mark is greater than 5 blocks.

This test checks the number of long and short table scans per transaction. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

(DeltaLongScans + DeltaShortScans) / Transactions
where:

- DeltaLongScans: difference in 'select value from v$sysstat where name='table scans (long tables)" between end and start of sample period
- DeltaShortScans: difference in 'select value from v$sysstat where name='table scans (short tables)" between end and start of sample period
- DeltaShortScans: difference in 'select value from v$sysstat where name='table scans (short tables)" between end and start of sample period
- DBA_index_fast_full_scans_full
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and the number of total table scans per transaction.

Recommended Frequency
5 minutes

User Action
A table scan indicates that the entire table is being scanned record-by-record in order to satisfy the query. For small tables that can easily be read into and kept in the buffer cache, this may be advantageous. But larger tables will force many physical reads and potentially push other required buffers out of the cache. SQL statements with large physical read and logical read counts are candidates for table scans. They can be identified through two different methods. The Top Sessions by Physical Reads Chart displays sessions that are responsible for the current I/O activity. The Top SQL (Physical Reads) Chart lists the SQL statements in the cache by the amount of I/O they have performed. Some of these SQL statements may have high I/O numbers but they may not be attributing to the current I/O load.

The Table Scans per Transaction Chart shows the individual table scan rates on a per-transaction rate. This chart provides an understanding of what type of table scan activity each transaction is performing. The per-transaction figures may be easier to use for comparisons to determine whether application performance has been improved or degraded. While the transaction rate may change from time to time, the amount of work the transactions do may stay the same, thus giving you a more concrete number for comparisons.

Tablespace Full

Description
As segments within a tablespace grow, the free space within that tablespace decreases. Should free space become insufficient, the creation of new segments or the extension of existing segments will fail.

This event test checks for the total free space in the tablespace specified by the Tablespace name. If the percentage of used space is greater than the values specified in the threshold arguments, then a warning or critical alert is generated.

Parameters

- Tablespace name filter: Filter of the tablespace names to be monitored, or * for all tablespaces. Tablespaces that are either read-only or off-line are excluded. Default is *. The filter must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'. **Note:** There are higher resource requirements if there is a large number of objects being monitored at high frequencies, for example, checking the space for all 200 tablespaces every 2 minutes. Where possible, Oracle recommends that you use the filters to narrow the scope of the objects being monitored. Also, set the polling schedule to a value that is appropriate to your environment. For example, tablespaces that do not grow rapidly in size may be checked every 2 days instead of every 5 minutes.
- Critical threshold: Threshold value for critical alert (%). Default is 90%.
- Warning threshold: Threshold value for warning alert (%). Default is 80%.

Output

- Tablespace name
- Current used space in percentage
- Current free space in kilobytes

Recommended Frequency

30 seconds

User Action

Increase the size of the tablespace by enabling automatic extension for one of its data files, manually resizing one of its data files, or adding a new datafile.

Note: If the tablespace you are monitoring has Autoextend ON, then the percentage of space used is calculated as follows.

Variables are: A = maximum size of tablespace; B = current size of tablespace; C = used size of datafile; D = free space

If you specify a maximum size for the tablespace and free space is greater than the maximum size of tablespace minus the current size of the tablespace (D > A - B), then the usage is calculated by dividing the used size of the datafile by the maximum size of the tablespace (C / A). For example, if D = 300M, A = 200M, B = 100M, and C = 50M, then this tablespace is 25% full (50M / 200M). Otherwise, the usage is calculated as [C / (B + D)]. For example, if D = 50M, A = 200M, B = 100M, and C = 30M, then this tablespace is 20% full [30M / (100M + 50M)].

If you specify a maximum size of unlimited, then the total available free space is taken into account [C / (B + D)]. For example, if you have a 100M tablespace with

50M used and the physical disk is 400M free space, then the usage is: [50M / (100M + 400M)] = 10%.

Note: Running the Tablespace Full event test may be a resource-intensive operation. Therefore, Oracle recommends running the Tablespace Full event test during off-peak periods.

Total Pings

Description

This data item represents the ping count per second for a Real Application Clusters database during this sample period.

This test checks the total number of pings per second. If the value is greater than the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaPings / Seconds
where:

- DeltaPings: difference of 'select sum(value) rac_pings from gv$sysstat where name = 'DBWR cross instance writes' between sample end and start

Parameters

- Warning Threshold: Default is 200 pings/sec.
- Critical Threshold: Default is 400 pings/sec.
- Number of Occurrences: Default is 1.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Total number of pings per second.

Recommended Frequency

5 minutes

User Action

Investigate further into which instance or which file contribute most of the database ping by drilldown to Instance Ping Chart and Ping By File Chart

Transactions Per Second

Description

This data item represents the total number of commits and rollbacks performed during this sample period.

This test checks the number of commits and rollbacks performed during sample period. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaCommits + DeltaRollbacks
where:

- DeltaCommits: difference of 'select value from v$sysstat where name='user commits'' between sample end and start
- DeltaRollbacks: difference of 'select value from v$sysstat where name='user rollbacks'' between sample end and start
- Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and transaction count per second.

Recommended Frequency

5 minutes

User Action

This statistic is an indication of how much work is being accomplished within the database. A spike in the transaction rate may not necessarily be bad. If response times stay close to normal, it means your system can handle the added load. Actually, a drop in transaction rates and an increase in response time may be indicators of problems. Depending upon the application, transaction loads may vary widely across different times of the day.

The Transaction Based Execution Rates Chart will allow you to quickly determine the amount of work or user activity being performed per transaction.

Quick analysis of the database's CPU consumption can be done by using the CPU Breakdown Chart. This chart breaks the database CPU consumption into 3 parts, and further analysis into the largest portion of the CPU time will lead you towards reducing your CPU consumption.

Unscheduled Jobs

Description

The Oracle server job queue is a database table that stores information about local jobs.

This event test checks for unscheduled DBMS jobs. An alert is generated when the number of jobs, whose execution time has exceeded the value specified by the Job Completion Time argument, exceeds the value specified in the Alert Threshold. A job's completion date/time is calculated by using the NEXT_DATE value in the SYS.DBA_JOBS view plus the approximate time it takes to complete a job as specified by the job completion time argument.

Parameters

- Alert threshold: Threshold for alert (number of jobs). Default is 0.
- Job completion time: Approximate time for job completion in minutes. Default is 10 minutes.

Output

Job identifiers of jobs that are not rescheduled for execution

Recommended Frequency

30 seconds

User Action

Check the FAILURES and BROKEN values in the SYS.DBA_JOBS view.

If the job failed to execute, check the ALERT log and trace files for error information and fix the error.

If the job was never executed, there may be a problem with the availability of SNP background processes. Check the initialization parameter JOB_QUEUE_ PROCESSES to determine the maximum number of background processes available and JOB_QUEUE_INTERVAL to determine how frequently each background process wakes up.

UpDown Database

Description
This event test checks whether the database being monitored is running. If this test is triggered, other database events are ignored.

Parameters
None

User Action
The Startup Database job task can be set up as a fixit job for automatically correcting the problem.

Note: If the listener serving a database is down, this event may be triggered because the Intelligent Agent uses the listener to communicate with the database. This note applies to Intelligent Agents released before 8.0.5.

User Audit

Description
This event test monitors specified database user connections. For example, an alert is displayed when a particular database user connection, specified by the User name filter argument, has been detected.

Parameters
User Name filter: Filter the user names to be monitored, or * for all users. Default is =’SYS’. The filter must include SQL syntax, for example, = 'ABC', in ('XYZ', 'ABC'), like '% ABC'.

Note: The user name is case sensitive. By default the user name is all upper case. To define a name in lower case, the name must be in double quotes, for example, "abc". The user name must be exactly as it appears in the all_users view.

Output
- User name
- Number of current sessions for user
- Operating system machine name where user is logged on

Recommended Frequency
5 minutes

User Action
User actions may vary depending on the user connection that is detected.

User Blocks

Description
This event test signifies that a database user is blocking at least one other user from performing an action, such as updating a table. An alert is generated if the number of consecutive blocking occurrences reaches the specified value.

Note: The catblock.sql script needs to be run on the managed database prior to using the User Blocks test. This script creates some additional tables, view, and public synonyms that are required by the User Blocks test.

Parameters
Number of occurrences: Number of consecutive occurrences a user can be blocked before an alert is generated. Default is three.

Output
Session Id of the user who is blocking other users

Recommended Frequency
30 seconds

User Action
Either have user who is blocking other users rollback the transaction, or wait until the blocking transaction has been committed.

User Call %

Description
This data item represents the percentage of user calls to recursive calls.

Occasionally, to execute a SQL statement issued by a user, the Oracle Server must issue additional statements. Such statements are called recursive calls or recursive SQL statements. For example, if you insert a row into a table that does not have enough space to hold that row, the Oracle Server makes recursive calls to allocate the space dynamically if dictionary managed tablespaces are being used. Recursive calls are also generated:

When data dictionary information is not available in the data dictionary cache and must be retrieved from disk

- In the firing of database triggers
- In the execution of DDL statements
- In the execution of SQL statements within stored procedures, functions, packages and anonymous PL/SQL blocks
- In the enforcement of referential integrity constraints

This test checks the percentage of user calls to recursive calls. If the value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

(DeltaUserCalls/(DeltaRecursiveCalls + DeltaUserCalls)) * 100
where:

- DeltaRecursiveCalls: difference in 'select value from v$sysstat where name='recursive calls'' between sample end and start
- DeltaUserCalls: difference in 'select value from v$sysstat where name='user calls'' between sample end and start

Parameters

- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance Name and user call percentage.

Recommended Frequency

5 minutes

User Action

A low value for this data item means that the Oracle Server is making a large number of recursive calls. If the Oracle Server appears to be making excessive recursive calls while your application is running, determine what activity is causing these recursive calls. If you determine that the recursive calls are caused by dynamic

extension, either reduce the frequency of extension by allocating larger extents or, if you are using Oracle 8*i*, considering taking advantage of locally managed tablespaces.

User Calls Per Second

Description

This data item represents the number of logins, parses, or execute calls per second during the sample period,

This test checks the number of logins, parses, or execute calls. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaUserCalls / Seconds
where:

- DeltaUserCalls: difference in 'select value from v$sysstat where name='user calls'' between end and start of sample period
- Seconds: number of seconds in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output

Instance name and user calls per second.

Recommended Frequency

5 minutes

User Action

This statistic is a reflection of how much activity is going on within the database. Spikes in the total user call rate should be investigated to determine which of the underlying calls is actually increasing. Parse, execute and logon calls each signify

different types of user or application actions and should be addressed individually. User Calls is an overall activity level monitor.

The Transaction Based Execution Rates Chart will allow you to quickly determine the amount of work or user activity being performed per transaction.

Quick analysis of the database's CPU consumption can be done by using the CPU Breakdown Chart. This chart breaks the database CPU consumption into 3 parts, and further analysis into the largest portion of the CPU time will lead you towards reducing your CPU consumption.

User Calls Per Transaction

Description

This data item represents the number of logins, parses, or execute calls per transaction during the sample period,

The value of this statistic will be zero if there have not been any write or update transactions committed or rolled back during the last sample period. If the bulk of the activity to the database is read only, the corresponding "per second" data item of the same name will be a better indicator of current performance.

This test checks the number of logins, parses, or execute calls per second. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

DeltaUserCalls / Transactions
where:

- DeltaUserCalls: difference in 'select value from v$sysstat where name='user calls'' between end and start of sample period
- Transactions: number of transactions in sample period

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Instance name and user calls per transaction.

Recommended Frequency
5 minutes

User Action
This statistic is a reflection of how much activity is going on within the database. Spikes in the total user call rate should be investigated to determine which of the underlying calls is actually increasing. Parse, execute and logon calls each signify different types of user or application actions and should be addressed individually. User Calls is an overall activity level monitor.

User Limit

Description
The LICENSE_MAX_SESSIONS initialization parameter specifies the maximum number of concurrent user sessions allowed simultaneously.

This event test checks whether the number of users logged on is reaching the license limit. If the percentage of the number of concurrent user sessions to the limit set in the LICENSE_MAX_SESSIONS initialization parameter exceeds the values specified in the threshold arguments, then a warning or critical alert is generated. If LICENSE_MAX_SESSIONS is not explicitly set to a value, the test does not trigger.

Note: This event test is most useful when session licensing is enabled. Refer to the Oracle Server Reference Manual for more information on LICENSE_MAX_ SESSIONS and LICENSE_MAX_USERS.

Example

If there are 15 concurrent user sessions and the value of LICENSE_MAX_SESSIONS is 20, the percentage is 75% (15/20 x 100). This value is compared against the specified thresholds.

Parameters
- Critical threshold: Threshold value for critical alert (%). Default is 90%.
- Warning threshold: Threshold value for warning alert (%). Default is 80%.

Output
Current value and the limit specified by SESSIONS

Recommended Frequency
30 seconds

User Action
This typically indicates that the license limit for the database has been reached. The user will need to acquire additional licenses, then increase LICENSE_MAX_SESSIONS to reflect the new value.

User-Defined SQL Event Test

Description
The User-Defined SQL event test allows you to define your own SQL script that evaluates an event test. The event tests you define should be written as queries (i.e. SELECT statements) that return condition values for which you are monitoring. These values are checked against the Critical threshold and Warning threshold limits you specify, and trigger the event if the threshold limits are reached.

Example

You have a custom application that runs against the Oracle database. Each time it finds an application error, it creates an entry into a table called "error_log". Using the "User-Defined SQL Test", you can write an event test that notifies you when it finds at least 50 errors. Specifically, you define the following SQL statement:

select count(*) from error_log

This returns the number of rows in the error_log table. Since you want a critical alert raised when it reaches at least 50, you specify the Operator " >= ", a Critical Threshold value of 50, and perhaps a Warning Threshold value of 30.

Support for PL/SQL Functions
If your query for the event condition requires more complex processing than is allowed in a single SELECT statement, you can first create a pl/sql function that contains the extra processing steps, and then use the pl/sql function with the User-Defined SQL event test. Your pl/sql function must still return a value that can be compared against the Critical and Warning thresholds.

Example

You need to trigger a critical alert whenever an employee's salary is $500 higher than the highest manager's salary. You first define a pl/sql function as follows:

create or replace function overpaid_emp return number is

max_mgr_sal number;

```
max_emp_sal number;

begin

select max(sal) into max_mgr_sal from scott.emp where job = 'MANAGER' or job =
'PRESIDENT';

select max(sal) into max_emp_sal from scott.emp where job != 'MANAGER' and job
!= 'PRESIDENT';

return (max_emp_sal - max_mgr_sal);

end;
```

This pl/sql function returns the difference between the highest employee's salary and the highest manager's salary. If the difference is a positive number, then an employee has the higher pay. If the difference is more than 500, then a critical alert needs to be triggered.

When defining this event this using the User-Defined SQL event test, you define the SQL statement as follows:

```
select overpaid_emp from dual
```

Then use the Operator ">" and Warning threshold of 100 and Critical threshold of 500.

Note that ROLES are not enabled within pl/sql functions, so any privileges that are granted via ROLES will not work from within the function. You may need to grant the privileges directly to the database user account that is used for the event. (The database user account used for the event is either the Preferred Credentials user for the database, or is the credentials specified to overwrite the preferred credentials).

Parameters

- Override Preferred Credential: Check this box if you want to change the user name or password or both.
- Operator: Select one of the following comparison operators: == (equal); < (less than); > (greater than); <= (less than or equal to); >= (greater than or equal to); != (not equal)
- Critical Threshold: Depending on the SQL script, type a number or a text string.
- Warning Threshold: Depending on the SQL script, type a number or a text string.

- Occurrences Preceding Notifications: Type a numeric value indicating how many times this test must return true before an alert flag is displayed in the Console and before a notification is sent.
- SQL: Type the SQL script you want to use. You can also cut and paste SQL from an existing script.

Output
Value returned by the SQL script

Recommended Frequency
60 seconds

User Action
The action depends on the SQL script and hence Oracle cannot make any recommendations.

Wait by Session Count

Description
This data item represents the number of sessions currently waiting on this event.

This test checks the number of sessions currently waiting for the event specified by the Wait Event(s) parameter. If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Select event,count(*) from v$session_wait where wait_time = 0 group by event

Parameters
- Wait Event(s): Name of the wait event.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Wait event and wait by session count.

Recommended Frequency
5 minutes

User Action
The wait event that has the largest number of sessions waiting for it may show the largest area of contention. The event may also show where delays for resources are occurring. Further investigation into the details of these wait events will help determine the exact reason for waits.

Wait by Time

Description
This data item represents the length of time, in seconds, spent waiting for the event during the last sample period. This value will always be 0 unless the TIMED_ STATISTICS parameter is TRUE.

This test checks the length of time, in seconds, spent waiting for the event specified by the Wait Event(s) parameter during the last sample period If the value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
DeltaTimeWaited
where:

- DeltaTimeWaited: difference of 'select time_waited from v$system_event' between sample end and start

Parameters
- Wait Event(s): The name of the event.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: Default is 3.

For information about setting appropriate threshold values, see Baselining Threshold Values.

Output
Event name and the number of waits.

Recommended Frequency

5 minutes

User Action

Time spent waiting is time that could have been spent processing. Attacking the wait event with the largest wait time will probably produce the largest gain. Drilldowns are available to charts that are tailored to help diagnose and improve the performance of individual wait events.

If this data item's value is 0 and the wait count is non-zero, then the database parameter TIMED_STATISTICS is currently set to FALSE. There is a drilldown chart available for all wait events called Timed Statistics Chart. This chart shows the current value for the TIMED_STATISTICS parameter. Use the Turn On Timed Statistics drilldown to turn on timed statistics for the instance.

3

Compaq Tru64 Event Tests

The Oracle Enterprise Manager Advanced Event Tests for Compaq Tru64 are divided into a series of classes or groupings that will enable you to find the event test you are interested in registering.

The class names and some of the events that you can register within the classes are listed as follows.

- File System Class: includes percentage of free space and free kilobytes (See Table 3–1)
- Process Class: includes virtual size of the process, thread counts, and system time (See Table 3–2)

Summary of Compaq Tru64 Event Tests

The following tables list the Compaq Tru64 event tests by class. The full descriptions of the individual event tests follow the tables. The event tests are in alphabetical order.

Table 3–1 File System Class Event Tests

Event Test	Description
Available (KB)	Available is the amount of space, in kilobytes, available for the creation of new files by users who do not have superuser privileges. This test checks for available space on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the space available is less than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Used (KB)	Used is the amount of space (in kilobytes) allocated to existing files. This test checks for space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all file systems). If the space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Utilized (%)	Utilized is the percentage of space that is currently allocated to all files on the file system. This test checks for the percentage of space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the percentage of space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 3–2 Process Class Event Tests

Event Test	Description
Percent Memory Used	Percent Memory Used is the ratio of the resident set size of a process to the physical memory on the machine, expressed as a percentage. This test checks the percent memory used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the percent memory used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Resident Size	Resident Size is the resident set size of a process, in kilobytes. This test checks the resident size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the resident size of one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Time	System Time (%) is the percentage of system level CPU time that a process used. This test checks the percentage of system time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the System Time (%) value used by any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 3–2 Process Class Event Tests (Cont.)

Event Test	Description
Threads	Threads is the number of lwps (lightweight processes) in a process.
	This test checks the number of threads in the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the number of threads is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
User Time	User Time (%) is the percentage of user level CPU time that a process used.
	This test checks the percentage of user time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the User Time (%) value used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Virtual Size	Virtual Size is the total size of a process in virtual memory, in kilobytes.
	This test checks the total size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the total size of any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Descriptions of Compaq Tru64 Event Tests

The Compaq Tru64 Event Tests are listed in alphabetical order.

Available (KB)

Description

Available is the amount of space, in kilobytes, available for the creation of new files by users who do not have superuser privileges.

This test checks for available space on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the space available is less than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from statvfs.

Parameters

- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use

Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".

- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The available space in kilobytes on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Percent Memory Used

Description
Percent Memory Used is the ratio of the resident set size of a process to the physical memory on the machine, expressed as a percentage.

This test checks the percent memory used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the percent memory used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from /proc.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Process name with process ID: To identify the exact process.

Percent Memory Used: The ratio of a process's resident set size to the physical memory on the machine.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Resident Size (KB)

Description
Resident Size is the resident set size of a process, in kilobytes.

This test checks the resident size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the resident size of one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from /proc.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Process name with process ID: To identify the exact process.

Resident Size: The resident set size of a process, in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Time (%)

Description
System Time (%) is the percentage of system level CPU time that a process used.

This test checks the percentage of system time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the System Time (%) value used by any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from /proc.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Process name with process ID: To identify the exact process.

System Time: The percentage of system level CPU time that a process used.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Threads

Description
Threads is the number of lwps (lightweight processes) in a process.

This test checks the number of threads in the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the number of threads is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from /proc.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Process name with process ID: To identify the exact process.

Threads: the number of threads in a process.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Used (KB)

Description
Used is the amount of space (in kilobytes) allocated to existing files.

This test checks for space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all file systems). If the space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from statvfs.

Parameters
- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The used space in kilobytes on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

User Time

Description
User Time (%) is the percentage of user level CPU time that a process used.

This test checks the percentage of user time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the User Time (%) value used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from /proc.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Process name with process ID: To identify the exact process.

User Time: The percentage of user level CPU time that a process used.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Utilized (%)

Description
Utilized is the percentage of space that is currently allocated to all files on the file system.

This test checks for the percentage of space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the percentage of space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from statvfs.

Parameters

- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of space used on the file system.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Virtual Size (KB)

Description

Virtual Size is the total size of a process in virtual memory, in kilobytes.

This test checks the total size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the total size of any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from /proc.

Parameters

- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert, in kilobytes.

- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

Process name with process ID: To identify the exact process.

Virtual Size: the total size of a process in virtual memory, in kilobytes.

Recommended Frequency

5 minutes

User Action

Specific to your site.

4

HP-UX Event Tests

The Oracle Enterprise Manager Advanced Event Tests for HP-UX are divided into a series of classes or groupings that will enable you to find the event test you are interested in registering.

The class names and some of the events that you can register within the classes are listed as follows.

- CPU Utilization Class: includes information from the kernel as percentages of User, System, Idle, and Wait (See Table 4–1)
- File System Class: includes space utilization of every file system (including NFS) as percentages (See Table 4–2)
- IPC Class: includes information on shared memory segments, semaphores, and message queues (See Table 4–3)
- Memory Class: includes information about free physical memory (KB) (See Table 4–4)
- Process Class: includes details of all processes running on the system (See Table 4–5)
- System Class: includes information about system calls, paging, physical and logical character reads and writes, interrupts, forks, execs, and vforks (See Table 4–6)
- Threads Class: includes details of all user-level threads for every multi-threaded process on the system (See Table 4–7)
- Virtual Memory Class: includes system calls, free memory, and total faults (See Table 4–8)

Summary of HP-UX Event Tests

The following tables list the HP-UX event tests by class. The full descriptions of the individual event tests follow the tables. The event tests are in alphabetical order.

