IBM Tivoli Monitoring
Version 6.2.3 Fix Pack 1

Windows OS Agent User's Guide

SC32-9445-05

IBM Tivoli Monitoring
Version 6.2.3 Fix Pack 1

Windows OS Agent User's Guide

SC32-9445-05

Note
Before using this information and the product it supports, read the information in "Notices" on page 497.

This edition applies to version 6.2.3 Fix Pack 1 of IBM Tivoli Monitoring: Windows OS Agent (product number 5724-C04) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Tables

Chapter 1. Overview of the Monitoring Agent for Windows OS

The Monitoring Agent for Windows OS provides you with the capability to monitor Microsoft Windows, and to perform basic actions with Microsoft Windows. This chapter provides a description of the features, components, and interface options for the Monitoring Agent for Windows OS.

IBM Tivoli Monitoring overview

IBM Tivoli Monitoring is the base software for the Monitoring Agent for Windows OS. IBM Tivoli Monitoring provides a way to monitor the availability and performance of all the systems in your enterprise from one or several designated workstations. It also provides useful historical data that you can use to track trends and to troubleshoot system problems.

You can use IBM Tivoli Monitoring to do the following:

- Monitor for alerts on the systems that you are managing by using predefined situations or custom situations.
- Establish your own performance thresholds.
- Trace the causes leading to an alert.
- Gather comprehensive data about system conditions.
- Use policies to perform actions, schedule work, and automate manual tasks.

The Tivoli Enterprise Portal is the interface for IBM Tivoli Monitoring products. By providing a consolidated view of your environment, the Tivoli Enterprise Portal permits you to monitor and resolve performance issues throughout the enterprise.

See the IBM Tivoli Monitoring publications listed in “IBM Tivoli Monitoring library” on page 491 for complete information about IBM Tivoli Monitoring and the Tivoli Enterprise Portal.

Features of Monitoring Agent for Windows OS

The Monitoring Agent for Windows OS offers a central point of management for your Microsoft Windows server environment. It provides a comprehensive means for gathering exactly the information you need to detect problems early and to prevent them. Information is standardized across your enterprise. The Monitoring Agent for Windows OS lets you easily collect and analyze server-specific information such as the following:

- Operating system and CPU performance
- Disk information and performance analysis
- Process status analysis
- Internet session data
- Monitored logs information
- Internet server statistics
- Message queuing statistics
- Printer and job status data
- Remote Access Services statistics
- Services information

The Monitoring Agent for Windows OS provides the following benefits:

- Increases knowledge with extensive reporting capabilities that provide real-time access to reliable, up-to-the-minute data. Thus, you can make faster, better-informed operating decisions.
- Enhances system performance by letting you integrate, monitor, and manage your system, environment, console, and mission-critical applications. For example, the monitoring agent can alert you when conditions in your environment meet or exceed the thresholds you set. These alerts notify your system administrator to limit and control system traffic.
- Simplifies application and system management by managing applications, platforms, and resources across your system.

New in this release

For version 6.2.3 of the Monitoring Agent for Windows OS, the following enhancements have been made:

- Support for self-describing agents. See the *IBM® Tivoli® Monitoring Installation and Setup Guide* for more information.
- Enhanced reporting capabilities, including a redesigned installer for OS Agent reports and new reports for Tivoli Common Reporting. See Chapter 8, "Tivoli Common Reporting for the monitoring agent," on page 267 for additional informatiton about reporting capabilities.
- A new Tivoli Monitoring capability allows you to perform prerequisite checking for agents before performing an installation. The two mechanisms available are a manually executed stand-alone prerequisite scanner, or a remote prerequisite scanner facility that extends the capabilities of IBM Tivoli Monitoring's remote deployment component. See the *IBM Tivoli Monitoring: Installation and Setup Guide* and the *IBM Tivoli Monitoring: Command Reference* for more information.
- The following situations:
  - NT_BP_ProcMissing_Critical
  - NT_BP_Evt_Source_Critical
  - NT_BP_ProcCpuPct_Warning
  - NT_BP_MemAvailKB_Critical
  - NT_BP_TcpRetrans_Warning

  These predefined situations are based on best practices. While they might not prove perfectly suited to every monitoring environment, they offer a useful starting point for many users.

For version 6.2.3 Fix Pack 1 of the Monitoring Agent for Windows OS, the following enhancements have been made:

- Support for monitoring any event log in the Windows Event Viewer, instead of only the five standard Windows event logs: Application, System, Security, DNS Server, and Directory Service or File Replication Service.