Table 4–1 CPU Utilization Class Event Tests

Event Test	Description
Average CPU Load (1 Minute	The run queue or the load average is an average of the number of runnable processes waiting for the CPU during the last sixty seconds. This test checks the load average during the last minute for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If the load average is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Average CPU Load (5 Minute)	The run queue or the load average is an average of the number of runnable processes waiting for the CPU during the last five minutes. This test checks the load average during the last five minutes for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If the load average is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Average CPU Load (15 Minutes)	The run queue or the load average is an average of the number of runnable processes waiting for this CPU during the last 15 minutes. This test checks the load average during the last 15 minute for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If the load average is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Idle (%)	Idle (%) is the percentage of time that the CPU was idle and the system did not have an outstanding disk I/O request. This test checks the percentage of processor time in idle mode for the CPU(s) specified by the Host CPU parameter, such as CPU0, or * (for all CPUs on the system). If the Idle (%) value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Kernel (%)	Kernel (%) is the portion of time that the CPU is running in system mode. This test checks the kernel (%) for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If kernel (%) is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–1 CPU Utilization Class Event Tests (Cont.)

Event Test	Description
Sxbrk (%)	Sxbrk (%) is the portion of time that CPU is in sxbrk state. This test checks the sxbrk (%) for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If sxbrk (%) is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
User (%)	User (%) is the portion of processor time running in user mode. This test checks the percentage of processor time in user mode for the CPU(s) specified by the Host CPU parameter, such as CPU0, or * (for all CPUs on the system). If the User (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Wait (%)	Wait (%) is the percentage of time that the CPU was idle during which the system had an outstanding disk I/O request. This test checks the percentage of processor time in wait mode for the CPU(s) specified by the Host CPU parameter, such as CPU0, or * (for all CPUs on the system). If the Wait (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–2 File System Class Event Tests

Event Test	Description
Available (KB)	Available is the amount of space, in kilobytes, available for the creation of new files by users who do not have super user privileges. This test checks for available space on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the space available is less than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Used (KB)	Used is the amount of space (in kilobytes) allocated to existing files. This test checks for space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all file systems). If the space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Utilized (%)	Utilized is the percentage of space that is currently allocated to all files on the file system. This test checks for the percentage of space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the percentage of space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–3 IPC Class Event Tests

Event Test	Description
Number of Message Queues in Use	Message Queues in Use (#) is the number of message queues currently in use. This test checks the number of message queues currently in use. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of Semaphore Identifiers in Use	Semaphore IDs (#) is the number of semaphore identifiers currently in use. This test checks the number of semaphore identifiers currently in use. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of Shared Memory Segments in Use	Shared Memory Segments (#) is the number of shared memory segments currently in use. This test checks the number of shared memory segments currently in use. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of System Message Headers	System Message Headers (#) is the number of system message headers for all messages. This test checks the number of system message headers. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–4 Memory Class Event Test

Event Test	Description
Free Memory (KB)	Free Memory (KB) is the free physical memory in kilobytes. This test checks the free physical memory on the system. If the Free Memory (KB) is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–5 Process Class Event Tests

Event Test	Description
Number of Threads	Number of threads is the number of threads in this process. This test checks the number of threads in the process(es) specified by the process names parameter, such as dbsnmp or * (for all processes running on the system). If the number of threads is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Percent Memory Used	Percent Memory Used is the ratio of the resident set size of a process to the physical memory on the machine, expressed as a percentage. This test checks the percentage memory used by process(es) specified by the process names parameter, such as dbsnmp or * (for all processes running on the system). If the memory used by any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Resident Size (KB)	Resident Size is the resident set size of a process, in kilobytes. This test checks the resident size of the process(es) specified by the process names parameter, such as dbsnmp or * (for all processes running on the system). If the resident size of one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Virtual Size (KB)	Virtual Size is the total size of a process in virtual memory, in kilobytes. This test checks the total size of the process(es) specified by the process names parameter, such as dbsnmp or * (for all processes running on the system). If the total size of any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–6 System Class Event Tests

Event Test	Description
Block I/O Reads (#/s)	Block I/O Reads is the number of physical block reads per second. Block I/O Reads are generally performed by the kernel to manage the block buffer cache area. This test checks the block I/O read rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Block I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Block I/O Writes (#/s)	Block I/O Writes is the number of physical block writes per second. Block I/O Writes are generally performed by the kernel to manage the block buffer cache area. This test checks the block I/O write rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Block I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–6 System Class Event Tests (Cont.)

Event Test	Description
Calls to Syscall() (#/s)	Calls to syscall() is the number of calls (per second) to the system service routines that perform basic scheduling and synchronizing of activities on the computer.
	This test checks the system calls rate for CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Device Interrupts (#/s)	Device Interrupts is the number of device interruptions the processor is experiencing per second. These device interruptions can result from devices such as the mouse, network cards, and so on. This metric also measures the activity of those devices are in the overall system environment.
	This test checks the device interruptions rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Device Interrupts value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Fork System Calls (#/s)	Fork System Calls is the number of calls fork() per second.
	This test checks the calls to system call fork() rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Physical I/O Reads (#/s)	Physical I/O Reads is the number of raw I/O reads per second.
	This test checks the physical I/O read rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Physical I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Physical I/O Writes (#/s)	Physical I/O Writes is the number of raw I/O writes per second.
	This test checks the physical I/O write rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Physical I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–6 System Class Event Tests (Cont.)

Event Test	Description
Read System Calls (#/s)	Read System Calls is the number of system calls read() per second. This test checks the read() system calls rate for CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Write System Calls (#/s)	Write System Calls is the number of system calls write() per second. This test checks the write() system calls rate for CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–7 Threads Class Event Tests

Event Test	Description
Number of Block Input Operations	Block Inputs (#/s) is the number of block input operations per second. This test checks the number of block input operations per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of Block Output Operations	Block Outputs (#/s) is the number of block output operations per second. This test checks the number of block output operations per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of Characters Read/Written	Char Read/Written (#/s) is the number of characters read or written by a thread per second. This test checks the number of characters read or written per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of Messages Received	Messages Received (#/s) is the number of messages received per second. This test checks the number of messages received per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–7 Threads Class Event Tests (Cont.)

Event Test	Description
Number of Messages Sent	Messages Sent (#/s) is the number of messages sent out per second. This test checks the number of messages sent per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages sent is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of Page Faults Requiring Disk Access	Page Faults (#/s) is the number of page faults requiring disk access per second. This test checks the number of page faults per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of Page Reclaims	Page Reclaims (#/s) is the number of page reclaims by this thread per second. This test checks the number of page reclaims per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Number of System Calls	System Calls (#/s) is the number of system calls per second. This test checks the number of system calls per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–8 Virtual Memory Class Event Tests

Event Test	Description
Context Switches (#/s)	Context Switches/sec is the rate of switches from one thread to another. Thread switches can occur either inside a single process or across processes. A thread switch can happen when one thread requests information from another thread, or when a higher priority thread preempts another thread. This test checks the number of context switches per second. If the number of context switches is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Forks (#/s)	Forks (#/s) is the number of calls per second to system call fork(). This event test checks the number of calls per second to system call fork(). If the system calls is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–8 Virtual Memory Class Event Tests (Cont.)

Event Test	Description
Free Memory (Pages)	Free Memory is the size of the free list in system pages. This test checks the size of the free memory on the system. If the size is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Interrupts (#/s)	Interrupts is the number of device interruptions the processor is experiencing per second. Those device interruptions may be caused by system devices such as the mouse, network cards, etc. This metric also indicates how busy those devices are in the overall system environment. This test checks the system interruptions per second. If the system interruptions per second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Page Ins (#/s)	Page Ins is the number of page read ins (read from disk to resolve fault memory references) by the virtual memory manager per second. Along with the page out statistic, this represents the amount of real I/O initiated by the virtual memory manager. This test checks the number of page read ins per second. If the number of page read ins is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Page Outs (#/s)	Page Outs is the number of page write outs to disk per second. This test checks the number of page write outs per second. If the number of page write outs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pages Freed (#/s)	Pages Freed is one of the statistics for the virtual memory management subsystem. This statistic reports on pages placed on the free list by the page stealing daemon. A related statistic is Page Scans per Second. The Page Scans per Second statistic reports on pages per second scanned by the page stealing daemon.
Pages Swapped In (#/s)	Pages Swapped In are the total number of page ins from the disk during the interval. This includes pages paged in from paging space and from the file system. This test checks the number of page ins per second. If the number of page ins is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pages Swapped Out (#/s)	Pages Swapped Out is the total number of page outs from the disk during the interval. This includes pages paged out to paging space and to the file system. This test checks the number of page outs per second. If the number of page outs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 4–8 Virtual Memory Class Event Tests (Cont.)

Event Test	Description
System Calls (#/s)	Systems Calls is the number of calls, per second, to the system service routines that perform basic scheduling and synchronizing of activities on the computer. This test checks the system calls per second. If the system calls per second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Total Faults (#/s)	Total Faults per Second measures the number of Page Faults in the processor per second. A page fault occurs when a virtual memory page is referenced by a process and that page is not in the current Working Set of the main memory. This test checks the number of page faults per second. If the number of page faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Descriptions of HP-UX Event Tests

The HP-UX Event Tests are listed in alphabetical order.

Available (KB)

Description

Available is the amount of space, in kilobytes, available for the creation of new files by users who do not have super user privileges.

This test checks for available space on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the space available is less than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from statvfs.

Parameters

- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert, in kilobytes.

- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The available space in kilobytes on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Average CPU Load (1 Minute)

Description
The run queue or the load average is an average of the number of runnable processes waiting for the CPU during the last sixty seconds.

This test checks the load average during the last minute for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If the load average is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getdynamic (struct pst_dynamic).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Average load for the CPU during the last 1 minute.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Average CPU Load (5 Minutes)

Description
The run queue or the load average is an average of the number of runnable processes waiting for the CPU during the last five minutes.

This test checks the load average during the last five minutes for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If the load average is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getdynamic (struct pst_dynamic).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Average load for the CPU during the last 5 minutes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Average CPU Load (15 Minutes)

Description
The run queue or the load average is an average of the number of runnable processes waiting for this CPU during the last 15 minutes.

This test checks the load average during the last 15 minute for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If the load average is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getdynamic (struct pst_dynamic).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Average load for the CPU during the last 15 minutes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Block I/O Reads (#/s)

Description

Block I/O Reads is the number of physical block reads per second. Block I/O Reads are generally performed by the kernel to manage the block buffer cache area.

This test checks the block I/O read rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Block I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters

- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of physical block reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Block I/O Writes (#/s)

Description

Block I/O Writes is the number of physical block writes per second. Block I/O Writes are generally performed by the kernel to manage the block buffer cache area.

This test checks the block I/O write rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Block I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters

- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of physical block writes per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Calls to Syscall() (#/s)

Description

Calls to syscall() is the number of calls (per second) to the system service routines that perform basic scheduling and synchronizing of activities on the computer.

This test checks the system calls rate for CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of system calls per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Context Switches (#/s)

Description
Context Switches / sec is the rate of switches from one thread to another. Thread switches can occur either inside a single process or across processes. A thread switch can happen when one thread requests information from another thread, or when a higher priority thread preempts another thread.

This test checks the number of context switches per second. If the number of context switches is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters

- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of context switches per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Device Interrupts (#/s)

Description

Device Interrupts is the number of device interruptions the processor is experiencing per second. These device interruptions can result from devices such as the mouse, network cards, and so on. This metric also measures the activity of those devices are in the overall system environment.

This test checks the device interruptions rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Device Interrupts value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters

- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager

or Capacity Planner and connect to the target node, then click on the class "System".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of device interruptions per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Fork System Calls (#/s)

Description
Fork System Calls is the number of calls fork() per second.

This test checks the calls to system call fork() rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of calls of fork() per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Forks (#/s)

Description
Forks (#/s) is the number of calls per second to system call fork().

This event test checks the number of calls per second to system call fork(). If the system calls is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters
- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of calls of fork() per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Free Memory (KB)

Description
Free Memory (KB) is the free physical memory in kilobytes.

This test checks the free physical memory on the system. If the Free Memory (KB) is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getvminfo (struct pst_vminfo).

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The free physical memory in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Free Memory (Pages)

Description
Free Memory is the size of the free list in system pages.

This test checks the size of the free memory on the system. If the size is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters
- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert, in system pages.
- Critical Threshold: Threshold for critical alert, in system pages.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The size of the free memory in system pages.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Idle (%)

Description
Idle (%) is the percentage of time that the CPU was idle and the system did not have an outstanding disk I/O request.

This test checks the percentage of processor time in idle mode for the CPU(s) specified by the Host CPU parameter, such as CPU0, or * (for all CPUs on the system). If the Idle (%) value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getdynamic (struct pst_dynamic).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager

or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".

- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of time that the CPU was idle and no outstanding disk I/O request in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Interrupts (#/s)

Description
Interrupts is the number of device interruptions the processor is experiencing per second. Those device interruptions may be caused by system devices such as the mouse, network cards, etc. This metric also indicates how busy those devices are in the overall system environment.

This test checks the system interruptions per second. If the system interruptions per second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters
- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of device interruptions per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Kernel (%)

Description
Kernel (%) is the portion of time that the CPU is running in system mode.

This test checks the kernel (%) for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If kernel (%) is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getdynamic (struct pst_dynamic).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of time that the CPU is running in the system mode in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of Block Input Operations

Description
Block Inputs (#/s) is the number of block input operations per second.

This test checks the number of block input operations per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getlwp (struct lwp_status).

Parameters
- Thread ID(s): Filter for threads, * for all threads running on the system. **Note:** To access the list of available thread IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Threads".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of block input operations per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of Block Output Operations

Description
Block Outputs (#/s) is the number of block output operations per second.

This test checks the number of block output operations per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getlwp (struct lwp_status).

Parameters
- Thread ID(s): Filter for threads, * for all threads running on the system. **Note:** To access the list of available thread IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Threads".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of block output operations per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of Characters Read/Written

Description

Char Read / Written (# / s) is the number of characters read or written by a thread per second.

This test checks the number of characters read or written per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from system call pstat_getlwp (struct lwp_status).

Parameters

- Thread ID(s): Filter for threads, * for all threads running on the system. **Note:** To access the list of available thread IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Threads".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of characters read or written per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Number of Message Queues in Use

Description

Message Queues in Use (#) is the number of message queues currently in use.

This test checks the number of message queues currently in use. If the number is greater than or equal to the threshold values specified by the threshold arguments,

and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getipc (struct pst_ipcinfo).

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of message queues in use.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of Messages Received

Description
Messages Received (#/s) is the number of messages received per second.

This test checks the number of messages received per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getlwp (struct lwp_status).

Parameters
- Thread ID(s): Filter for threads, * for all threads running on the system. **Note:** To access the list of available thread IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Threads".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of messages received per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of Messages Sent

Description
Messages Sent (#/s) is the number of messages sent out per second.

This test checks the number of messages sent per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages sent is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getlwp (struct lwp_status).

Parameters
- Thread ID(s): Filter for threads, * for all threads running on the system. **Note:** To access the list of available thread IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Threads".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of messages sent per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of Page Faults Requiring Disk Access

Description
Page Faults (#/s) is the number of page faults requiring disk access per second.

This test checks the number of page faults per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getlwp (struct lwp_status).

Parameters
- Thread ID(s): Filter for threads, * for all threads running on the system. **Note:** To access the list of available thread IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Threads".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page faults per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of Page Reclaims

Description

Page Reclaims (#/s) is the number of page reclaims by this thread per second.

This test checks the number of page reclaims per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from system call pstat_getlwp (struct lwp_status).

Parameters

- Thread ID(s): Filter for threads, * for all threads running on the system. **Note:** To access the list of available thread IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Threads".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of page reclaims per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Number of Semaphore Identifiers in Use

Description

Semaphore IDs (#) is the number of semaphore identifiers currently in use.

This test checks the number of semaphore identifiers currently in use. If the number is greater than or equal to the threshold values specified by the threshold

arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getipc (struct pst_ipcinfo).

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The semaphore identifiers currently in use.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of Shared Memory Segments in Use

Description
Shared Memory Segments (#) is the number of shared memory segments currently in use.

This test checks the number of shared memory segments currently in use. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getipc (struct pst_ipcinfo).

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of shared memory segments currently in use.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of System Calls

Description
System Calls (#/s) is the number of system calls per second.

This test checks the number of system calls per second for the thread(s) specified by the Thread ID(s) parameter. (* for all threads running on the system). If the number of messages received is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getlwp (struct lwp_status).

Parameters
- Thread ID(s): Filter for threads, * for all threads running on the system. **Note:** To access the list of available thread IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Threads".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of system calls per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Number of System Message Headers

Description

System Message Headers (#) is the number of system message headers for all messages.

This test checks the number of system message headers. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from system call pstat_getipc (struct pst_ipcinfo).

Parameters

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of system message headers

Recommended Frequency

5 minutes

User Action

Specific to your site.

Number of Threads

Description

Number of threads is the number of threads in this process.

This test checks the number of threads in the process(es) specified by the process names parameter, such as dbsnmp or * (for all processes running on the system). If the number of threads is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getproc (struct pst_status).

Parameters
- Process(es): Filter for processes, such as dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.
- Thread: The number of threads in this process.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Page Ins (#/s)

Description
Page Ins is the number of page read ins (read from disk to resolve fault memory references) by the virtual memory manager per second. Along with the page out statistic, this represents the amount of real I/O initiated by the virtual memory manager.

This test checks the number of page read ins per second. If the number of page read ins is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters

- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of page read ins per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Page Outs (#/s)

Description

Page Outs is the number of page write outs to disk per second.

This test checks the number of page write outs per second. If the number of page write outs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters

- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page write outs per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pages Freed (#/s)

Description
Pages Freed is one of the statistics for the virtual memory management subsystem. This statistic reports on pages placed on the free list by the page stealing daemon. A related statistic is Page Scans per Second. The Page Scans per Second statistic reports on pages per second scanned by the page stealing daemon.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters
- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of pages freed per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pages Swapped In (#/s)

Description

Pages Swapped In are the total number of page ins from the disk during the interval. This includes pages paged in from paging space and from the file system.

This test checks the number of page ins per second. If the number of page ins is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters

- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of page ins per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Pages Swapped Out (#/s)

Description

Pages Swapped Out is the total number of page outs from the disk during the interval. This includes pages paged out to paging space and to the file system.

This test checks the number of page outs per second. If the number of page outs is greater than or equal to the threshold values specified by the threshold arguments,

and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters
- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page outs per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Percent Memory Used

Description
Percent Memory Used is the ratio of the resident set size of a process to the physical memory on the machine, expressed as a percentage.

This test checks the percentage memory used by process(es) specified by the process names parameter, such as dbsnmp or * (for all processes running on the system). If the memory used by any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getproc (struct pst_status).

Parameters

- Process(es): Filter for processes, such as dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Process name with process ID: To identify the exact process.
- Percent Memory Used: The ratio of a process's resident set size to the physical memory on the machine.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Physical I/O Reads (#/s)

Description

Physical I/O Reads is the number of raw I/O reads per second.

This test checks the physical I/O read rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Physical I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters

- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of physical I/O reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Physical I/O Writes (#/s)

Description
Physical I/O Writes is the number of raw I/O writes per second.

This test checks the physical I/O write rate for the CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the Physical I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of physical I/O writes per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Read System Calls (#/s)

Description
Read System Calls is the number of system calls read() per second.

This test checks the read() system calls rate for CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of read system calls per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Resident Size (KB)

Description
Resident Size is the resident set size of a process, in kilobytes.

This test checks the resident size of the process(es) specified by the process names parameter, such as dbsnmp or * (for all processes running on the system). If the resident size of one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getproc (struct pst_status).

Parameters
- Process(es): Filter for processes, such as dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.
- Resident Size: The resident set size of a process, in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Sxbrk (%)

Description
Sxbrk (%) is the portion of time that CPU is in sxbrk state.

This test checks the sxbrk (%) for the CPU(s) specified by the Host CPU(s) parameter, such as CPU0, or * (for all CPUs on the system). If sxbrk (%) is greater

than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getdynamic (struct pst_dynamic).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of time that the CPU was in sxbrk state in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Calls (#/s)

Description
Systems Calls is the number of calls, per second, to the system service routines that perform basic scheduling and synchronizing of activities on the computer.

This test checks the system calls per second. If the system calls per second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters
- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of system calls per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Total Faults (#/s)

Description
Total Faults per Second measures the number of Page Faults in the processor per second. A page fault occurs when a virtual memory page is referenced by a process and that page is not in the current Working Set of the main memory.

This test checks the number of page faults per second. If the number of page faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getvminfo (struct pst_vminfo).

Parameters
- Virtual Memory Statistics: Instance name, default is "HPUX". **Note:** To access the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Virtual Memory Statistics".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page faults per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Used (KB)

Description
Used is the amount of space (in kilobytes) allocated to existing files.

This test checks for space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all file systems). If the space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from statvfs.

Parameters
- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The used space in kilobytes on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

User (%)

Description
User (%) is the portion of processor time running in user mode.

This test checks the percentage of processor time in user mode for the CPU(s) specified by the Host CPU parameter, such as CPU0, or * (for all CPUs on the system). If the User (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from pstat_getdynamic (struct pst_dynamic).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Percentage of time that the CPU is running in the user mode in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Utilized (%)

Description
Utilized is the percentage of space that is currently allocated to all files on the file system.

This test checks for the percentage of space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the percentage of space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from statvfs.

Parameters
- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of space used on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Virtual Size

Description
Virtual Size is the total size of a process in virtual memory, in kilobytes.

This test checks the total size of the process(es) specified by the process names parameter, such as dbsnmp or * (for all processes running on the system). If the total size of any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getproc (struct pst_status).

Parameters
- Process(es): Filter for processes, such as dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.
- Virtual Size: The total size of a process in virtual memory, in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Wait (%)

Description
Wait (%) is the percentage of time that the CPU was idle during which the system had an outstanding disk I/O request.

This test checks the percentage of processor time in wait mode for the CPU(s) specified by the Host CPU parameter, such as CPU0, or * (for all CPUs on the system). If the Wait (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from pstat_getdynamic (struct pst_dynamic).

Parameters

- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

Percentage of time that the CPU was idle and wait for disk I/O in the last interval.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Write System Calls (#/s)

Description

Write System Calls is the number of system calls write() per second.

This test checks the write() system calls rate for CPU(s) specified by the Host CPU parameter, such as CPU0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold

arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from system call pstat_getprocessor (struct pst_processor).

Parameters
- System Host CPU(s): Filter for CPUs, such as CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of write system calls per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

5

IBM AIX Event Tests

The Oracle Enterprise Manager Advanced Event Tests for IBM AIX are divided into a series of classes or groupings that enable you to find the event test you want to register.

The class names and the events that you can register within the classes are listed as follows:

- CPU Utilization Class: includes the percentage of time the CPU was idle, in a wait state, in system mode, and in user mode (See Table 5–1)
- File System Class: includes available space and used space (See Table 5–2)
- I/O Class: includes read and write operations (See Table 5–3)
- Memory/Swap Class: includes free memory, available swap, and swap queue (See Table 5–4)
- Network Class: includes packet statistics, incoming and outgoing errors, and collisions on the network interface (See Table 5–5)
- Process Class: includes process ID, parent process ID, priority of the process, and size of the process (See Table 5–6)
- System Class: includes operations for page ins, page outs, pages paged in, and pages paged out (See Table 5–7)

Summary of IBM AIX Event Tests

The following tables list the IBM AIX event tests by class. The full descriptions of the individual event tests follow the tables. The event tests are in alphabetical order.

Table 5–1 CPU Utilization Event Tests

Event Test	Description
Idle (%)	Idle (%) is the percentage of time that the CPU was idle and the system did not have an outstanding disk I/O request. This test checks the percentage of processor time in idle mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Idle (%) value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Sys (%)	Sys (%) is the percentage of time that the CPU is running in system mode (kernel). This test checks the percentage of processor time in system mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Sys (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
User (%)	User (%) is the portion of processor time running in user mode. This test checks the percentage of processor time in user mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the User (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Wait (%)	Wait (%) is the percentage of time that the CPU was idle during which the system had an outstanding disk I/O request. This test checks the percentage of processor time in wait mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Wait (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–2 File System Class Event Tests

Event Test	Description
Available (KB)	Available is the amount of space, in kilobytes, available for the creation of new files by users who do not have superuser privileges. This test checks for available space on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the space available is less than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–2 File System Class Event Tests (Cont.)

Event Test	Description
Used (KB)	Used is the amount of space (in kilobytes) allocated to existing files. This test checks for space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all file systems). If the space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Utilized (%)	Utilized is the percentage of space that is currently allocated to all files on the file system. This test checks for the percentage of space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the percentage of space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–3 I/O Class Event Tests

Event Test	Description
Reads (#/s)	Reads is the number of reads per second. This test checks the read rate. If the read rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Writes (#/s)	Writes is the number of writes per second. This test checks the write rate. If the write rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–4 Memory/Swap Class Event Tests

Event Test	Description
Available Swap (KB)	Available Swap is the amount of swap space currently available in kilobytes. This test checks the size of currently available swap space on the system. If the size in kilobytes is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Free Memory (KB)	Free Memory is the size of the free list in kilobytes. This test checks the size of the free memory in kilobytes on the system. If the size is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–4 Memory/Swap Class Event Tests (Cont.)

Event Test	Description
Run Queue	Run Queue is the average number of processes in memory and subject to be run in the last interval. This test checks the run queue. If the run queue is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Swap Queue	Swap Queue is the average number of swapped processes in the last interval. This test checks the average number of swapped processes. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Waiting	Waiting is the average number of jobs waiting for I/O in the last interval. This test checks the average number of jobs waiting for I/O. If the waiting queue is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–5 Network Class Event Tests

Event Test	Description
Collisions (#/s)	Collisions is the number of collisions per second. This test checks the rate of collisions on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Incoming Errors (#/s)	Incoming Errors is the number of input errors, per second, encountered on the device for unsuccessful reception due to hardware/network errors. This test checks the rate of input errors on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Incoming Packets (#/s)	Incoming Packets is the number of packets, per second, that have been received successfully by the device. This test checks the rate at which packets are received on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–5 Network Class Event Tests (Cont.)

Event Test	Description
Outgoing Errors (#/s)	Outgoing Errors is the number of output errors per second. This test checks the rate of output errors on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Outgoing Packets (#/s)	Outgoing Packets is the number of packets, per second, that have been sent out by the device. This test checks the rate at which packets are sent on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–6 Process Class Event Tests

Event Test	Description
System Time	System Time (%) is the percentage of system level CPU time that a process used. This test checks the percentage of system time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the System Time (%) value used by any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
User Time	User Time (%) is the percentage of user level CPU time that a process used. This test checks the percentage of user time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the User Time (%) value used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Virtual Size	Size is the total size of a process in virtual memory, in kilobytes. This test checks the total size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the total size of any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 5–7 System Class Event Tests

Event Test	Description
Page Ins (#/s)	Page Ins is the number of page read ins per second (read from disk to resolve fault memory references) by the virtual memory manager. Along with Page Outs, this statistic represents the amount of real I/O initiated by the virtual memory manager. This test checks the number of page read ins for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of page read ins is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Page Outs (#/s)	Page Outs is the number of page write outs to disk per second. This test checks the number of page write outs for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of page write outs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pages Paged In (#/s)	Pages Paged In is the number of pages paged in (read from disk to resolve fault memory references) per second. This test checks the number of pages paged in for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of pages paged in is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pages Paged Out (#/s)	Pages Paged Out is the number of pages written out (per second) by the virtual memory manager. Along with Pages Paged In, this statistic represents the amount of real I/O initiated by the virtual memory manager. This test checks the number of pages paged out for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of pages paged out is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Call Forks (#/s)	System Call Forks is the number of calls fork() per second. This test checks the calls to system call fork() rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Descriptions of IBM AIX Event Tests

The IBM AIX Event Tests are listed in alphabetical order.

Available (KB)

Description

Available is the amount of space, in kilobytes, available for the creation of new files by users who do not have superuser privileges.

This test checks for available space on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the space available is less than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from statvfs.

Parameters

- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The available space in kilobytes on the file system.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Available Swap (KB)

Description

Available Swap is the amount of swap space currently available in kilobytes.

This test checks the size of currently available swap space on the system. If the size in kilobytes is less than or equal to the threshold values specified by the threshold

arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct vmk psfreeblks).

Parameters

- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The size of currently available swap space in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Collisions (#/s)

Description
Collisions is the number of collisions per second.

This test checks the rate of collisions on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct ifnet_s colls).

Parameters

- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available

network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.

- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The rate of collisions on the network interface.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Free Memory (KB)

Description
Free Memory is the size of the free list in kilobytes.

This test checks the size of the free memory in kilobytes on the system. If the size is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct vmk numfrb).

Parameters
- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The size of the free memory in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Idle (%)

Description
Idle (%) is the percentage of time that the CPU was idle and the system did not have an outstanding disk I/O request.

This test checks the percentage of processor time in idle mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Idle (%) value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct sysinfo cpu).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of time that the CPU was idle and no outstanding disk I/O request in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Incoming Errors (#/s)

Description
Incoming Errors is the number of input errors, per second, encountered on the device for unsuccessful reception due to hardware/network errors.

This test checks the rate of input errors on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct ifnet_s ierrs).

Parameters
- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The rate of input errors on the network interface.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Incoming Packets (#/s)

Description
Incoming Packets is the number of packets, per second, that have been received successfully by the device.

This test checks the rate at which packets are received on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct ifnet_s ipkts).

Parameters
- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The rate at which packets are received on the network interface.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Outgoing Errors (#/s)

Description

Outgoing Errors is the number of output errors per second.

This test checks the rate of output errors on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from the system call for kernel statistics (struct ifnet_s oerrs).

Parameters

- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The rate of output errors on the network interface.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Outgoing Packets (#/s)

Description

Outgoing Packets is the number of packets, per second, that have been sent out by the device.

This test checks the rate at which packets are sent on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from the system call for kernel statistics (struct ifnet_s opkts).

Parameters

- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The rate at which packets are sent on the network interface.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Page Ins (#/s)

Description

Page Ins is the number of page read ins per second (read from disk to resolve fault memory references) by the virtual memory manager. Along with Page Outs, this statistic represents the amount of real I/O initiated by the virtual memory manager.

This test checks the number of page read ins for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of page read ins is greater than or equal to the threshold values specified by the

threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct vmi pageins).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page read ins per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Page Outs (#/s)

Description
Page Outs is the number of page write outs to disk per second.

This test checks the number of page write outs for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of page write outs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct vmi pageouts).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of page write outs per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Pages Paged In (#/s)

Description

Pages Paged In is the number of pages paged in (read from disk to resolve fault memory references) per second.

This test checks the number of pages paged in for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of pages paged in is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from the system call for kernel statistics (struct vmi pgspgin).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of pages paged in per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pages Paged Out (#/s)

Description
Pages Paged Out is the number of pages written out (per second) by the virtual memory manager. Along with Pages Paged In, this statistic represents the amount of real I/O initiated by the virtual memory manager.

This test checks the number of pages paged out for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of pages paged out is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct vmi pgspgout).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of pages paged out per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Reads (#/s)

Description
Reads is the number of reads per second.

This test checks the read rate. If the read rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct dkstat dk_rblks).

Parameters
- Disk Device Name(s): Filter for disk names, such as sd0 or * for all disks on the system. **Note:** To access the list of available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "I/O".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Run Queue

Description
Run Queue is the average number of processes in memory and subject to be run in the last interval.

This test checks the run queue. If the run queue is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct sysinfo runque).

Parameters
- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The run queue in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Swap Queue

Description
Swap Queue is the average number of swapped processes in the last interval.

This test checks the average number of swapped processes. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct sysinfo swpque).

Parameters
- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The average swap queue length in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Sys (%)

Description
Sys (%) is the percentage of time that the CPU is running in system mode (kernel).

This test checks the percentage of processor time in system mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Sys (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct sysinfo cpu).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

Percentage of time that the CPU is running in the system mode in the last interval.

Recommended Frequency

5 minutes

User Action

Specific to your site.

System Call Forks (#/s)

Description

System Call Forks is the number of calls fork() per second.

This test checks the calls to system call fork() rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from the system call for kernel statistics (struct sysinfo sysfork).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance

Manager or Capacity Planner and connect to the target node, then click on the class "System".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of fork system calls per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Time

Description
System Time (%) is the percentage of system level CPU time that a process used.

This test checks the percentage of system time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the System Time (%) value used by any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from getproc.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Process name with process ID: To identify the exact process.
- System Time: The percentage of system level CPU time that a process used.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Used (KB)

Description

Used is the amount of space (in kilobytes) allocated to existing files.

This test checks for space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all file systems). If the space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Data obtained from statvfs.

Parameters

- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The used space in kilobytes on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

User (%)

Description
User (%) is the portion of processor time running in user mode.

This test checks the percentage of processor time in user mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the User (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct sysinfo cpu).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Percentage of time that the CPU is running in the user mode in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

User Time

Description
User Time (%) is the percentage of user level CPU time that a process used.

This test checks the percentage of user time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the User Time (%) value used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from getproc.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.
- User Time: The percentage of user level CPU time that a process used.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Utilized (%)

Description
Utilized is the percentage of space that is currently allocated to all files on the file system.

This test checks for the percentage of space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the percentage of space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from statvfs.

Parameters
- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of space used on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Virtual Size

Description
Size is the total size of a process in virtual memory, in kilobytes.

This test checks the total size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the total size of any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in

the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from getproc.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.
- Size: the total size of a process in virtual memory, in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Wait (%)

Description
Wait (%) is the percentage of time that the CPU was idle during which the system had an outstanding disk I/O request.

This test checks the percentage of processor time in wait mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Wait (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct sysinfo cpu).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

Percentage of time that the CPU was idle and wait for disk I/O in the last interval.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Waiting

Description

Waiting is the average number of jobs waiting for I/O in the last interval.

This test checks the average number of jobs waiting for I/O. If the waiting queue is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

Not available.

Parameters

- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The average waiting queue length in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Writes (#/s)

Description
Writes is the number of writes per second.

This test checks the write rate. If the write rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
Data obtained from the system call for kernel statistics (struct dkstat dk_wblks).

Parameters
- Disk Device Name(s): Filter for disk names, such as sd0 or * for all disks on the system. **Note:** To access the list of available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "I/O".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of writes per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

6

Solaris Event Tests

The Oracle Enterprise Manager Advanced Event Tests for Solaris are divided into a series of classes or groupings that will enable you to find the event test you are interested in registering.

The class names and some of the events that you can register within the classes are listed as follows.

- CPU Utilization Class: includes the percentage of time the CPU was idle, in a wait state, in system mode, and in user mode (See Table 6–1)
- File System Class: includes available space, space allocated to existing files, and percentage of space allocated to existing files (See Table 6–2)
- I/O Class: includes read and write throughput, number of read and write operations, and average service time (See Table 6–3)
- Memory/Swap Class: includes free memory, swap space, average number of processes in memory, and average number of jobs waiting for I/O (See Table 6–4)
- Network Class: includes packet statistics, ingoing and outgoing errors, and collisions on the network interface (See Table 6–5)
- Process Class: includes virtual size of the process, resident set size of a process, and number of lwps (lightweight processes) (See Table 6–6)
- System Class: includes file read/write operations, system call operations, and system page operations (See Table 6–7)

Summary of Solaris Event Tests

The following tables list the Solaris event tests by class. The full descriptions of the individual event tests follow the tables. The event tests are in alphabetical order.

Table 6–1 CPU Utilization Event Tests

Event Test	Description
CPU Utilization (%)	CPU Utilization (%) is the percentage of time that the CPU was busy. For a multiple processors system, this is an overall average across all processors.
Idle (%)	Idle (%) is the percentage of time that the CPU was idle and the system did not have an outstanding disk I/O request. This test checks the percentage of processor time in idle mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Idle (%) value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Sys (%)	Sys (%) is the percentage of time that the CPU is running in system mode (kernel). This test checks the percentage of processor time in system mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Sys (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
User (%)	User (%) is the portion of processor time running in user mode. This test checks the percentage of processor time in user mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the User (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Wait (%)	Wait (%) is the percentage of time that the CPU was idle during which the system had an outstanding disk I/O request. This test checks the percentage of processor time in wait mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Wait (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–2 File System Class Event Tests

Event Test	Description
Available (KB)	Available is the amount of space, in kilobytes, available for the creation of new files by users who do not have superuser privileges. This test checks for available space on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the space available is less than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–2 File System Class Event Tests (Cont.)

Event Test	Description
Used (KB)	Used is the amount of space (in kilobytes) allocated to existing files. This test checks for space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all file systems). If the space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Utilized (%)	Utilized is the percentage of space that is currently allocated to all files on the file system. This test checks for the percentage of space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the percentage of space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–3 I/O Class Event Tests

Event Test	Description
Average Response Time (ms)	Average Response Time (ms) calculates the average time (in milliseconds) of a disk operation.
Average Service Time (ms)	Average Service Time is the average service time, in milliseconds. This test checks the average service time. If the average service time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Read Throughput	Read Throughput is the number of kilobytes read per second. This test checks the read throughput. If the read throughput is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Reads (#/s)	Reads is the number of reads per second. This test checks the read rate. If the read rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Write Throughput	Write Throughput is the number of kilobytes written per second. This test checks the write throughput. If the write throughput is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Writes (#/s)	Writes is the number of writes per second. This test checks the write rate. If the write rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–4 MemorySwap Class Event Tests

Event Test	Description
Available Swap (KB)	Available Swap is the amount of swap space currently available in kilobytes. This test checks the size of currently available swap space on the system. If the size in kilobytes is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Free Memory (%)	Available Memory (%) is the percentage of the free physical memory of the total physical memory.
Free Memory (KB)	Free Memory is the size of the free list in kilobytes. This test checks the size of the free memory in kilobytes on the system. If the size is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Run Queue	Run Queue is the average number of processes in memory and subject to be run in the last interval. This test checks the run queue. If the run queue is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Swap Queue	Swap Queue is the average number of swapped processes in the last interval. This test checks the average number of swapped processes. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Waiting	Waiting is the average number of jobs waiting for I/O in the last interval. This test checks the average number of jobs waiting for I/O. If the waiting queue is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–5 Network Class Event Tests

Event Test	Description
Collisions (#/s)	Collisions is the number of collisions per second. This test checks the rate of collisions on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Incoming Errors (#/s)	Incoming Errors is the number of input errors, per second, encountered on the device for unsuccessful reception due to hardware/network errors. This test checks the rate of input errors on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Incoming Packets (#/s)	Incoming Packets is the number of packets, per second, that have been received successfully by the device. This test checks the rate at which packets are received on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Outgoing Errors (#/s)	Outgoing Errors is the number of output errors per second. This test checks the rate of output errors on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Outgoing Packets (#/s)	Outgoing Packets is the number of packets, per second, that have been sent out by the device. This test checks the rate at which packets are sent on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–6 Process Class Event Tests

Event Test	Description
Percent Memory Used	Percent Memory Used is the ratio of the resident set size of a process to the physical memory on the machine, expressed as a percentage. This test checks the percent memory used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the percent memory used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Resident Size	Resident Size is the resident set size of a process, in kilobytes. This test checks the resident size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the resident size of one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Time	System Time (%) is the percentage of system level CPU time that a process used. This test checks the percentage of system time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the System Time (%) value used by any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Threads	Threads is the number of lwps (lightweight processes) in a process. This test checks the number of threads in the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the number of threads is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
User Time	User Time (%) is the percentage of user level CPU time that a process used. This test checks the percentage of user time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the User Time (%) value used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Virtual Size	Virtual Size is the total size of a process in virtual memory, in kilobytes. This test checks the total size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the total size of any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–7 System Class Event Tests

Event Test	Description
AS Faults (#/s)	AS (address space) Faults is the number of minor page faults via as_fault() per second.
	This test checks the number of AS faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of AS faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Block IO Reads (#/s)	Block I/O Reads is the number of physical block reads per second. Block I/O Reads are generally performed by the kernel to manage the block buffer cache area.
	This test checks the block I/O read rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Block I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Block IO Writes (#/s)	Block I/O Writes is the number of physical block writes per second. Block I/O Writes are generally performed by the kernel to manage the block buffer cache area.
	This test checks the block I/O write rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Block I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
COW Faults (#/s)	COW (copy-on-write) Faults is the number of copy-on-write faults per second. If one of the processes sharing the page attempts to write to the page, a copy-on-write page fault occurs. Another page is taken from the free list and the original page is copied.
	This test checks the number of COW faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of COW faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
HAT Faults (#/s)	HAT (hardware address translation) Faults is the minor page faults by way of hat_fault() per second.
	This test checks the number of HAT faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of HAT faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Logical IO Reads (#/s)	Logical I/O Reads is the number of logical block reads per second. When a logical read from a block device is performed, a logical transfer size of less than a full block size may be requested.
	This test checks the logical I/O read rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Logical I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–7 System Class Event Tests (Cont.)

Event Test	Description
Logical IO Writes (#/s)	Logical I/O Writes is the number of logical block writes per second. When a logical write to a block device is performed, a logical transfer size of less than a full block size may be requested. This test checks the logical I/O write rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Logical I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Maj Faults (#/s)	Maj (major) Faults is the number of major page faults per second. This test checks the number of major faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of major faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Physical IO Reads (#/s)	Physical I/O Reads is the number of raw I/O reads per second. This test checks the physical I/O read rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Physical I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Physical IO Writes (#/s)	Physical I/O Writes is the number of raw I/O writes per second. This test checks the physical I/O write rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Physical I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Prot Faults (#/s)	Prot (protection) Faults is the number of protection faults per second. Protection faults occur when a program attempts to access memory it should not access, receives a segmentation violation signal, and dumps a core file. This test checks the number of protection faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of protection faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Call Forks (#/s)	System Call Forks is the number of calls fork() per second. This test checks the calls to system call fork() rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–7 System Class Event Tests (Cont.)

Event Test	Description
System Call VForks (#/s)	System Call VFork is the number of calls vfork() per second. This test checks the calls to system call vfork() rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Calls (#/s)	Systems Calls is the number of calls (per second) to the system service routines that perform basic scheduling and synchronizing of activities on the computer. This test checks the system calls rate for CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Interrupts (#/s)	System Interrupts is the number of device interruptions the processor is experiencing per second. These device interruptions can result from system devices such as the mouse, network cards, and so on. This metric also measures the activity of those devices are in the overall system environment. This test checks the system interruptions rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Interruptions value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Page Ins (#/s)	System Page Ins is the number of page read ins per second (read from disk to resolve fault memory references) by the virtual memory manager. Along with Page Out, this statistic represents the amount of real I/O initiated by the virtual memory manager. This test checks the number of page read ins for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of page read ins is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Page Outs (#/s)	System Page Outs is the number of page write outs to disk per second. This test checks the number of page write outs for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of page write outs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 6–7 System Class Event Tests (Cont.)

Event Test	Description
System Pages Paged In (#/s)	System Pages Paged In is the number of pages paged in (read from disk to resolve fault memory references) per second. This test checks the number of pages paged in for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of pages paged in is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Pages Paged Out (#/s)	System Page Outs is the number of pages written out (per second) by the virtual memory manager. Along with Page Out, this statistic represents the amount of real I/O initiated by the virtual memory manager. This test checks the number of pages paged out for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of pages paged out is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Descriptions of Solaris Event Tests

The Solaris event tests are listed in alphabetical order.

AS Faults (#/s)

Description

AS (address space) Faults is the number of minor page faults via as_fault() per second.

This test checks the number of AS faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of AS faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of address space (AS) faults per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Available (KB)

Description
Available is the amount of space, in kilobytes, available for the creation of new files by users who do not have superuser privileges.

This test checks for available space on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the space available is less than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved through system call statvfs().

Parameters
- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The available space in kilobytes on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Available Memory (%)

Description
Available Memory (%) is the percentage of the free physical memory of the total physical memory.

Data Source
(Available Memory) / (Total Physical Memory) * 100%

Parameters
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Available physical memory in percentage.

Recommended Frequency
5 minutes

Available Swap (KB)

Description
Available Swap is the amount of swap space currently available in kilobytes.

This test checks the size of currently available swap space on the system. If the size in kilobytes is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class vm vminfo).

Parameters
- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The size of currently available swap space in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Average Response Time (ms)

Description
Average Response Time (ms) calculates the average time (in milliseconds) of a disk operation.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The average response time in milliseconds.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Average Service Time (ms)

Description
Average Service Time is the average service time, in milliseconds.

This test checks the average service time. If the average service time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class disk).

Parameters
- Disk Device Name(s): Filter for disk names, such as sd0 or * for all disks on the system. **Note:** To access the list of available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "I/O".
- Warning Threshold: Threshold for warning alert, in milliseconds.
- Critical Threshold: Threshold for critical alert, in milliseconds.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The average service time in milliseconds.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Block IO Reads (#/s)

Description

Block I/O Reads is the number of physical block reads per second. Block I/O Reads are generally performed by the kernel to manage the block buffer cache area.

This test checks the block I/O read rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Block I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of physical block reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Block IO Writes (#/s)

Description

Block I/O Writes is the number of physical block writes per second. Block I/O Writes are generally performed by the kernel to manage the block buffer cache area.

This test checks the block I/O write rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Block I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of physical block writes per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Collisions (#/s)

Description
Collisions is the number of collisions per second.

This test checks the rate of collisions on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class net).

Parameters
- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner to connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The rate of collisions on the network interface.

Recommended Frequency
5 minutes

User Action
Specific to your site.

COW Faults (#/s)

Description
COW (copy-on-write) Faults is the number of copy-on-write faults per second. If one of the processes sharing the page attempts to write to the page, a copy-on-write page fault occurs. Another page is taken from the free list and the original page is copied.

This test checks the number of COW faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of COW faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of copy-on-write (COW) faults per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

CPU Utilization (%)

Description
CPU Utilization (%) is the percentage of time that the CPU was busy.For a multiple processors system, this is an overall average across all processors.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

CPU Utilization (%) = 100% - Idle (%)

Parameters
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of time that the CPU(s) were busy.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Free Memory (KB)

Description
Free Memory is the size of the free list in kilobytes.

This test checks the size of the free memory in kilobytes on the system. If the size is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class vm vminfo).

Parameters
- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The size of the free memory in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

HAT Faults (#/s)

Description
HAT (hardware address translation) Faults is the minor page faults by way of hat_ fault() per second.

This test checks the number of HAT faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of HAT faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of hardware address translation (HAT) faults per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Idle (%)

Description
Idle (%) is the percentage of time that the CPU was idle and the system did not have an outstanding disk I/O request.

This test checks the percentage of processor time in idle mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Idle (%) value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of time that the CPU was idle and no outstanding disk I/O request in the last interval.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Logical IO Reads (#/s)

Description

Logical I/O Reads is the number of logical block reads per second. When a logical read from a block device is performed, a logical transfer size of less than a full block size may be requested.

This test checks the logical I/O read rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Logical I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of logical block reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Logical IO Writes (#/s)

Description
Logical I/O Writes is the number of logical block writes per second. When a logical write to a block device is performed, a logical transfer size of less than a full block size may be requested.

This test checks the logical I/O write rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Logical I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in

the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of logical block writes per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Maj Faults (#/s)

Description
Maj (major) Faults is the number of major page faults per second.

This test checks the number of major faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of major faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of major faults per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Incoming Errors (#/s)

Description

Incoming Errors is the number of input errors, per second, encountered on the device for unsuccessful reception due to hardware/network errors.

This test checks the rate of input errors on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from the kernel statistics (class net).

Parameters

- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner to connect to the target node, then click on the class "Network". If no "Network" class

displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The rate of input errors on the network interface.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Incoming Packets (#/s)

Description
Incoming Packets is the number of packets, per second, that have been received successfully by the device.

This test checks the rate at which packets are received on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class net).

Parameters
- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner to connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The rate at which packets are received on the network interface.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Outgoing Errors (#/s)

Description
Outgoing Errors is the number of output errors per second.

This test checks the rate of output errors on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class net).

Parameters
- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner to connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The rate of output errors on the network interface.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Outgoing Packets (#/s)

Description
Outgoing Packets is the number of packets, per second, that have been sent out by the device.

This test checks the rate at which packets are sent on the network interface specified by the network device names parameter, such as le0 or * (for all network interfaces). If the rate is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class net).

Parameters
- Network Device Name(s): Filter for network device names, such as le0 or * for all network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner to connect to the target node, then click on the class "Network". If no "Network" class displays for the target node, this means the interface on the target node is not supported by the Oracle Intelligent Agent.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The rate at which packets are sent on the network interface.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Percent Memory Used

Description
Percent Memory Used is the ratio of the resident set size of a process to the physical memory on the machine, expressed as a percentage.

This test checks the percent memory used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the percent memory used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from file /proc/<pid>/psinfo.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.
- Percent Memory Used: The ratio of a process's resident set size to the physical memory on the machine.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Physical IO Reads (#/s)

Description
Physical I/O Reads is the number of raw I/O reads per second.

This test checks the physical I/O read rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Physical I/O Reads value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of physical I/O reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Physical IO Writes (#/s)

Description

Physical I/O Writes is the number of raw I/O writes per second.

This test checks the physical I/O write rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the Physical I/O Writes value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of physical I/O writes per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Prot Faults (#/s)

Description

Prot (protection) Faults is the number of protection faults per second. Protection faults occur when a program attempts to access memory it should not access, receives a segmentation violation signal, and dumps a core file.

This test checks the number of protection faults for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of protection faults is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of protection faults per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Read Throughput

Description

Read Throughput is the number of kilobytes read per second.

This test checks the read throughput. If the read throughput is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class disk).

Parameters
- Disk Device Name(s): Filter for disk names, such as sd0 or * for all disks on the system. **Note:** To access the list of available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "I/O".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of kilobytes read per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Reads (#/s)

Description
Reads is the number of reads per second.

This test checks the read rate. If the read rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class disk).

Parameters
- Disk Device Name(s): Filter for disk names, such as sd0 or * for all disks on the system. **Note:** To access the list of available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "I/O".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Resident Size (KB)

Description
Resident Size is the resident set size of a process, in kilobytes.

This test checks the resident size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the resident size of one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from file /proc/<pid>/psinfo.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.

- Resident Size: The resident set size of a process, in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Run Queue

Description
Run Queue is the average number of processes in memory and subject to be run in the last interval.

This test checks the run queue. If the run queue is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class vm vminfo).

Parameters
- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The run queue in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Swap Queue

Description
Swap Queue is the average number of swapped processes in the last interval.

This test checks the average number of swapped processes. If the number is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class vm vminfo).

Parameters
- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The average swap queue length in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Sys (%)

Description
Sys (%) is the percentage of time that the CPU is running in system mode (kernel).

This test checks the percentage of processor time in system mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Sys (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the

value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Percentage of time that the CPU is running in the system mode in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Call Forks (#/s)

Description
System Call Forks is the number of calls fork() per second.

This test checks the calls to system call fork() rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of calls of fork() per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

System Call VForks (#/s)

Description

System Call VFork is the number of calls vfork() per second.

This test checks the calls to system call vfork() rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of calls of vfork() per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Calls (#/s)

Description
Systems Calls is the number of calls (per second) to the system service routines that perform basic scheduling and synchronizing of activities on the computer.

This test checks the system calls rate for CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Calls value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of system calls per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Interrupts (#/s)

Description
System Interrupts is the number of device interruptions the processor is experiencing per second. These device interruptions can result from system devices such as the mouse, network cards, and so on. This metric also measures the activity of those devices are in the overall system environment.

This test checks the system interruptions rate for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0 or * (for all CPUs on the system). If the System Interruptions value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of device interruptions per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Page Ins (#/s)

Description
System Page Ins is the number of page read ins per second (read from disk to resolve fault memory references) by the virtual memory manager. Along with Page Out, this statistic represents the amount of real I/O initiated by the virtual memory manager.

This test checks the number of page read ins for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of page read ins is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page read ins per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Page Outs (#/s)

Description
System Page Outs is the number of page write outs to disk per second.

This test checks the number of page write outs for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of page write outs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page write outs per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Pages Paged In (#/s)

Description
System Pages Paged In is the number of pages paged in (read from disk to resolve fault memory references) per second.

This test checks the number of pages paged in for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of pages paged in is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of system pages paged in per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Pages Paged Out (#/s)

Description
System Page Outs is the number of pages written out (per second) by the virtual memory manager. Along with Page Out, this statistic represents the amount of real I/O initiated by the virtual memory manager.

This test checks the number of pages paged out for the CPU(s) specified by the Host CPU(s) parameter, such as cpu_stat0 or * (for all CPUs on the system). If the number of pages paged out is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in

the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of system pages paged out per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Time (%)

Description
System Time (%) is the percentage of system level CPU time that a process used.

This test checks the percentage of system time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the System Time (%) value used by any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from file /proc/<pid>/status.

Parameters

- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Process name with process ID: To identify the exact process.
- System Time: The percentage of system level CPU time that a process used.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Threads

Description

Threads is the number of lwps (lightweight processes) in a process.

This test checks the number of threads in the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the number of threads is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from file /proc/<pid>/status.

Parameters

- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Process name with process ID: To identify the exact process.
- Threads: the number of threads in a process.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Used (KB)

Description

Used is the amount of space (in kilobytes) allocated to existing files.

This test checks for space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all file systems). If the space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved through system call statvfs().

Parameters

- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The used space in kilobytes on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

User (%)

Description
User (%) is the portion of processor time running in user mode.

This test checks the percentage of processor time in user mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the User (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters
- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Percentage of time that the CPU is running in the user mode in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

User Time

Description
User Time (%) is the percentage of user level CPU time that a process used.

This test checks the percentage of user time that has been used by the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the User Time (%) value used by one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from file /proc/<pid>/status.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.
- User Time: The percentage of user level CPU time that a process used.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Utilized (%)

Description
Utilized is the percentage of space that is currently allocated to all files on the file system.

This test checks for the percentage of space used on the disk specified by the File System Name parameter, such as /, /tmp, or * (for all disks). If the percentage of space used is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved through system call statvfs().

Parameters
- File System Name(s): Filter for file system names, such as /, /tmp, or * for all file systems on the system. **Note:** To access the list of available file systems, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "File System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of space used on the file system.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Virtual Size (KB)

Description
Virtual Size is the total size of a process in virtual memory, in kilobytes.

This test checks the total size of the process(es) specified by the process names parameter, such as vppdc or * (for all processes running on the system). If the total size of any one process is greater than or equal to the values specified in the threshold arguments, and the number of occurrences exceeds the value specified in

the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from file /proc/<pid>/psinfo.

Parameters
- Process(es): Filter for processes, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Process name with process ID: To identify the exact process.
- Virtual Size: the total size of a process in virtual memory, in kilobytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Wait (%)

Description
Wait (%) is the percentage of time that the CPU was idle during which the system had an outstanding disk I/O request.

This test checks the percentage of processor time in wait mode for the CPU(s) specified by the Host CPU parameter, such as cpu_stat0, CPU0, or * (for all CPUs on the system). If the Wait (%) value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class misc cpu_stat).

Parameters

- System Host CPU(s): Filter for CPUs, such as cpu_stat0, CPU0, or * for all CPUs on the system. **Note:** To access the list of available CPU IDs, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "CPU Utilization".
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

Percentage of time that the CPU was idle and wait for disk I/O in the last interval.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Waiting

Description

Waiting is the average number of jobs waiting for I/O in the last interval.

This test checks the average number of jobs waiting for I/O. If the waiting queue is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from the kernel statistics (class vm vminfo).

Parameters

- System: To access the available system instance, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory/Swap".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The average waiting queue length in the last interval.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Writes (#/s)

Description
Writes is the number of writes per second.

This test checks the write rate. If the write rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class disk).

Parameters
- Disk Device Name(s): Filter for disk names, such as sd0 or * for all disks on the system. **Note:** To access the list of available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "I/O".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of writes per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Write Throughput

Description
Write Throughput is the number of kilobytes written per second.

This test checks the write throughput. If the write throughput is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from the kernel statistics (class disk).

Parameters
- Disk Device Name(s): Filter for disk names, such as sd0 or * for all disks on the system. **Note:** To access the list of available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "I/O".
- Warning Threshold: Threshold for warning alert, in kilobytes.
- Critical Threshold: Threshold for critical alert, in kilobytes.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of kilobytes written per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

7

Windows NT Event Tests

The Oracle Enterprise Manager Advanced Event Tests for Windows NT are divided into a series of classes or groupings that will enable you to find the event test you are interested in registering.

The class names and some of the events that you can register within the classes are listed as follows.

- Cache: includes data maps, pin reads, MDL statistics, lazy write statistics, and data flush information (See Table 7–1)
- Logical Disk: includes percentage of free space and free megabytes (See Table 7–2)
- Memory: includes free memory, swap space, average number of processes in memory, and average number of jobs waiting for I/O (See Table 7–3)
- Network Interface: includes packet statistics, current bandwidth, and bytes sent and received (See Table 7–4)
- Objects: includes processes, threads, events, semaphores, mutexes, and sections (See Table 7–5)
- Paging File: includes usage and peak usage percentages (See Table 7–6)
- Physical Disk: includes queue lengths, disk read / write times, disk transfers, and average disk byte statistics (See Table 7–7)
- Process: includes virtual bytes, working sets, thread counts, and handle counts (See Table 7–8)
- Processor: includes user time, processor time, privileged time, DPC rates (See Table 7–9)
- System: includes file read / write operations, system call operations, and system page operations (See Table 7–10)

Summary of Windows NT Event Tests

The following tables list the Windows NT event tests by class. The full descriptions of the individual event tests follow the tables. The event tests are in alphabetical order.

Table 7–1 Cache Class Event Tests

Event Test	Description
Async Copy Reads/sec	Async Copy Reads per Second measures the frequency of cache page reads that include placing a memory copy of the data from the cache on the application's buffer. The application will be able to access the disk and retrieve the page immediately. If the value of Async Copy Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Async Data Maps/sec	Async Data Maps per Second measures the frequency that the NTFS or HPFS file systems map a page of a file into the cache to read the page and does not wait for the cache to retrieve the page (if the page is not in the main memory.) If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Async Fast Reads/sec	Async Fast Reads per Second measures the frequency of cache page reads that retrieve data directly from the cache without going through the installed file system. In a typical read, the I/O requests prompt the file system to retrieve data from a file. If the data is not in the cache, a fast read will still eliminate one invocation of the file system. The request will have immediate control of the data even if the data is not in the cache. If the value of Async Fast Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Async MDL Reads/sec	Async MDL (Memory Descriptor List) Reads per Second measures the frequency of cache page reads that access data using the MDL. The physical address of each page within the transfer is contained in the memory descriptor list. This information enables the Direct Memory Access (DMA) device to secure the copy. The access device will not wait for the pages to fault from the disk if the pages are not in the main memory. If the value of Async MDL Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–1 Cache Class Event Tests (Cont.)

Event Test	Description
Async Pin Reads/sec	Async Pin Reads per Second measures the frequency of reading data into the cache before the data is written back to disk. When pages are read this way they become pinned in memory when the read is complete. The file system will have immediate control of the page and will be able to access the disk and retrieve the page immediately if needed. A pinned page's physical address cannot be modified. If the value of Async Pin Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Copy Read Hits %	Copy Read Hits measures the percentage of copy read hit requests that the cache receives. Copy read hits do not require a disk read to access a page in the cache. A copy read is a type of file read operation that allows a memory copy from a cache page to the application's buffer. The Local Area Network (LAN) Redirector, the LAN Server and the disk file systems use the copy reads for retrieving cache information. If the value of Copy Read Hits per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Copy Reads/sec	Copy Reads per Second measures the frequency of cache page reads that includes placing a memory copy of the data from the cache on the application's buffer. The Local Area Network (LAN) Redirector, the LAN Server, and the disk file systems use copy reads for retrieving cache information. If the value of Copy Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Data Flush Pages/sec	Data Flush Pages per Second calculates the number of pages have been flushed to disk from the Cache. Pages are flushed when the cache approves a write-through file write request of its content to disk. Note that more than one page can be transferred for each flush operation. If the value of Data Flush Pages per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Data Flushes	Data Flushes per Second measures the frequency at which the cache has approved a write-through file write request of its content to disk. Note that for each flush operation, more than one page can be transferred. If the value of Data Flushes per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–1 Cache Class Event Tests (Cont.)

Event Test	Description
Data Map Hits %	Data Map Hits calculates the percentage of Data Maps in the cache that can be resolved without retrieving a page from the disk. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Data Map Pins / sec	Data Map Pins per Second measures the frequency of Data Maps in the cache that caused a page to be pinned in the main memory. When a page is pinned the physical address in main memory and its virtual address in the cache cannot be modified. If the value of Data Map Pins per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Data Maps / sec	Data Maps per Second measures the frequency that the NTFS or HPFS file systems map a page of a file into the cache. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Fast Read Not Possibles / sec	Fast Read Not Possibles per Second is the frequency at which calls are made by the Application Program Interface (API) to try and avoid the file system to get cache data. This metric monitors the number of times that these calls fail because the file system must be accessed. If the value of Fast Read Not Possibles per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Fast Read Resource Misses / sec	Fast Read Resource Misses per Second measures the frequency at which cache reads are missed due to a lack of resources to satisfy the request. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Fast Reads / sec	Fast Reads per Second measures the frequency of cache page reads that retrieve data directly from the cache without going through the installed file system. In a typical read, the I / O requests prompt the file system to retrieve data from a file. If the data is not in the cache, a fast read will still eliminate one invocation of the file system. If the value of Fast Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–1 Cache Class Event Tests (Cont.)

Event Test	Description
Lazy Write Flushes/sec	Lazy Write Flushes per Second measures the frequency at which the lazy write thread involves updating the disk after the page has been changed in memory. By doing this the application requesting the file change will not have to wait for the disk write to complete before proceeding. Note that more than one page can be transferred on each writer operation. If the value of Lazy Write Flushes per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Lazy Write Pages/sec	Lazy Write Pages per Second measures the frequency at which the lazy write thread involves updating the disk after the page has been changed in memory. By doing this the application requesting the file change will not have to wait for the disk write to complete before proceeding. Note that more than one page can be transferred on a single disk write operation. If the value of Lazy Write Pages per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
MDL Read Hits %	MDL (Memory Descriptor List) Read Hits measures the percentage of requests that the cache receives for cache memory descriptor (MDL) list reads. MDL reads provide memory access to the cache pages without accessing the disk. If the Percentage of MDL Read Hits is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
MDL Reads/sec	MDL (Memory Descriptor List) Reads per Second measures the frequency of cache page reads that access data using the MDL. The physical address of each page within the transfer is contained in the memory descriptor list. This information enables the Direct Memory Access (DMA) device to secure the copy. If the value of MDL Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pin Read Hits %	Pin Read Hits calculates the percentage of pin requests that the cache receives. A pin read request does not require a disk read to access the page in cache. A pinned page's physical address in the cache cannot be modified. The Local Area Network (LAN) Redirector, the LAN Server, and the disk file system use pin reads to retrieve cache information. If the value of Pin Read Hits is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–1 Cache Class Event Tests (Cont.)

Event Test	Description
Pin Reads/sec	Pin Reads per Second measures the frequency of reading data into the cache before the data is written back to disk. When pages are read this way they become pinned in memory when the read is complete. A pinned page's physical cache address cannot be modified. If the value of Pin Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Read Aheads/sec	Read Aheads per Second measures the frequency at which cache reads detect sequential file access. Read aheads reduce overhead access by enabling the data to be transferred in larger blocks than those requested by the application. If the value of Read Aheads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Sync Copy Reads/sec	Sync Copy Reads per Second measures the frequency of cache page reads that include placing a copy of the data from the cache on the application's buffer. The file system will not be able to access the disk and retrieve the page until the copy operation is complete. If the value of Sync Copy Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Sync Data Maps/sec	Sync Data Maps per Second measures the frequency that the NTFS or HPFS file systems map a page of a file into the cache and waits for the cache to retrieve the page (if the page is not in the main memory.) If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Sync Fast Reads/sec	Sync Fast Reads per Second measures the frequency of cache page reads that retrieve data directly from the cache without going through the installed file system. In a typical read, the I/O requests prompt the file system to retrieve data from a file. If the data is not in the cache, a fast read will still eliminate one invocation of the file system. The request will not wait until the data has been retrieved from disk if the data is not in the cache. If the value of Sync Fast Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–1 Cache Class Event Tests (Cont.)

Event Test	Description
Sync MDL Reads/sec	Sync MDL (Memory Descriptor List) Reads per Second measures the frequency of cache page reads that access data using the MDL. The physical address of each page within the transfer is contained in the memory descriptor list. This information enables the Direct Memory Access (DMA) device to secure the copy. The access device will wait for the pages to fault from the disk if the pages are not in the main memory. If the value of Sync MDL Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Sync Pin Reads/sec	Sync Pin Reads per Second measures the frequency of reading data into the cache before the data is written back to disk. When pages are read this way they become pinned in memory when the read is complete. When the page is pinned in the cache the file system can regain control of the page. Until the page is pinned in cache, however, the file system cannot access the disk and retrieve the page. A pinned page's physical address in the cache cannot be changed. If the value of Sync Pin Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–2 Logical Disk Class Event Tests

Event Test	Description
% Free Space	Percentage Free Space calculates the ratio of available free space on the logical disk unit to the total usable space provided by the selected logical disk drive.
Free Megabytes	Free Megabytes measures the available (unallocated) space on the selected disk drive in megabytes. One megabyte = 1,048,576 bytes.

Table 7–3 Memory Class Event Tests

Event Test	Description
% Committed Bytes In Use	Percentage of Committed Bytes in Use measures the real-time ratio of committed bytes to the commit limit. The ratio indicates the amount of virtual memory in use. Note that if the paging file is extended the commit limit may change. If the Percentage of Committed Bytes in Use is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Available Bytes	Available Bytes metric measures the real-time amount of virtual memory on the Zeroed, Free and Standby lists. If this value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–3 Memory Class Event Tests (Cont.)

Event Test	Description
Available Memory (%)	Available Memory % measures the real-time amount of free memory in the percentage of total physical memory.
Cache Bytes	Cache Bytes measures the number of bytes currently being used by the system cache. The system cache buffers data retrieved from the disk or local area network. The system cache then uses the memory that is not currently being used by any active system processes. If Cache Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Cache Faults / sec	Cache Faults per Second measures the number of times a cache fault occurs. Cache faults are caused when the cache manager fails to find a file's page in the immediate cache and requests the memory manager to locate the page in memory or on the disk so that it can be added to the immediate cache. If the value of Cache Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Commit Limit	Commit Limit measures the amount of virtual memory (in bytes) that can be committed without extending the paging files. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Committed Bytes	Committed Bytes measures the total amount of virtual memory (in bytes) that have been committed. Committed memory should not be confused with reserved memory. Committed memory must have available disk storage or the main memory must by large enough to contain the committed virtual memory. If the value of Committed Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Demand Zero Faults / sec	Demand Zero Faults per Second measures the number of page faults for pages that must be filled with zeroes before the fault is resolved. If the zeroed list is not empty, the fault can be resolved by removing a page from the zeroed list. If the value of Demand Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Free System Page Table Entries	Free system page table entries measure the number of page table entries that are not currently being used by the system. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–3 Memory Class Event Tests (Cont.)

Event Test	Description
Page Faults/sec	Page Faults per Second measures the number of Page Faults in the processor. A page fault occurs when a virtual memory page is referenced by a process and that page is not in the current Working Set of the main memory. If the value of Page Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Page Reads/sec	Page Reads per Second measures the number of times the disk was read to retrieve pages of virtual memory to resolve page faults. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Page Writes/sec	Page Writes per Second measures the number of times pages have been written to disk because they were modified since the last retrieval. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pages/sec	Pages per Second measures the number of pages read from the disk or written to the disk to resolve faulty memory references. The metric calculates the sum of pages input per second plus the pages output per second. Use this metric to monitor memory thrashing and excessive paging. If the value of Pages per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pages Input/sec	Pages Input per Second measures the number of pages read from the disk to resolve faulty memory references. This is an important metric to monitor if memory thrashing and excessive paging has become a problem. If the value of Pages Input per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pages Output/sec	Pages Output per Second measures the number of pages that were written to disk because the pages were modified in main memory. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pool Nonpaged Allocs	Pool Nonpaged Allocs (Allocations) is the number of times a call has been made to allocate space in the nonpaged pool. Nonpaged pool pages cannot be paged out to the paging file. As long as they are allocated they must remain in the main memory. If the value of Pool Nonpaged Allocs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–3 Memory Class Event Tests (Cont.)

Event Test	Description
Pool Nonpaged Bytes	Pool Nonpaged Bytes measures the number of bytes in the nonpaged pool. Nonpaged pool pages cannot be sorted in the paging file. As long as they are allocated, they must remain in the main memory. If the value of Pool Nonpaged Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pool Paged Allocs	Pool Paged Allocs (Allocations) is the number of times a call has been made to allocate space in the system paged pool. Paged pool pages can be paged out to the paging file when the pages are not being accessed for any sustained amount of time. If the value of Pool Paged Allocs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pool Paged Bytes	Pool Paged Bytes measures the number of bytes in the paged pool. Paged pool pages can be paged out to the paging file when not being used by the system for a sustained length of time. If Pool Paged Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pool Paged Resident Bytes	Pool Paged Resident Bytes measures the size of paged pool bytes that reside in the main memory. The pool paged resident bytes value indicates the actual cost of the paged pool allocation since it is currently in use and it uses real (physical) memory. If the value of Pool Paged Resident Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Cache Resident Bytes	System Cache Resident Bytes measures the total number of bytes residing in the disk cache. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Code Resident Bytes	System Code Resident Bytes measures the number of bytes of system code currently residing in the main memory. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Code Total Bytes	System Code Total Bytes monitors the ntoskrnl.exe, hal.dll, and the boot drivers and file systems loaded by the ntldr/osloader for the total number of bytes of the pageable pages. If System Code Total Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–3 Memory Class Event Tests (Cont.)

Event Test	Description
System Driver Resident Bytes	System Driver Resident Bytes measures the total number of system driver bytes residing in the core memory. The returned value is considered the code working set of pageable drivers. If the value of System Driver Resident Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Driver Total Bytes	System Driver Total Bytes monitors all of the system driver devices and returns the total number of pageable pages currently in the devices. If the value of System Driver Total Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Transition Faults / sec	Transition Faults per Second measures the number of page faults that have been resolved by recovering pages that were being written to disk when the page fault occurred. These pages can be recovered without any additional disk activity. If the value of Transition Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Write Copies / sec	Write Copies per Second measures the number of page faults that have been resolved by making a copy or the page when an attempt is made to write to the page. If the value of Write Copies per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–4 Network Interface Class Event Tests

Event Test	Description
Bytes Received / sec	Bytes Received per Second measures the rate at which bytes are received on the interface. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Bytes Sent / sec	Bytes Sent per Second measures the rate at which bytes are sent on the interface. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–4 Network Interface Class Event Tests (Cont.)

Event Test	Description
Bytes Total / sec	Bytes Total per Second measures the rate at which bytes are sent and received on the interface. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Current Bandwidth	Current Bandwidth estimates the interface's current bandwidth in bits per second (bps). The nominal bandwidth value is given for interfaces that do not vary in bandwidth or for those where no accurate estimation can be made. If the Current Bandwidth is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Output Queue Length	Output Queue Length measures the length of the output packet queue (in packets.) Performance delays occur when the output queue experiences a bottleneck (typically when the length is longer than 2). Eliminate bottlenecks for optimal performance. If the Output Queue Length is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets / sec	Packets per Second measures the rate at which packets are sent and received on the network interface. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Outbound Discarded	Packets Outbound Discarded measures the number of outbound packets that were chosen to be discarded (to prevent them from being transmitted) and possibly free up buffer space. If the number of Packets Outbound Discarded is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Outbound Errors	Packets Outbound Errors measures the total number of outbound packets that had errors and therefore could not be transmitted. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Received / sec	Packets Received per Second measures the rate at which packets are received on the network interface. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–4 Network Interface Class Event Tests (Cont.)

Event Test	Description
Packets Received Discarded	Packets Received Discarded measures the number of inbound packets that were chosen to be discarded to prevent them from being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space. If the number of Packets Received Discarded is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Received Errors	Packets Received Errors measures the total number of inbound packets that contained errors and prevented them from being delivered to a higher-layer protocol. If the number of Packet Received Errors is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Received Non-Unicast/sec	Packets Received Non-Unicast per Second measures the rate at which non-unicast (subnet broadcast or subnet multicast) packets are delivered to a higher-layer protocol. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Received Unicast/sec	Packets Received Unicast per Second measures the rate at which (subnet) unicast packets are delivered to a higher-layer protocol. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Received Unknown	Packets Received Unknown measures the total number of packets the interface received and discarded because of an unknown or unsupported protocol. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Sent/sec	Packets Sent per Second measures the rate at which packets are sent on the network interface. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–4 Network Interface Class Event Tests (Cont.)

Event Test	Description
Packets Sent Non-Unicast/sec	Packets Sent Non-Unicast per Second measures the rate at which higher-level protocols requested packets to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses. The packets sent non-unicast rate includes the packets that were discarded or not sent. If the value of Packets Sent Non-Unicast per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Packets Sent Unicast/sec	Packets Sent Unicast per Second measures the rate at which higher-level protocols requested packets to be transmitted to subnet-unicast addresses. The packets sent unicast rate includes the packets that were discarded or not sent. If the value of Packets Sent Unicast per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–5 Objects Class Event Tests

Event Test	Description
Events	The Events metric measures the total number of real-time events in the computer at the time of data collection. Events are used when two or more threads wish to synchronize execution. If the number of real-time events is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Mutexes	The Mutexes metric measures the total number of real-time mutexes in the computer at the time of data collection. Threads use mutexes to assure only one thread is executing some section of code. If the total number of real-time mutexes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Processes	Processes calculates the total number of real-time processes in the computer at the time of data collection. Each process represents the running of a program. If the number of Processes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Sections	The Sections metric measures the total number of real-time sections in the computer at the time of data collection. A section is a portion of virtual memory created by a process for data storage. Processes may share sections with other processes. If the total number of real-time sections is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–5 Objects Class Event Tests (Cont.)

Event Test	Description
Semaphores	The Semaphores metric measures the total number of real-time semaphores in the computer at the time of data collection. Semaphores are used by threads to obtain exclusive access to data structures that threads share with other threads. If the total number of real-time semaphores is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Threads	The Threads metric measures the total number of real-time threads in the computer at the time of data collection. (Threads execute instructions in a processor.) If the number of Threads is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–6 Paging File Class Event Tests

Event Test	Description
% Usage	Percent Usage measures the percentage of Page File instance usage. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–7 Physical Disk Class Event Tests

Event Test	Description
% Disk Read Time	Percentage Disk Read Time calculates the percentage of time that the selected disk drive is busy servicing read requests. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Disk Time	Percentage Disk Time calculates the total amount of time that the selected disk drive was busy servicing read or write requests. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Disk Write Time	Percentage Disk Write Time calculates the percentage of time that the selected disk drive was busy servicing write requests. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–7 Physical Disk Class Event Tests (Cont.)

Event Test	Description
Avg. Disk Bytes / Read	Average Disk Bytes / Read calculates the average number of bytes transferred from the disk during read operations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Avg. Disk Bytes / Transfer	Avg. Disk Bytes / Transfer calculates the average number of bytes transferred to or from the disk during write or read operations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Avg. Disk Bytes / Write	Average Disk Bytes / Write calculates the average number of bytes transferred to the disk during write operations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Avg. Disk sec / Read	Average Disk sec / Read calculates the average time (in seconds) of a data read from the disk. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Avg. Disk sec / Transfer	Average Disk Sec / Transfer calculates the average time (in seconds) of a disk transfer. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Avg. Disk sec / Write	Average Disk sec / Write calculates the average time (in seconds) of a data write to the disk. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Avg. Response Time (ms)	Average Response Time (ms) calculates the average time (in milliseconds) of a disk transfer.
Current Disk Queue Length	Current Disk Queue Length calculates the total real-time number of outstanding requests that are on the disk and are currently in service when the performance data is collected. To maintain optimal performance calculate the ratio of delayed request to the length of the disk queue minus the number of spindles on the disks. The difference should be less than 2. (Note that disk devices with multiple spindles can have multiple requests active at one time.) If the value of Current Disk Queue Length is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Disk Bytes / sec	Disk Bytes per Second calculates the frequency at which bytes are transferred to or from the disk during write or read operations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–7 Physical Disk Class Event Tests (Cont.)

Event Test	Description
Disk Read Bytes / sec	Disk Read Bytes per Second calculates the frequency at which bytes are transferred from the disk during read operations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Disk Reads / sec	Disk Reads per Second calculates the frequency of read operations on the disk. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Disk Transfers / sec	Disk Transfers per Second calculates the frequency of read and write operations on the disk. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Disk Write Bytes / sec	Disk Write Bytes per Second calculates the frequency at which bytes are transferred to the disk during write operations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Disk Writes / sec	Disk Writes per Second calculates the frequency of write operations on the disk. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–8 Process Class Event Tests

Event Test	Description
% Privileged Time	Percentage Privileged Time calculates the percentage of time that process threads have been executing code in Privileged Mode. Services often run in Privileged Mode to gain access to system-private data. Threads executing in User Mode protect system-private from access. System calls may be explicit or implicit (when a page fault or an interrupt occurs, for example.) Special process boundaries have been integrated with Windows NT so that code executing in User Mode will not interfere with the Windows NT Executive, Kernel, and device drivers. Note that you may see Windows NT-related tasks in other subsystem processes in addition to seeing the Privileged Time in your own process. If the Percentage Privileged Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Processor Time	Percentage Processor Time measures the total amount of time that the processor was used by the threads of a process to execute instructions. Instructions sent to handle certain hardware interrupts or trap conditions may be included in the percentage of processor time. If the Percentage Processor Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% User Time	Percentage User Time calculates the percentage of time that process threads have been executing code in User Mode. Special process boundaries have been integrated with Windows NT so that code executing in User Mode will not interfere with the Windows NT Executive, Kernel, and device drivers. Note that you may see Windows NT-related tasks in other subsystem processes in addition to seeing the Privileged Time in your own process. If the Percentage User Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Elapsed Time	Elapsed time measures the total amount of time (in seconds) that the process has been running. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Handle Count	Handle Count calculates the total number of handles currently open by each thread in this process. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Page Faults/sec	Page Faults per Second measures the rate of Page Faults by the threads executing in this process. Page faults occur when threads reference a virtual memory page that is not in currently its working set in main memory. When the page is not in the working set it cannot be fetched from disk if it is in main memory or when the shared page is being used by another process. If the value of Page Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–8 Process Class Event Tests (Cont.)

Event Test	Description
Page File Bytes	Page File Bytes measures the total number of bytes this process has used in the paging file(s). Paging files store pages of memory used by the process but are not contained in other files. Paging files are shared by all processes but if there is insufficient space in the paging files, other processes may not be able to allocate memory. If the value of Page File Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pool Nonpaged Bytes	Pool Nonpaged Bytes calculates the total number of bytes in the Nonpaged Pool. The Paged Pool is the area in the system memory where operating system components acquire space to accomplish tasks. Nonpaged Pool pages remain in main memory as long as they are allocated and cannot be paged out to the paging file. If the value of Pool Nonpaged Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Pool Paged Bytes	Pool Paged Bytes calculates the total number of bytes in the Paged Pool. The Paged Pool is the area in the system memory where operating system components acquire space to accomplish tasks. When not being accessed by the system, Paged Pool pages can be paged out to the paging file. If the value of Pool Paged Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Private Bytes	Private Bytes calculates the total number of bytes allocated by the process that cannot be shared with other processes. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Thread Count	Thread Count measures the number of threads in the process that are currently active. Threads are responsible for executing instructions (basic units of application work). Every active process has at least one thread. If the Thread Count is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–8 Process Class Event Tests (Cont.)

Event Test	Description
Virtual Bytes	Virtual Bytes calculates the current size (in bytes) of the virtual address space being used by a process. Using too much virtual memory may limit the ability to load libraries. Note that using virtual address space is not an indication that you are also using disk or main memory pages. If the value of Virtual Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Working Set	Working Set measures total number of bytes currently in the Working Set of the process. The Working Set is the set of memory pages recently accessed by the threads in the process. If the system's free memory rises above a threshold, the pages are left in the Working Set even if they are not in use. If the system's free memory falls below a threshold, the pages are trimmed from Working Sets. If the memory pages are needed they will then be soft-faulted back into the Working Set before they leave main memory. If the value of Working Set is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–9 Processor Class Event Tests

Event Test	Description
% DPC Time	Percentage of DPC (Deferred Procedure Call) Time measures the percentage of time the processor spends in DPC mode. This metric can also assist in determining the cause of excessive privileged mode usage. A deferred procedure call is caused when a hardware device interrupts the processor and the Interrupt Handler chooses to execute its work in a deferred procedure call. DPCs enable interrupts to occur because deferred procedure calls run at a lower priority than interrupts. If the Percentage of DPC Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Interrupt Time	Percentage of Interrupt Time measures the percentage of time a processor spends handling hardware interrupts. When the processor is interrupted by a hardware device, the Interrupt Handler signals an I/O completion and issues another pending I/O request. This metric can also be used to determine the source of excessive Privileged mode usage. If the Percentage of Interrupt Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Privileged Time	Percentage of Privileged Time measures the percentage of time a processor spends in Privileged mode with non-idle threads. The Percentage of Privileged Time metric includes Windows NT service layer, the Executive routines, the Windows NT Kernel, and device drivers in the calculation of total Privileged time. If the Percentage of Privileged Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–9 Processor Class Event Tests (Cont.)

Event Test	Description
% Processor Time	Percentage of Processor Time measures the total amount of time that a processor is busy executing a non-idle thread. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% User Time	Percentage of User Time measures the percentage of time a processor spends in user mode with non-idle threads. The Percentage of User Time metric includes the amount of time that all application code and peripheral devices execute in user mode. If the Percentage of User Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
APC Bypasses / sec	APC (Asynchronous Procedure Call) Bypasses per Second calculates the rate at which kernel APC interrupts are circumvented. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
DPC Bypasses / sec	DPC (Deferred Procedure Call) Bypasses per Second calculates the average rate at which Dispatch interrupts are circumvented. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
DPC Rate	DPC (Deferred Procedure Call) Rate calculates the average rate at which DPC objects are added to the processor's DPC queue. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
DPCs Queued / sec	DPCs (Deferred Procedure Calls) Queued per Second measures the rate at which DPC objects are added to the processor's DPC queue. If this rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Interrupts / sec	Interrupts per Second measures the number of times the processor experiences an interrupt caused by a device. Device interruptions occur when the device completes a task or when the device requires attention. These interruptions suspend normal thread executions which can cause the processor to switch to a higher priority thread. If Interrupts per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–10 System Class Event Tests

Event Test	Description
% Registry Quota In Use	Percentage (%) Registry Quota In Use measures the total amount of registry quota allowed by the system. If the value of Percentage Registry Quota In Use is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Total DPC Time	Percentage (%) Total DPC (Deferred Procedure Call) Time calculates the percentage of total DPC time divided by the number of system processors. If the Percentage Total DPC Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Total Interrupt Time	Percentage (%) Total Interrupt Time calculates the total percentage of interrupt time for all processors divided by the number of system processors. If the Percentage Total Interrupt Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Total Privileged Time	The Percentage (%) of Total Privileged Time measures the amount of time the processors are running in Privileged mode. For example, if multiple processors are all running in Privileged mode, then the Percentage of Total Privileged Time would be 100%. If only half of the processors are running in Privileged mode then the percentage would be 50%. If the percentage of time that the processors are running in Privileged mode is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Total Processor Time	Percentage (%) of Total Processor Time is the fraction or percentage of time that the system processor is running non-idle threads. For example, if all of the system processors are busy the Percentage of Total Processor Time would be 100%. If only half of the processors are busy running non-idle threads, then the Percentage of Total Processor Time would be 50%. If the percentage of time that the system processor is running non-idle threads is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
% Total User Time	The Percentage (%) of Total User Time measures the amount of time the processors are running in user mode. For example, if multiple processors are all running in user mode, then the Percentage of Total User Time would be 100%. If only half of the processors are running in user mode then the percentage would be 50%. If the percentage of time that the processors are running in user mode is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–10 System Class Event Tests (Cont.)

Event Test	Description
Alignment Fixups / sec	Alignment Fixups per Second measures the rate by which the system is able to fix alignment faults. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Context Switches / sec	Context Switches per Second measures the rate of switches among threads. Switches can occur either inside of a single process or across multiple processes. A thread switch can happen when one thread requests information from another thread or when a higher priority thread preempts another thread. In addition to the traditional protection of User and Privileged modes, Windows NT also uses process boundaries for subsystem protection. These protection boundaries may appear in other subsystem processes in addition to the Privileged Time in the application. Switching to the subsystem process causes one Context Switch in the application thread. Switching back causes another Context Switch in the subsystem thread. If the value of Context Switches per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Exception Dispatches / sec	Exception Dispatches per Second measures the rate that the system dispatches exceptions. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
File Control Bytes / sec	File Control Bytes per Second is the sum total of bytes transferred for all file system including file system control requests or requests for information about device characteristics or status. (Does not include read or write operations.) If the value of File Control Bytes per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
File Control Operations / sec	File Control Operations per Second is the sum total of all file system operations including file system control requests or requests for information about device characteristics or status. (Does not include read or write operations.) If the value of File Control Operations per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
File Data Operations / sec	File Data Operations per Second measures the number of Read and Write operations being issued by the computer to file system devices. This metric does not measure File Control Operations. If the value of File Data Operations per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–10 System Class Event Tests (Cont.)

Event Test	Description
File Read Bytes / sec	File Read Bytes per Second is the sum total of bytes transferred for all the file system read operations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
File Read Operations / sec	File Read Operations per Second is the sum total of all the file system read operations on the system. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
File Write Bytes / sec	File Write Bytes per Second is the sum total of bytes transferred for all the file system write operations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
File Write Operations / sec	File Write Operations per Second is the sum total of all the file system write operations on the system. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Floating Emulations / sec	Floating Emulations per Second measures the rate by which the system performs floating emulations. If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Processor Queue Length	Processor Queue Length measures the number of threads in the current processor queue (not the threads that are currently executing.) Note that the Processor Queue Length metric is a real-time count of threads and not an average count over time. If the Processor Queue Length is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
System Calls / sec	Systems Calls per Second measures the frequency of calls to system service routines that perform basic scheduling and synchronizing of activities on the computer. These routines also provide access to non-graphical devices, memory management, and name space management. If the value of System Calls per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Total APC Bypasses / sec	Total APC (Asynchronous Procedure Call) Bypasses per Second measures the overall rate at which APC interrupts were circumvented across all processors. If this rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Table 7–10 System Class Event Tests (Cont.)

Event Test	Description
Total DPC Bypasses / sec	Total DPC (Deferred Procedure Call) Bypasses per Second measures the rate at which Dispatch Interrupts were circumvented across all platforms. If this rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Total DPC Rate	Total DPC (Deferred Procedure Call) Rate is the average speed (measured in seconds) by which DPC objects are added to the processor's DPC queue. If the Total DPC Rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Total DPCs Queued / sec	Total DPCs (Deferred Procedure Calls) Queued per Second measures the rate at which objects are added to the processor's DPC queue. If this rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.
Total Interrupts / sec	Total Interrupts per Second measures the rate that the computer is handling interruptions from system devices such as the mouse, network cards, and system clocks. This metric also indicates how busy those devices are in the overall system environment. If the value of Total Interrupts per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Descriptions of Windows NT Event Tests

The Windows NT event tests are listed in alphabetical order.

% Committed Bytes In Use

Description

Percentage of Committed Bytes in Use measures the real-time ratio of committed bytes to the commit limit. The ratio indicates the amount of virtual memory in use. Note that if the paging file is extended the commit limit may change.

If the Percentage of Committed Bytes in Use is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of committed bytes in use.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Disk Read Time

Description
Percentage Disk Read Time calculates the percentage of time that the selected disk drive is busy servicing read requests.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use

Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".

- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Percentage disk read time

Recommended Frequency

5 minutes

User Action

Specific to your site.

% Disk Time

Description

Percentage Disk Time calculates the total amount of time that the selected disk drive was busy servicing read or write requests.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".

- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Disk name
- Percentage disk time

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Disk Write Time

Description
Percentage Disk Write Time calculates the percentage of time that the selected disk drive was busy servicing write requests.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0

- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Percentage disk write time

Recommended Frequency

5 minutes

User Action

Specific to your site.

% DPC Time

Description

Percentage of DPC (Deferred Procedure Call) Time measures the percentage of time the processor spends in DPC mode. This metric can also assist in determining the cause of excessive privileged mode usage. A deferred procedure call is caused when a hardware device interrupts the processor and the Interrupt Handler chooses to execute its work in a deferred procedure call. DPCs enable interrupts to occur because deferred procedure calls run at a lower priority than interrupts.

If the Percentage of DPC Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".

- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of DPC time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Free Space

Description
Percentage Free Space calculates the ratio of available free space on the logical disk unit to the total usable space provided by the selected logical disk drive.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Logical Disk(s): Filter for logical disks to be monitored, such as "0 ==> C:" or "0 ==> C:, 1 ==> D:" for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Logical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Disk name
- Percentage of free space

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Interrupt Time

Description
Percentage of Interrupt Time measures the percentage of time a processor spends handling hardware interrupts. When the processor is interrupted by a hardware device, the Interrupt Handler signals an I/O completion and issues another pending I/O request. This metric can also be used to determine the source of excessive Privileged mode usage.

If the Percentage of Interrupt Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of interrupt time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Privileged Time (Process Class)

Description
Percentage Privileged Time calculates the percentage of time that process threads have been executing code in Privileged Mode. Services often run in Privileged Mode to gain access to system-private data. Threads executing in User Mode protect system-private from access. System calls may be explicit or implicit (when a page fault or an interrupt occurs, for example.) Special process boundaries have been integrated with Windows NT so that code executing in User Mode will not interfere with the Windows NT Executive, Kernel, and device drivers. Note that you may see Windows NT-related tasks in other subsystem processes in addition to seeing the Privileged Time in your own process.

If the Percentage Privileged Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage privileged time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Privileged Time (Processor Class)

Description
Percentage of Privileged Time measures the percentage of time a processor spends in Privileged mode with non-idle threads. The Percentage of Privileged Time metric includes Windows NT service layer, the Executive routines, the Windows NT Kernel, and device drivers in the calculation of total Privileged time.

If the Percentage of Privileged Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of privileged time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Processor Time (Process Class)

Description
Percentage Processor Time measures the total amount of time that the processor was used by the threads of a process to execute instructions. Instructions sent to handle certain hardware interrupts or trap conditions may be included in the percentage of processor time.

If the Percentage Processor Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of processor time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Processor Time (Processor Class)

Description

Percentage of Processor Time measures the total amount of time that a processor is busy executing a non-idle thread.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of processor time.

Recommended Frequency

5 minutes

User Action

Specific to your site.

% Registry Quota In Use

Description

Percentage (%) Registry Quota In Use measures the total amount of registry quota allowed by the system.

If the value of Percentage Registry Quota In Use is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of registry quota in use.

Recommended Frequency

5 minutes

User Action

Specific to your site.

% Total DPC Time

Description

Percentage (%) Total DPC (Deferred Procedure Call) Time calculates the percentage of total DPC time divided by the number of system processors.

If the Percentage Total DPC Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of total DPC time.

Recommended Frequency

5 minutes

User Action

Specific to your site.

% Total Interrupt Time

Description

Percentage (%) Total Interrupt Time calculates the total percentage of interrupt time for all processors divided by the number of system processors.

If the Percentage Total Interrupt Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of total interrupt time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Total Privileged Time

Description
The Percentage (%) of Total Privileged Time measures the amount of time the processors are running in Privileged mode. For example, if multiple processors are all running in Privileged mode, then the Percentage of Total Privileged Time would be 100%. If only half of the processors are running in Privileged mode then the percentage would be 50%.

If the percentage of time that the processors are running in Privileged mode is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of total privileged time.

Recommended Frequency

5 minutes

User Action

Specific to your site.

% Total Processor Time

Description

Percentage (%) of Total Processor Time is the fraction or percentage of time that the system processor is running non-idle threads. For example, if all of the system processors are busy the Percentage of Total Processor Time would be 100%. If only half of the processors are busy running non-idle threads, then the Percentage of Total Processor Time would be 50%.

If the percentage of time that the system processor is running non-idle threads is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of total processor time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% Total User Time

Description
The Percentage (%) of Total User Time measures the amount of time the processors are running in user mode. For example, if multiple processors are all running in user mode, then the Percentage of Total User Time would be 100%. If only half of the processors are running in user mode then the percentage would be 50%.

If the percentage of time that the processors are running in user mode is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of total user time.

Recommended Frequency

5 minutes

User Action

Specific to your site.

% Usage

Description

Percent Usage measures the percentage of Page File instance usage.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Paging File(s): Filter for paging files to be monitored, such as _Total, or * for all paging files on the system. Note: To access the list of all available paging files, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Paging File".

- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of page file instance usage.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% User Time (Process Class)

Description
Percentage User Time calculates the percentage of time that process threads have been executing code in User Mode. Special process boundaries have been integrated with Windows NT so that code executing in User Mode will not interfere with the Windows NT Executive, Kernel, and device drivers. Note that you may see Windows NT-related tasks in other subsystem processes in addition to seeing the Privileged Time in your own process.

If the Percentage User Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.

- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of user time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

% User Time (Processor Class)

Description
Percentage of User Time measures the percentage of time a processor spends in user mode with non-idle threads. The Percentage of User Time metric includes the amount of time that all application code and peripheral devices execute in user mode.

If the Percentage of User Time is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of user time.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Alignment Fixups/sec

Description
Alignment Fixups per Second measures the rate by which the system is able to fix alignment faults.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The alignment faults fixed per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

APC Bypasses/sec

Description
APC (Asynchronous Procedure Call) Bypasses per Second calculates the rate at which kernel APC interrupts are circumvented.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of APC bypasses per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Async Copy Reads/sec

Description

Async Copy Reads per Second measures the frequency of cache page reads that include placing a memory copy of the data from the cache on the application's buffer. The application will be able to access the disk and retrieve the page immediately.

If the value of Async Copy Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of asynchronous copy reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Async Data Maps/sec

Description

Async Data Maps per Second measures the frequency that the NTFS or HPFS file systems map a page of a file into the cache to read the page and does not wait for the cache to retrieve the page (if the page is not in the main memory.)

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of asynchronous data maps per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Async Fast Reads/sec

Description

Async Fast Reads per Second measures the frequency of cache page reads that retrieve data directly from the cache without going through the installed file system. In a typical read, the I/O requests prompt the file system to retrieve data from a file.

If the data is not in the cache, a fast read will still eliminate one invocation of the file system. The request will have immediate control of the data even if the data is not in the cache.

If the value of Async Fast Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of asynchronous fast reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Async MDL Reads/sec

Description
Async MDL (Memory Descriptor List) Reads per Second measures the frequency of cache page reads that access data using the MDL. The physical address of each page within the transfer is contained in the memory descriptor list. This information enables the Direct Memory Access (DMA) device to secure the copy. The access device will not wait for the pages to fault from the disk if the pages are not in the main memory.

If the value of Async MDL Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of asynchronous MDL reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Async Pin Reads/sec

Description

Async Pin Reads per Second measures the frequency of reading data into the cache before the data is written back to disk. When pages are read this way they become pinned in memory when the read is complete. The file system will have immediate control of the page and will be able to access the disk and retrieve the page immediately if needed. A pinned page's physical address cannot be modified.

If the value of Async Pin Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of asynchronous pin reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Available Bytes

Description
Available Bytes metric measures the real-time amount of virtual memory on the Zeroed, Free and Standby lists.

If this value is less than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The available memory in bytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Available Memory (%)

Description
Available Memory % measures the real-time amount of free memory in the percentage of total physical memory.

Data Source
Available Free Memory / Total Physical Memory * 100%

Parameters
- Warning Threshold: Threshold for warning alert. The value can be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value can be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
Available physical memory in percentage.

Recommended Frequency
5 minutes

Average Response Time (ms)

Description
Average Response Time (ms) calculates the average time (in milliseconds) of a disk transfer.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The average response time in milliseconds.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Avg. Disk Bytes/Read

Description
Average Disk Bytes / Read calculates the average number of bytes transferred from the disk during read operations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Average number of bytes transferred per read

Recommended Frequency

5 minutes

User Action

Specific to your site.

Avg. Disk Bytes/Transfer

Description

Avg. Disk Bytes/Transfer calculates the average number of bytes transferred to or from the disk during write or read operations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Disk name
- Average number of bytes transferred per transfer

Recommended Frequency
5 minutes

User Action
Specific to your site.

Avg. Disk Bytes/Write

Description
Average Disk Bytes / Write calculates the average number of bytes transferred to the disk during write operations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Number of bytes transferred per write

Recommended Frequency

5 minutes

User Action

Specific to your site.

Avg. Disk sec/Read

Description

Average Disk sec/Read calculates the average time (in seconds) of a data read from the disk.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Average disk time in seconds per read

Recommended Frequency
5 minutes

User Action
Specific to your site.

Avg. Disk sec/Transfer

Description
Average Disk Sec/Transfer calculates the average time (in seconds) of a disk transfer.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Disk name
- Average disk time in seconds per transfer

Recommended Frequency
5 minutes

User Action
Specific to your site.

Avg. Disk sec/Write

Description

Average Disk sec/Write calculates the average time (in seconds) of a data write to the disk.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Average disk time in seconds per write

Recommended Frequency

5 minutes

User Action

Specific to your site.

Bytes Received/sec

Description

Bytes Received per Second measures the rate at which bytes are received on the interface.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of bytes are received on the interface per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Bytes Sent/sec

Description
Bytes Sent per Second measures the rate at which bytes are sent on the interface.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of bytes are sent on the interface per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Bytes Total/sec

Description

Bytes Total per Second measures the rate at which bytes are sent and received on the interface.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of bytes are sent and received on the interface per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Cache Bytes

Description
Cache Bytes measures the number of bytes currently being used by the system cache. The system cache buffers data retrieved from the disk or local area network. The system cache then uses the memory that is not currently being used by any active system processes.

If Cache Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The used system cache in bytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Cache Faults/sec

Description
Cache Faults per Second measures the number of times a cache fault occurs. Cache faults are caused when the cache manager fails to find a file's page in the immediate cache and requests the memory manager to locate the page in memory or on the disk so that it can be added to the immediate cache.

If the value of Cache Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of cache faults per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Commit Limit

Description
Commit Limit measures the amount of virtual memory (in bytes) that can be committed without extending the paging files.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The memory commit limit in bytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Committed Bytes

Description

Committed Bytes measures the total amount of virtual memory (in bytes) that have been committed. Committed memory should not be confused with reserved memory. Committed memory must have available disk storage or the main memory must by large enough to contain the committed virtual memory.

If the value of Committed Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The committed memory in bytes.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Context Switches/sec

Description

Context Switches per Second measures the rate of switches among threads. Switches can occur either inside of a single process or across multiple processes. A

thread switch can happen when one thread requests information from another thread or when a higher priority thread preempts another thread. In addition to the traditional protection of User and Privileged modes, Windows NT also uses process boundaries for subsystem protection. These protection boundaries may appear in other subsystem processes in addition to the Privileged Time in the application. Switching to the subsystem process causes one Context Switch in the application thread. Switching back causes another Context Switch in the subsystem thread.

If the value of Context Switches per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The context switches per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Copy Read Hits %

Description

Copy Read Hits measures the percentage of copy read hit requests that the cache receives. Copy read hits do not require a disk read to access a page in the cache. A

copy read is a type of file read operation that allows a memory copy from a cache page to the application's buffer. The Local Area Network (LAN) Redirector, the LAN Server and the disk file systems use the copy reads for retrieving cache information.

If the value of Copy Read Hits per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of copy read hits.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Copy Reads/sec

Description

Copy Reads per Second measures the frequency of cache page reads that includes placing a memory copy of the data from the cache on the application's buffer. The Local Area Network (LAN) Redirector, the LAN Server, and the disk file systems use copy reads for retrieving cache information.

If the value of Copy Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of copy reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Current Bandwidth

Description
Current Bandwidth estimates the interface's current bandwidth in bits per second (bps). The nominal bandwidth value is given for interfaces that do not vary in bandwidth or for those where no accurate estimation can be made.

If the Current Bandwidth is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The current bandwidth in bits per second (bps).

Recommended Frequency
5 minutes

User Action
Specific to your site.

Current Disk Queue Length

Description
Current Disk Queue Length calculates the total real-time number of outstanding requests that are on the disk and are currently in service when the performance data is collected. To maintain optimal performance calculate the ratio of delayed request to the length of the disk queue minus the number of spindles on the disks. The difference should be less than 2. (Note that disk devices with multiple spindles can have multiple requests active at one time.)

If the value of Current Disk Queue Length is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Disk name
- Current disk queue length

Recommended Frequency
5 minutes

User Action
Specific to your site.

Data Flush Pages/sec

Description
Data Flush Pages per Second calculates the number of pages have been flushed to disk from the Cache. Pages are flushed when the cache approves a write-through file write request of its content to disk. Note that more than one page can be transferred for each flush operation.

If the value of Data Flush Pages per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of data flush pages per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Data Flushes

Description

Data Flushes per Second measures the frequency at which the cache has approved a write-through file write request of its content to disk. Note that for each flush operation, more than one page can be transferred.

If the value of Data Flushes per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of data flushes per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Data Map Hits %

Description
Data Map Hits calculates the percentage of Data Maps in the cache that can be resolved without retrieving a page from the disk.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of data map hits.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Data Map Pins/sec

Description
Data Map Pins per Second measures the frequency of Data Maps in the cache that caused a page to be pinned in the main memory. When a page is pinned the physical address in main memory and its virtual address in the cache cannot be modified.

If the value of Data Map Pins per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The data map pins per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Data Maps/sec

Description
Data Maps per Second measures the frequency that the NTFS or HPFS file systems map a page of a file into the cache.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of data maps per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Demand Zero Faults/sec

Description

Demand Zero Faults per Second measures the number of page faults for pages that must be filled with zeroes before the fault is resolved. If the zeroed list is not empty, the fault can be resolved by removing a page from the zeroed list.

If the value of Demand Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of demand zero faults per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Disk Bytes/sec

Description

Disk Bytes per Second calculates the frequency at which bytes are transferred to or from the disk during write or read operations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Number of bytes transferred per second

Recommended Frequency

5 minutes

User Action

Specific to your site.

Disk Read Bytes/sec

Description

Disk Read Bytes per Second calculates the frequency at which bytes are transferred from the disk during read operations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Disk name
- Number of bytes read per second

Recommended Frequency
5 minutes

User Action
Specific to your site.

Disk Reads/sec

Description
Disk Reads per Second calculates the frequency of read operations on the disk.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Number of disk reads per second

Recommended Frequency

5 minutes

User Action

Specific to your site.

Disk Transfers/sec

Description

Disk Transfers per Second calculates the frequency of read and write operations on the disk.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Number of disk transfers per second

Recommended Frequency

5 minutes

User Action

Specific to your site.

Disk Write Bytes/sec

Description

Disk Write Bytes per Second calculates the frequency at which bytes are transferred to the disk during write operations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Number of bytes written per second

Recommended Frequency

5 minutes

User Action

Specific to your site.

Disk Writes/sec

Description

Disk Writes per Second calculates the frequency of write operations on the disk.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Physical Disk(s): Filter for physical disks to be monitored, such as 0, 1, or * for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Physical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

- Disk name
- Number of disk writes per second

Recommended Frequency

5 minutes

User Action
Specific to your site.

DPC Bypasses/sec

Description
DPC (Deferred Procedure Call) Bypasses per Second calculates the average rate at which Dispatch interrupts are circumvented.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of DPC bypasses per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

DPC Rate

Description

DPC (Deferred Procedure Call) Rate calculates the average rate at which DPC objects are added to the processor's DPC queue.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The DPC rate.

Recommended Frequency

5 minutes

User Action

Specific to your site.

DPCs Queued/sec

Description

DPCs (Deferred Procedure Calls) Queued per Second measures the rate at which DPC objects are added to the processor's DPC queue.

If this rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The DPCs queued per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Elapsed Time

Description

Elapsed time measures the total amount of time (in seconds) that the process has been running.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total amount of time (in seconds) that the process has been running.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Events

Description
The Events metric measures the total number of real-time events in the computer at the time of data collection. Events are used when two or more threads wish to synchronize execution.

If the number of real-time events is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Objects".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The total number of real-time events.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Exception Dispatches/sec

Description

Exception Dispatches per Second measures the rate that the system dispatches exceptions.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of exception dispatches per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Fast Read Not Possibles/sec

Description
Fast Read Not Possibles per Second is the frequency at which calls are made by the Application Program Interface (API) to try and avoid the file system to get cache data. This metric monitors the number of times that these calls fail because the file system must be accessed.

If the value of Fast Read Not Possibles per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of fast read not possibles per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Fast Read Resource Misses/sec

Description
Fast Read Resource Misses per Second measures the frequency at which cache reads are missed due to a lack of resources to satisfy the request.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of fast read resource misses per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Fast Reads/sec

Description

Fast Reads per Second measures the frequency of cache page reads that retrieve data directly from the cache without going through the installed file system. In a typical read, the I/O requests prompt the file system to retrieve data from a file. If the data is not in the cache, a fast read will still eliminate one invocation of the file system.

If the value of Fast Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of fast reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

File Control Bytes/sec

Description

File Control Bytes per Second is the sum total of bytes transferred for all file system including file system control requests or requests for information about device characteristics or status. (Does not include read or write operations.)

If the value of File Control Bytes per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The file control bytes per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

File Control Operations/sec

Description

File Control Operations per Second is the sum total of all file system operations including file system control requests or requests for information about device characteristics or status. (Does not include read or write operations.) If the value of

File Control Operations per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The file control operations per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

File Data Operations/sec

Description
File Data Operations per Second measures the number of Read and Write operations being issued by the computer to file system devices. This metric does not measure File Control Operations.

If the value of File Data Operations per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of file data operations per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

File Read Bytes/sec

Description
File Read Bytes per Second is the sum total of bytes transferred for all the file system read operations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of file read bytes per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

File Read Operations/sec

Description

File Read Operations per Second is the sum total of all the file system read operations on the system.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The file read operations per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

File Write Bytes/sec

Description
File Write Bytes per Second is the sum total of bytes transferred for all the file system write operations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of file write bytes per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

File Write Operations/sec

Description
File Write Operations per Second is the sum total of all the file system write operations on the system.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The file write operations per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Floating Emulations/sec

Description
Floating Emulations per Second measures the rate by which the system performs floating emulations.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of floating emulations per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Free Megabytes

Description
Free Megabytes measures the available (unallocated) space on the selected disk drive in megabytes. One megabyte = 1,048,576 bytes.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Logical Disk(s): Filter for logical disks to be monitored, such as "0 ==> C:" or "0 ==> C:, 1 ==> D:" for all disks on the system. **Note:** To access the list of all available disk names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Logical Disk".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
- Disk name
- Amount of free space in megabytes

Recommended Frequency
5 minutes

User Action
Specific to your site.

Free System Page Table Entries

Description
Free system page table entries measure the number of page table entries that are not currently being used by the system.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of page table entries that are free.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Handle Count

Description

Handle Count calculates the total number of handles currently open by each thread in this process.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of handles currently open by each thread in the process.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Interrupts/sec

Description
Interrupts per Second measures the number of times the processor experiences an interrupt caused by a device. Device interruptions occur when the device completes a task or when the device requires attention. These interruptions suspend normal thread executions which can cause the processor to switch to a higher priority thread.

If Interrupts per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Processor(s): Filter for processors, such as 0, 1, or * for all processors on the system. **Note**: To access the list of available instance names, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Processor".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The interrupts per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Lazy Write Flushes/sec

Description
Lazy Write Flushes per Second measures the frequency at which the lazy write thread involves updating the disk after the page has been changed in memory. By doing this the application requesting the file change will not have to wait for the disk write to complete before proceeding. Note that more than one page can be transferred on each writer operation.

If the value of Lazy Write Flushes per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of lazy write flushes per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Lazy Write Pages/sec

Description
Lazy Write Pages per Second measures the frequency at which the lazy write thread involves updating the disk after the page has been changed in memory. By doing this the application requesting the file change will not have to wait for the disk write to complete before proceeding. Note that more than one page can be transferred on a single disk write operation.

If the value of Lazy Write Pages per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of lazy write pages per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

MDL Read Hits %

Description
MDL (Memory Descriptor List) Read Hits measures the percentage of requests that the cache receives for cache memory descriptor (MDL) list reads. MDL reads provide memory access to the cache pages without accessing the disk.

If the Percentage of MDL Read Hits is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The percentage of MDL read hits.

Recommended Frequency
5 minutes

User Action
Specific to your site.

MDL Reads/sec

Description

MDL (Memory Descriptor List) Reads per Second measures the frequency of cache page reads that access data using the MDL. The physical address of each page within the transfer is contained in the memory descriptor list. This information enables the Direct Memory Access (DMA) device to secure the copy.

If the value of MDL Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of MDL reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Mutexes

Description

The Mutexes metric measures the total number of real-time mutexes in the computer at the time of data collection. Threads use mutexes to assure only one thread is executing some section of code.

If the total number of real-time mutexes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Objects".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The total number of real-time mutexes.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Output Queue Length

Description

Output Queue Length measures the length of the output packet queue (in packets.) Performance delays occur when the output queue experiences a bottleneck

(typically when the length is longer than 2). Eliminate bottlenecks for optimal performance.

If the Output Queue Length is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The length of the output packet queue in packets.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Packets/sec

Description
Packets per Second measures the rate at which packets are sent and received on the network interface.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of packets are sent and received on the network interface per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Packets Outbound Discarded

Description
Packets Outbound Discarded measures the number of outbound packets that were chosen to be discarded (to prevent them from being transmitted) and possibly free up buffer space.

If the number of Packets Outbound Discarded is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of outbound packets that were discarded.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Packets Outbound Errors

Description

Packets Outbound Errors measures the total number of outbound packets that had errors and therefore could not be transmitted.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of outbound packets that had errors.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Packets Received/sec

Description
Packets Received per Second measures the rate at which packets are received on the network interface.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of packets are received on the network interface per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Packets Received Discarded

Description
Packets Received Discarded measures the number of inbound packets that were chosen to be discarded to prevent them from being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

If the number of Packets Received Discarded is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of packets received discard.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Packets Received Errors

Description

Packets Received Errors measures the total number of inbound packets that contained errors and prevented them from being delivered to a higher-layer protocol.

If the number of Packet Received Errors is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The total number of packets received errors.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Packets Received Non-Unicast/sec

Description

Packets Received Non-Unicast per Second measures the rate at which non-unicast (subnet broadcast or subnet multicast) packets are delivered to a higher-layer protocol.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of packets received non-unicast per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Packets Received Unicast/sec

Description

Packets Received Unicast per Second measures the rate at which (subnet) unicast packets are delivered to a higher-layer protocol.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of packets received unicast per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Packets Received Unknown

Description

Packets Received Unknown measures the total number of packets the interface received and discarded because of an unknown or unsupported protocol.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of packets received and discarded because of an unknown or unsupported protocol.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Packets Sent/sec

Description
Packets Sent per Second measures the rate at which packets are sent on the network interface.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of packets are sent on the network interface per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Packets Sent Non-Unicast/sec

Description

Packets Sent Non-Unicast per Second measures the rate at which higher-level protocols requested packets to be transmitted to non-unicast (subnet broadcast or subnet multicast) addresses. The packets sent non-unicast rate includes the packets that were discarded or not sent.

If the value of Packets Sent Non-Unicast per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available

network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of packets sent non-unicast per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Packets Sent Unicast/sec

Description
Packets Sent Unicast per Second measures the rate at which higher-level protocols requested packets to be transmitted to subnet-unicast addresses. The packets sent unicast rate includes the packets that were discarded or not sent.

If the value of Packets Sent Unicast per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Network Interface(s): Filter for network interfaces to be monitored, such as 1, or * for network interfaces on the system. **Note:** To access the list of available network interfaces, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Network Interface".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.

- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of packets sent unicast per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Page Faults/sec (Memory Class)

Description
Page Faults per Second measures the number of Page Faults in the processor. A page fault occurs when a virtual memory page is referenced by a process and that page is not in the current Working Set of the main memory.

If the value of Page Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page faults per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Page Faults/sec (Process Class)

Description
Page Faults per Second measures the rate of Page Faults by the threads executing in this process. Page faults occur when threads reference a virtual memory page that is not in currently its working set in main memory. When the page is not in the working set it cannot be fetched from disk if it is in main memory or when the shared page is being used by another process.

If the value of Page Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The page faults per second in the process.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Page File Bytes

Description

Page File Bytes measures the total number of bytes this process has used in the paging file(s). Paging files store pages of memory used by the process but are not contained in other files. Paging files are shared by all processes but if there is insufficient space in the paging files, other processes may not be able to allocate memory.

If the value of Page File Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The total number of bytes the process has used in the paging file(s).

Recommended Frequency

5 minutes

User Action

Specific to your site.

Page Reads/sec

Description

Page Reads per Second measures the number of times the disk was read to retrieve pages of virtual memory to resolve page faults.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Page Writes/sec

Description
Page Writes per Second measures the number of times pages have been written to disk because they were modified since the last retrieval.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of page writes per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Pages/sec

Description

Pages per Second measures the number of pages read from the disk or written to the disk to resolve faulty memory references. The metric calculates the sum of pages input per second plus the pages output per second. Use this metric to monitor memory thrashing and excessive paging.

If the value of Pages per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of pages input/output per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pages Input/sec

Description
Pages Input per Second measures the number of pages read from the disk to resolve faulty memory references. This is an important metric to monitor if memory thrashing and excessive paging has become a problem.

If the value of Pages Input per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of page inputs per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pages Output/sec

Description
Pages Output per Second measures the number of pages that were written to disk because the pages were modified in main memory.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of pages output per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pin Read Hits %

Description

Pin Read Hits calculates the percentage of pin requests that the cache receives. A pin read request does not require a disk read to access the page in cache. A pinned page's physical address in the cache cannot be modified. The Local Area Network (LAN) Redirector, the LAN Server, and the disk file system use pin reads to retrieve cache information.

If the value of Pin Read Hits is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert. The value must be between 0.0 and 100.0.
- Critical Threshold: Threshold for critical alert. The value must be between 0.0 and 100.0.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The percentage of pin read hits.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Pin Reads/sec

Description

Pin Reads per Second measures the frequency of reading data into the cache before the data is written back to disk. When pages are read this way they become pinned in memory when the read is complete. A pinned page's physical cache address cannot be modified.

If the value of Pin Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of pin reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Pool Nonpaged Allocs

Description

Pool Nonpaged Allocs (Allocations) is the number of times a call has been made to allocate space in the nonpaged pool. Nonpaged pool pages cannot be paged out to the paging file. As long as they are allocated they must remain in the main memory.

If the value of Pool Nonpaged Allocs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of times to allocate space in the non-paged pool.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Pool Nonpaged Bytes (Memory Class)

Description

Pool Nonpaged Bytes measures the number of bytes in the nonpaged pool. Nonpaged pool pages cannot be sorted in the paging file. As long as they are allocated, they must remain in the main memory.

If the value of Pool Nonpaged Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of bytes in the non-paged pool.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Pool Nonpaged Bytes (Process Class)

Description

Pool Nonpaged Bytes calculates the total number of bytes in the Nonpaged Pool. The Paged Pool is the area in the system memory where operating system components acquire space to accomplish tasks. Nonpaged Pool pages remain in main memory as long as they are allocated and cannot be paged out to the paging file.

If the value of Pool Nonpaged Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of bytes in the Non-paged Pool.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pool Paged Allocs

Description
Pool Paged Allocs (Allocations) is the number of times a call has been made to allocate space in the system paged pool. Paged pool pages can be paged out to the paging file when the pages are not being accessed for any sustained amount of time.

If the value of Pool Paged Allocs is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of times to allocate space in the system paged pool.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pool Paged Bytes (Memory Class)

Description
Pool Paged Bytes measures the number of bytes in the paged pool. Paged pool pages can be paged out to the paging file when not being used by the system for a sustained length of time.

If Pool Paged Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of bytes in paged pool.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pool Paged Bytes (Process Class)

Description
Pool Paged Bytes calculates the total number of bytes in the Paged Pool. The Paged Pool is the area in the system memory where operating system components acquire space to accomplish tasks. When not being accessed by the system, Paged Pool pages can be paged out to the paging file.

If the value of Pool Paged Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of bytes in the Paged Pool.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Pool Paged Resident Bytes

Description
Pool Paged Resident Bytes measures the size of paged pool bytes that reside in the main memory. The pool paged resident bytes value indicates the actual cost of the paged pool allocation since it is currently in use and it uses real (physical) memory.

If the value of Pool Paged Resident Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The size of paged pool bytes that reside in the main memory.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Private Bytes

Description

Private Bytes calculates the total number of bytes allocated by the process that cannot be shared with other processes.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The total number of bytes allocated by the process that cannot be shared with other processes.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Processes

Description

Processes calculates the total number of real-time processes in the computer at the time of data collection. Each process represents the running of a program.

If the number of Processes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value

specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Objects".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of real-time processes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Processor Queue Length

Description
Processor Queue Length measures the number of threads in the current processor queue (not the threads that are currently executing.) Note that the Processor Queue Length metric is a real-time count of threads and not an average count over time.

If the Processor Queue Length is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of threads in the current processor queue.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Read Aheads/sec

Description

Read Aheads per Second measures the frequency at which cache reads detect sequential file access. Read aheads reduce overhead access by enabling the data to be transferred in larger blocks than those requested by the application.

If the value of Read Aheads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of read aheads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Sections

Description
The Sections metric measures the total number of real-time sections in the computer at the time of data collection. A section is a portion of virtual memory created by a process for data storage. Processes may share sections with other processes.

If the total number of real-time sections is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Objects".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of real-time sections.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Semaphores

Description
The Semaphores metric measures the total number of real-time semaphores in the computer at the time of data collection. Semaphores are used by threads to obtain exclusive access to data structures that threads share with other threads.

If the total number of real-time semaphores is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Objects".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of real-time semaphores.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Sync Copy Reads/sec

Description

Sync Copy Reads per Second measures the frequency of cache page reads that include placing a copy of the data from the cache on the application's buffer. The file system will not be able to access the disk and retrieve the page until the copy operation is complete.

If the value of Sync Copy Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of sync copy reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Sync Data Maps/sec

Description

Sync Data Maps per Second measures the frequency that the NTFS or HPFS file systems map a page of a file into the cache and waits for the cache to retrieve the page (if the page is not in the main memory.)

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of sync data maps per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Sync Fast Reads/sec

Description

Sync Fast Reads per Second measures the frequency of cache page reads that retrieve data directly from the cache without going through the installed file system. In a typical read, the I/O requests prompt the file system to retrieve data from a file.

If the data is not in the cache, a fast read will still eliminate one invocation of the file system. The request will not wait until the data has been retrieved from disk if the data is not in the cache.

If the value of Sync Fast Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of sync fast reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Sync MDL Reads/sec

Description
Sync MDL (Memory Descriptor List) Reads per Second measures the frequency of cache page reads that access data using the MDL. The physical address of each page within the transfer is contained in the memory descriptor list. This information enables the Direct Memory Access (DMA) device to secure the copy. The access device will wait for the pages to fault from the disk if the pages are not in the main memory.

If the value of Sync MDL Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of sync MDL reads per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Sync Pin Reads/sec

Description

Sync Pin Reads per Second measures the frequency of reading data into the cache before the data is written back to disk. When pages are read this way they become pinned in memory when the read is complete. When the page is pinned in the cache the file system can regain control of the page. Until the page is pinned in cache, however, the file system cannot access the disk and retrieve the page. A pinned page's physical address in the cache cannot be changed.

If the value of Sync Pin Reads per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences

exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Cache: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Cache".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of sync pin reads per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Cache Resident Bytes

Description
System Cache Resident Bytes measures the total number of bytes residing in the disk cache.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The total number of bytes residing in the disk cache.

Recommended Frequency

5 minutes

User Action

Specific to your site.

System Calls/sec

Description

Systems Calls per Second measures the frequency of calls to system service routines that perform basic scheduling and synchronizing of activities on the computer. These routines also provide access to non-graphical devices, memory management, and name space management.

If the value of System Calls per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of system calls per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Code Resident Bytes

Description
System Code Resident Bytes measures the number of bytes of system code currently residing in the main memory.

If this value is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The size of system code residing in the main memory in bytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Code Total Bytes

Description
System Code Total Bytes monitors the ntoskrnl.exe, hal.dll, and the boot drivers and file systems loaded by the ntldr/osloader for the total number of bytes of the pageable pages.

If System Code Total Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total system code size in bytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

System Driver Resident Bytes

Description

System Driver Resident Bytes measures the total number of system driver bytes residing in the core memory. The returned value is considered the code working set of pageable drivers.

If the value of System Driver Resident Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The total number of system driver bytes residing in the core memory.

Recommended Frequency

5 minutes

User Action

Specific to your site.

System Driver Total Bytes

Description

System Driver Total Bytes monitors all of the system driver devices and returns the total number of pageable pages currently in the devices.

If the value of System Driver Total Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of pageable pages currently in the devices in bytes.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Thread Count

Description
Thread Count measures the number of threads in the process that are currently active. Threads are responsible for executing instructions (basic units of application work). Every active process has at least one thread.

If the Thread Count is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of threads in the process that are currently active.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Threads

Description
The Threads metric measures the total number of real-time threads in the computer at the time of data collection. (Threads execute instructions in a processor.)

If the number of Threads is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Objects".

- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total number of real-time threads.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Total APC Bypasses/sec

Description
Total APC (Asynchronous Procedure Call) Bypasses per Second measures the overall rate at which APC interrupts were circumvented across all processors.

If this rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total APC bypasses per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Total DPC Bypasses/sec

Description
Total DPC (Deferred Procedure Call) Bypasses per Second measures the rate at which Dispatch Interrupts were circumvented across all platforms.

If this rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total DPC bypasses per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Total DPC Rate

Description

Total DPC (Deferred Procedure Call) Rate is the average speed (measured in seconds) by which DPC objects are added to the processor's DPC queue.

If the Total DPC Rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The total DPC rate.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Total DPCs Queued/sec

Description

Total DPCs (Deferred Procedure Calls) Queued per Second measures the rate at which objects are added to the processor's DPC queue.

If this rate is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The total DPCs queued per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Total Interrupts/sec

Description
Total Interrupts per Second measures the rate that the computer is handling interruptions from system devices such as the mouse, network cards, and system clocks. This metric also indicates how busy those devices are in the overall system environment.

If the value of Total Interrupts per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- System: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "System".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of total interrupts per second.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Transition Faults/sec

Description
Transition Faults per Second measures the number of page faults that have been resolved by recovering pages that were being written to disk when the page fault occurred. These pages can be recovered without any additional disk activity.

If the value of Transition Faults per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output

The number of transition faults per second.

Recommended Frequency

5 minutes

User Action

Specific to your site.

Virtual Bytes

Description

Virtual Bytes calculates the current size (in bytes) of the virtual address space being used by a process. Using too much virtual memory may limit the ability to load libraries. Note that using virtual address space is not an indication that you are also using disk or main memory pages.

If the value of Virtual Bytes is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source

The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters

- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.

- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The current size in bytes of the virtual address space used by the process.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Working Set

Description
Working Set measures total number of bytes currently in the Working Set of the process. The Working Set is the set of memory pages recently accessed by the threads in the process. If the system's free memory rises above a threshold, the pages are left in the Working Set even if they are not in use. If the system's free memory falls below a threshold, the pages are trimmed from Working Sets. If the memory pages are needed they will then be soft-faulted back into the Working Set before they leave main memory.

If the value of Working Set is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Process(es): Filter for processes to be monitored, such as vppdc, dbsnmp, or * for all processes on the system.
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of bytes currently in the Working Set of the process.

Recommended Frequency
5 minutes

User Action
Specific to your site.

Write Copies/sec

Description
Write Copies per Second measures the number of page faults that have been resolved by making a copy or the page when an attempt is made to write to the page.

If the value of Write Copies per Second is greater than or equal to the threshold values specified by the threshold arguments, and the number of occurrences exceeds the value specified in the "Number of Occurrences" parameter, then a warning or critical alert is generated.

Data Source
The data for this item was retrieved from a performance counter exposed in the system registry.

Parameters
- Memory: Default is "NT Operating System". **Note:** To get the available instance name, use Performance Manager or Capacity Planner and connect to the target node, then click on the class "Memory".
- Warning Threshold: Threshold for warning alert.
- Critical Threshold: Threshold for critical alert.
- Number of Occurrences: The number of consecutive occurrences. The default is 5.

Output
The number of write copy faults per second.

Recommended Frequency
5 minutes

User Action

Specific to your site.

8

Management Pack for Oracle Applications Event Tests

The Oracle Applications Advanced Event Tests include a library of applications-specific event tests which are provided for lights-out event monitoring and problem detection of the Applications subsystem.

Note: To successfully use the event tests, the node credentials on Windows NT must be for a user with the "logon as batch" privilege.

The Application subsystem specific events notify administrators of fault, performance, and space problems. The event tests according to category are:

Note: The Fault and Performance event tests are specific to the version of the Agent. The Space event test is independent of the version of the Agent. To determine the version of the Agent, go to the Enterprise Manager Console and find the node on which the concurrent manager is running. Right mouse click on the node target and select "Properties".

The event tests for release 8.1.6 and earlier targets are included for backward compatibility purposes. It is highly encouraged that you upgrade to the new event tests because the old event tests may not be supported in future releases of the Management Pack for Oracle Applications.

Summary of Applications Event Tests

The following tables list the Applications event tests. The full descriptions of the individual event tests follow the tables. The event tests are in alphabetical order.

Table 8–1 Applications Fault Management Event Tests

Event Test	Description
Concurrent Manager UpDown	This event test monitors the state of the Internal Concurrent Manager (ICM). If the ICM goes down, an alert is generated.
CRM Waiting on a Lock	This event test checks whether the Conflict Resolution Manager is waiting to get a lock. If the lock wait time reaches a specified amount of time, a warning is issued.
ICM Waiting on a Lock	This event test checks whether the Internal Concurrent Manager is waiting to get a lock. If the lock wait time reaches a specified amount of time, a warning alert is issued.
Request Error Rate	This event test monitors the error rate of concurrent requests. When the error rate reaches the threshold parameters set by the user, a warning or critical alert is generated.
Request Warning Rate	This event test monitors the warning rate of concurrent requests. When the warning rate reaches the threshold parameters set by the user, a warning or critical alert is generated.
Unresponsive Concurrent Manager	This event test checks the responsiveness of the concurrent managers. If any of your concurrent managers are down at the beginning of the test and are still down after the number of seconds you entered as a parameter, they are considered unresponsive. In other words, this event test tells you if the concurrent manager is having trouble coming back up or can not be brought back online, giving you the opportunity to resolve the problem. The difference between the Unresponsive Concurrent Manager event and the Concurrent Manager UpDown event is that the Concurrent Manager UpDown event notifies you when the internal concurrent manager has gone down or comes back up. The Unresponsive Concurrent Manager event test notifies you if any of the other concurrent managers are down over the time period you specify.

Table 8–2 Applications Performance Management Event Tests

Event Test	Description
Inactive Request Pending	This event test monitors the state of the requests submitted to the Concurrent Manager(s). If any of the requests is in an inactive state, an alert is generated.
Pending Concurrent Request Backlog	This event test monitors for concurrent requests that have been in the pending state for a time period exceeding the threshold, and triggers an alert if they exceed the 'total concurrent requests' threshold.
Request Pending Time	This event test monitors for requests that have been in the pending state for a time period exceeding the threshold set by the user.
Runalone Request Submitted	This event test monitors the state of the requests submitted to the Concurrent Manager(s). If any of the requests is in a run alone state, a warning is generated.

Table 8–3 Applications Space Management Event Tests

Event Test	Description
Concurrent Manager Disk Free	This event test monitors the growth rates of the log, output, and other partitions for the concurrent requests. A check box is provided to select any or all of these partitions, or any other partition on the concurrent processing server node.

Table 8–4 Applications Fault Management Event Tests for V8.1.6 and Earlier Agents

Event Test	Description
Concurrent Manager UpDown	This event test monitors the state of the Internal Concurrent Manager (ICM). If the ICM goes down, an alert is generated.
CRM Waiting on a Lock	This event test checks whether the Conflict Resolution Manager is waiting to get a lock. If the lock wait time reaches a specified amount of time, a warning is issued.
ICM Waiting on a Lock	This event test checks whether the Internal Concurrent Manager is waiting to get a lock. If the lock wait time reaches a specified amount of time, a warning alert is issued.
Request Error Rate	This event test monitors the error rate of concurrent requests. When the error rate reaches the threshold parameters set by the user, a warning or critical alert is generated.
Request Warning Rate	This event test monitors the warning rate of concurrent requests. When the warning rate reaches the threshold parameters set by the user, a warning or critical alert is generated.

Table 8–5 Performance Management Event Tests for V8.1.6 and Earlier Agents

Event Test	Description
Inactive Request Pending	This event test monitors the state of the requests submitted to the Concurrent Manager(s). If any of the requests is in an inactive state, an alert is generated.
Pending Concurrent Request Backlog	This event test monitors for concurrent requests that have been in the pending state for a time period exceeding the threshold, and triggers an alert if they exceed the 'total concurrent requests' threshold.
Request Pending Time	This event test monitors for requests that have been in the pending state for a time period exceeding the threshold set by the user.
Runalone Request Submitted	This event test monitors the state of the requests submitted to the Concurrent Manager(s). If any of the requests is in a runalone request, a warning is generated.

The Oracle Applications event library also includes node events. See Chapter 3, "Compaq Tru64 Event Tests", Chapter 4, "HP-UX Event Tests", Chapter 5, "IBM AIX Event Tests", Chapter 6, "Solaris Event Tests", and Chapter 7, "Windows NT Event Tests" for listings of the node-specific event tests.

For more information on submitting or scheduling events, see the *Oracle Enterprise Manager Administrator's Guide.* Pay special attention to the event frequency value, which can be set on the General tab of the Create Event panel. This value

determines the frequency of polling for event occurrences. The default value is every 60 seconds, but for many application management events, you may wish to choose larger values, for better performance and a lower overall impact on system resources.

Note: To expand the Intelligent Agent messages related to the Management Pack for Oracle Applications, at the system prompt from the Agent's Oracle home type: oerr <*facility*> <*message number*> where <*facility*> is **smamp**. For example:

oerr smamp 6001

Cause: Failed to open a cursor.

Action: Verify that the maximum cursors limit has not been exceeded.

Before running any program from the command line (UNIX or Windows NT), verify that all the correct values are present in the necessary environment variables, for example, ORACLE_HOME and PATH.

Descriptions of Applications Event Tests

The Applications event tests for release 9*i* are listed in alphabetical order.

Concurrent Manager Disk Free

This event test monitors the growth rates of the log, output, and other partitions for the concurrent requests. A check box is provided to select any or all of these partitions, or any other partition on the concurrent processing server node.

Note: This event test requires the Application environment (APPLSYS.env) file which is located in the Application code base (APPL_TOP).

Parameters

1. Critical threshold for log: Free space threshold in percentage. Default is 30%.
2. Warning threshold for log: Free space threshold in percentage. Default is 50%.

3. Critical threshold for output: Free space threshold in percentage. Default is 30%.
4. Warning threshold for output: Free space threshold in percentage. Default is 50%.
5. Name of partition. (* is not a supported name.)
6. Critical threshold for other partitions: Free space threshold in percentage. Default is 30%.
7. Warning threshold for other partitions: Free space threshold in percentage. Default is 50%.

Output
Partition name and space available in percentage on the partition.

Default Frequency
60 seconds.

User Action
Purge the log or output files.

Note: You can configure the Run OS Command job task as a fixit job to remove the log/output files from the Oracle Applications APPL_TOP.

See the *Oracle Enterprise Manager Administrator's Guide* for more information on configuring job tasks.

Concurrent Manager UpDown

This event test monitors the state of the Internal Concurrent Manager (ICM). If the ICM goes down, an alert is generated.

Parameters
None.

Output
None.

Default Frequency
60 seconds.

User Action

Submit a standalone concurrent manager startup job when the event issues an alert. The startup concurrent manager job could also be configured as a fix-it job to automatically restart the ICM when it goes down.

CRM Waiting on a Lock

This event test checks whether the Conflict Resolution Manager is waiting to get a lock. If the lock wait time reaches a specified amount of time, a warning is issued.

Parameters

1. Critical threshold: Lock wait time (in minutes) for a critical alert. Default is 3 minutes.
2. Warning threshold: Lock wait time (in minutes) for a warning alert. Default is 2 minutes.

> **Note:** Threshold values must be between 2 and 32 minutes.

Output

- Session identification number.
- Operating system process identification number.
- Lock mode.
- Machine name.
- Terminal name for the locking session.

Default Frequency

60 seconds.

User Action

Locate the session that is blocking the Conflict Resolution Manager and determine if the session can be deleted.

> **Note:** A fixit job could be registered to automatically delete the blocking session when the event is triggered.

ICM Waiting on a Lock

This event test checks whether the Internal Concurrent Manager is waiting to get a lock. If the lock wait time reaches a specified amount of time, a warning alert is issued.

Parameters

1. Critical threshold: Lock wait time (in minutes) for a critical alert. Default is 3 minutes.
2. Warning Threshold: Lock wait time (in minutes) for a warning alert. Default is 2 minutes.

> **Note:** Threshold values must be between 2 and 32 minutes.

Output

- Session identification number.
- Operating system process identification number.
- Lock mode.
- Machine name.
- Terminal name for the locking session.

Default Frequency

60 seconds.

User Action

Locate the session that is blocking the Internal Concurrent Manager and determine if the session can be deleted.

> **Note:** A fixit job could be registered to automatically delete the blocking session when the event is triggered.

Inactive Request Pending

This event test monitors the state of the requests submitted to the Concurrent Manager(s). If any of the requests is in an inactive state, an alert is generated.

Parameters

1. Monitor Field: Specify or exclude certain concurrent programs from monitoring. Choose one of the following: All Concurrent Programs, All Except These Concurrent Programs, or Only These Specific Concurrent Programs. The default is to monitor all concurrent programs.
2. List Field: Type the application name and concurrent program name for which the event will filter or exclude from monitoring. These names can be found in the Oracle Applications Manager. The default is empty and disabled.

Output

- The number of inactive requests in the concurrent manager(s) queue.
- Table containing the concurrent programs that violated the event test. The columns in the table are: Request ID, Requested By, Application Name, Concurrent Program Name, and Hours Runalone.

Default Frequency

60 seconds.

User Action

Locate the inactive request and remove it from the queue.

Pending Concurrent Request Backlog

This event test monitors for concurrent requests that have been in the pending state for a time period exceeding the threshold, and triggers an alert if they exceed the 'total concurrent requests' threshold.

Parameters

1. Monitor Field: Specify or exclude certain concurrent programs from monitoring. Choose one of the following: All Concurrent Programs, All Except These Concurrent Programs, or Only These Specific Concurrent Programs. The default is to monitor all concurrent programs.
2. List Field: Type the application name and concurrent program name for which the event will filter or exclude from monitoring. These names can be found in the Oracle Applications Manager. The default is empty and disabled.
3. Threshold for total number of requests pending: Number of requests pending in the queue. Default is 1.
4. Time Threshold (in minutes) for including requests in the pending queue backlog. Default is 1 minute.

Output

- Number of requests currently pending.
- Table containing the concurrent programs that violated the event test. The columns in the table are: Request ID, Requested By, Application Name, Concurrent Program Name, and Hours Runalone.
- Length of time the requests has been pending in the queue.

Default Frequency

60 seconds.

User Action

Increase the number of concurrent processes to handle the load.

Request Error Rate

This event test monitors the error rate of concurrent requests. When the error rate reaches the threshold parameters set by the user, a warning or critical alert is generated.

Parameters

1. Monitor Field: Specify or exclude certain concurrent programs from monitoring. Choose one of the following: All Concurrent Programs, All Except These Concurrent Programs, or Only These Specific Concurrent Programs. The default is to monitor all concurrent programs.
2. List Field: Type the application name and concurrent program name for which the event will filter or exclude from monitoring. These names can be found in the Oracle Applications Manager. The default is empty and disabled.
3. Critical threshold: Percentage of requests marked with errors for critical alert. Default is 10%.
4. Warning threshold: Percentage of requests marked with errors for warning alert. Default is 5%.

Output

Percentage of requests with errors.

Default Frequency

60 seconds.

User Action

Review the Request Log files in the APPL_TOP/log directory to determine which requests need to be corrected.

Request Pending Time

This event test monitors for requests that have been in the pending state for a time period exceeding the threshold set by the user.

Parameters

1. Monitor Field: Specify or exclude certain concurrent programs from monitoring. Choose one of the following: All Concurrent Programs, All Except These Concurrent Programs, or Only These Specific Concurrent Programs. The default is to monitor all concurrent programs.
2. List Field: Type the application name and concurrent program name for which the event will filter or exclude from monitoring. These names can be found in the Oracle Applications Manager. The default is empty and disabled.
3. Hours pending: Number of hours the request has been pending. Default is 1 hour.
4. Minutes pending: Number of minutes the request has been pending. Default is 30 minutes.

Output

- Number of hours or minutes that the request has been pending.
- Table containing the concurrent programs that violated the event test. The columns in the table are: Request ID, Requested By, Application Name, Concurrent Program Name, and Hours Runalone.

Default Frequency

60 seconds.

User Action

Check to see if the queue is being serviced actively. Increase the processes for the queue manager to balance the load, if necessary.

Request Warning Rate

This event test monitors the warning rate of concurrent requests. When the warning rate reaches the threshold parameters set by the user, a warning or critical alert is generated.

Parameters

1. Monitor Field: Specify or exclude certain concurrent programs from monitoring. Choose one of the following: All Concurrent Programs, All Except These Concurrent Programs, or Only These Specific Concurrent Programs. The default is to monitor all concurrent programs.
2. List Field: Type the application name and concurrent program name for which the event will filter or exclude from monitoring. These names can be found in the Oracle Applications Manager. The default is empty and disabled.
3. Critical threshold: Percentage of requests marked for critical alert. Default is 10%.
4. Warning threshold: Percentage of requests marked for warning alert. Default is 5%.

Output

Percentage of requests with warnings.

Default Frequency

60 seconds.

User Action

Review the Request Log files in the APPL_TOP/log directory to determine which requests need to be corrected.

Run Alone Request Submitted

This event test monitors the state of the requests submitted to the Concurrent Manager(s). If any of the requests is in a run alone state, a warning is generated.

Parameters

1. Monitor Field: Specify or exclude certain concurrent programs from monitoring. Choose one of the following: All Concurrent Programs, All Except These Concurrent Programs, or Only These Specific Concurrent Programs. The default is to monitor all concurrent programs.
2. List Field: Type the application name and concurrent program name for which the event will filter or exclude from monitoring. These names can be found in the Oracle Applications Manager. The default is empty and disabled.

Output

- The number of run alone requests in the concurrent manager(s) queue.

- Table containing the concurrent programs that violated the event test. The columns in the table are: Request ID, Requested By, Application Name, Concurrent Program Name, and Hours Runalone.

Default Frequency
60 seconds.

User Action
Determine whether or not the run alone request submitted is necessary. If it is not, the request should be deleted so that other requests can be processed.

Unresponsive Concurrent Manager

This event test checks the responsiveness of the concurrent managers. If any of your concurrent managers are down at the beginning of the test and are still down after the number of seconds you entered as a parameter, they are considered unresponsive.

In other words, this event test tells you if the concurrent manager is having trouble coming back up or can not be brought back online, giving you the opportunity to resolve the problem.

The difference between the Unresponsive Concurrent Manager event and the Concurrent Manager UpDown event is that the Concurrent Manager UpDown event notifies you when the internal concurrent manager has gone down or comes back up. The Unresponsive Concurrent Manager event test notifies you if any of the other concurrent managers are down over the time period you specify.

Parameters
Unresponsive Seconds: Type the number of seconds for the time period. This value should be roughly equivalent to the time taken for 2 PMON (Process Monitor) cycles. Calculate this value by multiplying the PMON value by the SLEEP value. The default number of iterations for PMON is 20 and the default number of sleep seconds is 60. Therefore the default is 2400 seconds (2*20*60).

Descriptions of Applications Event Tests for V8.1.6 and Earlier Agents

The Applications event tests for v8.1.6 and earlier agents are listed in alphabetical order.

Concurrent Manager UpDown (for V8.1.6 and Earlier Agents)

This event test monitors the state of the Internal Concurrent Manager (ICM). If the ICM goes down, an alert is generated.

Parameters
None.

Output
None.

Default Frequency
60 seconds.

User Action
Submit a standalone concurrent manager startup job when the event issues an alert. The startup concurrent manager job could also be configured as a fix-it job to automatically restart the ICM when it goes down.

CRM Waiting on a Lock (for V8.1.6 and Earlier Agents)

This event test checks whether the Conflict Resolution Manager is waiting to get a lock. If the lock wait time reaches a specified amount of time, a warning is issued.

Parameters

1. Critical threshold: Lock wait time (in minutes) for a critical alert. Default is 3 minutes.
2. Warning threshold: Lock wait time (in minutes) for a warning alert. Default is 2 minutes.

> **Note:** Threshold values must be between 2 and 32 minutes.

Output

- Session identification number.
- Operating system process identification number.
- Lock mode.
- Machine name.
- Terminal name for the locking session.

Default Frequency
60 seconds.

User Action
Locate the session that is blocking the Conflict Resolution Manager and determine if the session can be deleted.

> **Note:** A fixit job could be registered to automatically delete the blocking session when the event is triggered.

ICM Waiting on a Lock (for V8.1.6 and Earlier Agents)

This event test checks whether the Internal Concurrent Manager is waiting to get a lock. If the lock wait time reaches a specified amount of time, a warning alert is issued.

Parameters
1. Critical threshold: Lock wait time (in minutes) for a critical alert. Default is 3 minutes.
2. Warning Threshold: Lock wait time (in minutes) for a warning alert. Default is 2 minutes.

> **Note:** Threshold values must be between 2 and 32 minutes.

Output
- Session identification number.
- Operating system process identification number.
- Lock mode.
- Machine name.
- Terminal name for the locking session.

Default Frequency
60 seconds.

User Action
Locate the session that is blocking the Internal Concurrent Manager and determine if the session can be deleted.

Note: A fixit job could be registered to automatically delete the blocking session when the event is triggered.

Inactive Request Pending (for V8.1.6 and Earlier Agents)

This event test monitors the state of the requests submitted to the Concurrent Manager(s). If any of the requests is in an inactive state, an alert is generated.

Parameters

None.

Output

The number of inactive requests in the concurrent manager(s) queue.

Default Frequency

60 seconds.

User Action

Locate the inactive request and remove it from the queue.

Pending Concurrent Request Backlog (for V8.1.6 and Earlier Agents)

This event test monitors for concurrent requests that have been in the pending state for a time period exceeding the threshold, and triggers an alert if they exceed the 'total concurrent requests' threshold.

Parameters

1. Threshold for total number of requests pending: Number of requests pending in the queue. Default is 1.
2. Time Threshold (in minutes) for including requests in the pending queue backlog. Default is 1 minute.

Output

- Number of requests currently pending.
- Length of time the requests has been pending in the queue.

Default Frequency

60 seconds.

User Action

Increase the number of concurrent processes to handle the load.

Request Error Rate (for V8.1.6 and Earlier Agents)

This event test monitors the error rate of concurrent requests. When the error rate reaches the threshold parameters set by the user, a warning or critical alert is generated.

Parameters

1. Critical threshold: Percentage of requests marked with errors for a critical alert. Default is 10%.
2. Warning threshold: Percentage of requests marked with errors for a warning alert. Default is 5%.

Output

Percentage of requests with errors.

Default Frequency

60 seconds.

User Action

Review the Request Log files in the APPL_TOP/log directory to determine which requests need to be corrected.

Request Pending Time (for V8.1.6 and Earlier Agents)

This event test monitors for requests that have been in the pending state for a time period exceeding the threshold set by the user.

Parameters

1. Hours pending: Number of hours the request has been pending. Default is 1 hour.
2. Minutes pending: Number of minutes the request has been pending. Default is 30 minutes.

Output

Number of hours or minutes that the request has been pending.

Default Frequency

60 seconds.

User Action

Check to see if the queue is being serviced actively. Increase the processes for the concurrent manager to balance the load, if necessary.

Request Warning Rate (for V8.1.6 and Earlier Agents)

This event test monitors the warning rate of concurrent requests. When the warning rate reaches the threshold parameters set by the user, a warning or critical alert is generated.

Parameters

1. Critical threshold: Percentage of requests marked for critical alert. Default is 10%.
2. Warning threshold: Percentage of requests marked for warning alert. Default is 5%.

Output

Percentage of requests with warnings.

Default Frequency

60 seconds.

User Action

Review the Request Log files in the APPL_TOP/log directory to determine which requests need to be corrected.

Run Alone Request Submitted (for V8.1.6 and Earlier Agents)

This event test monitors the state of the requests submitted to the Concurrent Manager(s). If any of the requests is in a runalone request, a warning is generated.

Parameters

None.

Output

The number of run alone requests in the concurrent manager(s) queue.

Default Frequency

60 seconds.

User Action

Determine whether or not the runalone request submitted is necessary. If it is not, the request should be deleted so that other requests can be processed.

9

SAP Event Tests

The Oracle Management Pack for SAP R/3 provides SAP event tests and node event tests. Most of these event tests can be customized with user-defined thresholds and monitoring intervals. The user can establish an event-metric threshold and an occurrence threshold. Event-metric thresholds can be set at a warning level and at an alert level. When the thresholds are met or exceeded, the user is notified. The user can specify how often the Event System should check for the existence of an exceeded event-metric threshold.

For information on using the Event System, see the *Oracle Enterprise Manager Administrator's Guide.*

Summary of SAP Event Tests

The following table lists the SAP event tests. The full descriptions of the individual event tests follow the tables. The event tests are in alphabetical order.

Table 9–1 SAP Event Tests

Event Test	Description
Bad Buffer Quality	This event test checks for the buffer quality of SAP buffers. Performance of an SAP application instance will deteriorate when buffer hit ratio decreases. If the percentage of the buffer hit ratio is lower than the value specified in the threshold arguments, a warning or an alert is generated.
Bad Response Time	This event test checks for the response times of dialog work processes. The response time of dialog work processes gives a good overview of the system performance. If the response time exceeds the values specified in the threshold arguments, then a warning or alert is generated. When you create this event test, on the General page of the Create Event dialog box, choose only one SAP R/3 instance with which to populate the Monitored Destinations list.

Table 9–1 SAP Event Tests (Cont.)

Event Test	Description
Extended Memory Too Small	This event test checks for the size of the used extended memory. If the percentage of used in-memory extended memory increases the values specified in the threshold arguments, then a warning or alert is generated. When you create this event test, on the General page of the Create Event dialog box, choose only one SAP R/3 instance with which to populate the Monitored Destinations list.
In-Memory Roll Area Too Small	This event test checks for the size of the used roll area. If the percentage of used in-memory roll area exceeds the values specified in the threshold arguments, then a warning or alert is generated. When you create this event test, on the General page of the Create Event dialog box, choose only one SAP R/3 instance with which to populate the Monitored Destinations list.
In-Memory Page Area Too Small	This event test checks for the size of the used page area. If the percentage of used in-memory page area exceeds the values specified in the threshold arguments, then a warning or alert is generated. When you create this event test, on the General page of the Create Event dialog box, choose only one SAP R/3 instance with which to populate the Monitored Destinations list.

Descriptions of SAP Event Tests

This section describes the SAP event tests that are provided with the Oracle Management Pack for SAP R/3. The SAP event tests can only be registered on SAP R/3 services. To register an SAP event test on an SAP R/3 service, the 8.1.7 Intelligent Agent must be running on the NT proxy machine that refers to the SAP R/3 system in its sap.conf file. See the *Getting Started with the Oracle Management Pack for SAP R/3* for more information about configuring the NT proxy machine and the sap.conf file.

Note that in the Oracle Enterprise Manager console you must specify preferred credentials for any service on which you want to register events. See the *Getting Started with the Oracle Management Pack for SAP R/3* for more information on specifying preferred credentials.

Bad Buffer Quality

This event test checks for the buffer quality of SAP buffers. Performance of an SAP application instance will deteriorate when buffer hit ratio decreases. If the percentage of the buffer hit ratio is lower than the value specified in the threshold arguments, a warning or an alert is generated.

Parameters

1. SAP buffer name: Enter the name of the buffer to be monitored. The valid buffer names are:
   - CALE

- MDH
- CUA
- SNTAB
- PRES
- FTAB
- IRBD
- TABL
- TABLP
- PXA
- EIBUF
- TTAB

2. Alert threshold: Threshold value for alert (%). Default is 90%.
3. Warning threshold: Threshold value for warning (%). Default is 95%.

Output

- The name of the buffer
- Current buffer quality (%)

Default Frequency

60 seconds

User Action

Check the configuration of the application server and increase (if possible) the buffer that caused the trouble.

Bad Response Time

This event test checks for the response times of dialog work processes. The response time of dialog work processes gives a good overview of the system performance. If the response time exceeds the values specified in the threshold arguments, then a warning or alert is generated.

When you create this event test, on the General page of the Create Event dialog box, choose only one SAP R/3 instance with which to populate the Monitored Destinations list.

Parameters

1. Response Time Data: Enter the name of the SAP R/3 instance that you selected on the General page of the Create Event dialog box in the following format:

   smpsmn3_AT3_00

   In this format, smpsmn3 is the node name of the SAP R/3 message server, AT3 is the SAP R/3 system ID, and 00 is the system number of the SAP R/3 instance.

2. Alert threshold: Threshold value for alert (sec). Default is 4 sec.

3. Warning threshold: Threshold value for warning (sec). Default is 2 sec.

Output

- Application instance name
- Current response time

Default Frequency

60 seconds

User Action

Check the configuration of the application server.

Extended Memory Too Small

This event test checks for the size of the used extended memory. If the percentage of used in-memory extended memory increases the values specified in the threshold arguments, then a warning or alert is generated.

When you create this event test, on the General page of the Create Event dialog box, choose only one SAP R/3 instance with which to populate the Monitored Destinations list.

Parameters

1. SAP R/3 Memory Data: Enter the name of the SAP R/3 instance that you selected on the General page of the Create Event dialog box in the following format:

   smpsmn3_AT3_00

   In this format, smpsmn3 is the node name of the SAP R/3 message server, AT3 is the SAP R/3 system ID, and 00 is the system number of the SAP R/3 instance.

2. Alert threshold: Threshold value for alert (%). Default is 100%.
3. Warning threshold: Threshold value for warning (%). Default is 90%.

Output

- Application instance name
- Current used space in percentage

Default Frequency

60 seconds.

User Action

Check the configuration of the application server and increase the size of the extended memory.

In-Memory Roll Area Too Small

This event test checks for the size of the used roll area. If the percentage of used in-memory roll area exceeds the values specified in the threshold arguments, then a warning or alert is generated.

When you create this event test, on the General page of the Create Event dialog box, choose only one SAP R/3 instance with which to populate the Monitored Destinations list.

Parameters

1. SAP R/3 Memory Data: Enter the name of the SAP R/3 instance that you selected on the General page of the Create Event dialog box in the following format:

   smpsmn3_AT3_00

   In this format, smpsmn3 is the node name of the SAP R/3 message server, AT3 is the SAP R/3 system ID, and 00 is the system number of the SAP R/3 instance.
2. Alert threshold: Threshold value for alert (%). Default is 100%.
3. Warning threshold: Threshold value for warning (%). Default is 90%.

Output

- Application instance name
- Current used space in percentage

Default Frequency
60 seconds.

User Action
Check the configuration of the application server and increase the size of the roll area.

In-Memory Page Area Too Small

This event test checks for the size of the used page area. If the percentage of used in-memory page area exceeds the values specified in the threshold arguments, then a warning or alert is generated.

When you create this event test, on the General page of the Create Event dialog box, choose only one SAP R/3 instance with which to populate the Monitored Destinations list.

Parameters
1. SAP R/3 Memory Data: Enter the name of the SAP R/3 instance that you selected on the General page of the Create Event dialog box in the following format:

   smpsmn3_AT3_00

   In this format, smpsmn3 is the node name of the SAP R/3 message server, AT3 is the SAP R/3 system ID, and 00 is the system number of the SAP R/3 instance.
2. Alert threshold: Threshold value for alert (%). Default is 100%.
3. Warning threshold: Threshold value for warning (%). Default is 90%.

Output
- Application instance name
- Current used space in percentage

Default Frequency
60 seconds.

User Action
Check the configuration of the application server and increase the size of the page area.

10

e-Business Event Tests

The e-Business Tools advanced event tests are provided for lights-out event monitoring and problem detection of the HTTP server.

Aside from the basic up / down event tests provided for all services administered in the Oracle Enterprise Manager console, the e-Business tools provide a library of event tests specific to the HTTP Server. The types of event tests associated with the HTTP Server are:

- UpDown event test
- Threshold event tests

The HTTP Server UpDown event test checks whether the Apache HTTP server being monitored is running.

The threshold event tests are triggered by user-specified metrics. The full descriptions of the individual event tests follow. The event tests are in alphabetical order.

Summary of e-Business Event Tests

The following table lists the e-Business event tests. The full descriptions of the individual event tests follow the table. The event tests are in alphabetical order.

Table 10–1 Applications Fault Management Event Tests

Event Test	Description
Bytes per Second	This event test monitors the number of bytes transferred by the HTTP Server per second. The rate is calculated depending on the frequency of the event. For example, if the event was registered with a frequency of 100 seconds, the event will calculate the rate by dividing the number of bytes served in that period by 100.
Requests per Second	This event test monitors the number of requests made to the HTTP Server per second. The rate is calculated depending on the frequency of the event. For example, if the event was registered with a frequency of 100 seconds, the event will calculate the rate by dividing the number of requests in that period by 100.
Total Servers	This event test monitors the number of servers that the HTTP Server has spawned to handle the incoming requests. The HTTP Server increases the number of servers when there is a greater number of requests to handle and reduces the number of servers when there are fewer requests. This action maximizes the resource utilization on the system.

Descriptions of e-Business Event Tests

The e-Business event tests are listed in alphabetical order.

Bytes per Second

This event test monitors the number of bytes transferred by the HTTP Server per second. The rate is calculated depending on the frequency of the event. For example, if the event was registered with a frequency of 100 seconds, the event will calculate the rate by dividing the number of bytes served in that period by 100.

Parameters

- Critical Threshold: Number of request per seconds that will trigger the Critical alert event. Default is 10000.
- Warning Threshold: Number of request per seconds that will trigger the Warning alert event. Default is 2000.

Output

None

Default Frequency

60 seconds

User Action

Check the access logs to determine a cause. If the condition persists, tune the system to handle a larger data output.

Requests per Second

This event test monitors the number of requests made to the HTTP Server per second. The rate is calculated depending on the frequency of the event. For example, if the event was registered with a frequency of 100 seconds, the event will calculate the rate by dividing the number of requests in that period by 100.

Parameters

- Critical Threshold: Number of requests per second that will trigger the Critical alert event. Default is 50.
- Warning Threshold: Number of requests per second that will trigger the Warning alert event. Default is 20.

Output

None

Default Frequency

60 seconds

User Action

Check the access logs to determine a cause. If the condition persists, tune the system to handle a larger number of requests.

Total Servers

This event test monitors the number of servers that the HTTP Server has spawned to handle the incoming requests. The HTTP Server increases the number of servers when there is a greater number of requests to handle and reduces the number of servers when there are fewer requests. This action maximizes the resource utilization on the system.

Note: On Windows NT, servers represent the number of threads while on UNIX systems a server correlates to a process.

Parameters

- Critical Threshold: Number of servers that will trigger the Critical alert event. Default is 80.
- Warning Threshold: Number of servers that will trigger the Warning alert event. Default is 30.

Output

None

Default Frequency
60 seconds

User Action
Check the access logs to determine a cause. If the condition persists, tune the Web Server to use resources more efficiently or upgrade the hardware.