  Note: You must specify the exact name of the event log you want to monitor. The Windows Registry Editor lists the event log name as a key in either of two paths:
  - *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog*
  - *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*

The name of the event log is the key listed under the Eventlog or Channels key. For example, the Application event log has the key:
  - *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application*
- The following event variables:
  - NT_{*Event Log Name*}_LOG_THROTTLE to throttle events
  - NT_{*Event Log Name*}_LOG_DUPLICATE to drop duplicate events
  - NT_{*Event Log Name*}_LOG_MAX_TIME to process old events
  - NT_{*Event Log Name*}_LOG_MAX_EVTS to process old event
- The Monitored Logs workspace, including a Records view, Size view, and Monitored Logs view, indicates when performance changes occur in Windows applications. The Event Log workspace, including a Monitored Logs view and an Event Log view, provides a summary of size and usage data for Windows event logs. Both workspaces support your writing situations against the workspaces using Event Log attributes or Monitored Logs Report attributes.

Components of Monitoring Agent for Windows OS

After you install the Monitoring Agent for Windows OS (product code "knt" or "nt") as directed in the *IBM Tivoli Monitoring Installation and Setup Guide*, you have an environment with a client, server, and monitoring agent implementation for IBM Tivoli Monitoring that contains the following components:

- Tivoli Enterprise Portal client with a Java-based user interface for viewing and monitoring your enterprise.
- Tivoli Enterprise Portal Server that is placed between the client and the Tivoli Enterprise Monitoring Server and enables retrieval, manipulation, and analysis of data from the monitoring agents.
- Tivoli Enterprise Monitoring Server, which acts as a collection and control point for alerts received from the monitoring agents, and collects their performance and availability data.
- Monitoring Agent for Windows OS, which collects and sends data to a Tivoli Enterprise Monitoring Server. This component also embeds the Agent Management Services function.
- Operating system agents and application agents installed on the systems or subsystems you want to monitor. These agents collect and send data to the Tivoli Enterprise Monitoring Server.
- Tivoli Data Warehouse for storing historical data collected from agents in your environment. The data warehouse is located on a DB2®, Oracle, or Microsoft SQL Server database. To collect information to store in this database, you must install the Warehouse Proxy agent. To perform aggregation and pruning functions on the data, install the Warehouse Summarization and Pruning agent.
- Tivoli Enterprise Console event synchronization component for synchronizing the status of situation events that are forwarded to the event server. When the status of an event is updated because of IBM Tivoli Enterprise Console® rules or operator actions, the update is sent to the monitoring server, and the updated status is reflected in both the Situation Event Console and the Tivoli Enterprise Console event viewer. For more information, see *IBM Tivoli Monitoring Installation and Setup Guide*.

User interface options

Installation of the base software and other integrated applications provides the following interfaces that you can use to work with your resources and data:

Tivoli Enterprise Portal browser client interface
The browser interface is automatically installed with Tivoli Enterprise Portal. To start Tivoli Enterprise Portal in your Internet browser, enter the URL for a specific Tivoli Enterprise Portal browser client installed on your Web server.

Tivoli Enterprise Portal desktop client interface
The desktop interface is a Java-based graphical user interface (GUI) on a Windows or Linux workstation.

IBM Tivoli Enterprise Console
Event management application

Manage Tivoli Enterprise Monitoring Services window
The window for the Manage Tivoli Enterprise Monitoring Services utility is used for configuring the agent and starting Tivoli services not already designated to start automatically.

Chapter 2. Requirements for the monitoring agent

This chapter contains information about the requirements for the Monitoring Agent for Windows OS.

In addition to the requirements described in the *IBM Tivoli Monitoring Installation and Setup Guide*, the Monitoring Agent for Windows OS has the requirements listed in Table 1. For more information on requirements and scenarios for attribute groups and workspaces, see Appendix B, "Workspaces additional information: requirements and scenarios," on page 367.

Table 1. System requirements for the Monitoring Agent for Windows OS

Operating system	**Windows**
Operating system versions	• Windows 2000 Server (32-bit) • Windows 2000 Advanced Server (32-bit) • Windows XP Professional, Service Pack 1 (32-bit) • Windows Server 2003 Data Center Edition, Service Pack 1 (32-bit, x86) • Windows Server 2003 Standard Edition, Service Pack 1 (32-bit) • Windows Server 2003 Enterprise Edition, Service Pack 1 (32-bit) • Windows Server 2003 R2 Enterprise x64 Edition (64-bit, x86-64) • Windows Server 2003 R2 Standard x64 Edition (64-bit, x86-64) • Windows Server 2003 R2 Data Center Edition x64 Edition (64-bit, x86-64) • Windows Server 2003 Enterprise Itanium Edition (64-bit, IA64) • Windows Server 2008 Standard Edition (32-bit) • Windows Server 2008 Data Center Edition (32-bit) • Windows Server 2008 Enterprise Edition (32-bit) • Windows Server 2008 R2 Enterprise x64 Edition (64-bit, x86-64) • Windows Server 2008 R2 Standard x64 Edition (64-bit, x86-64) • Windows Server 2008 R2 Data Center Edition x64 Edition (64-bit, x86-64) • Windows Vista Professional • Windows Vista Ultimate • Windows 7 Professional • Windows 7 Ultimate
Memory	• 35 MB RAM for the Monitoring Agent for Windows OS

Table 1. System requirements for the Monitoring Agent for Windows OS (continued)

Operating system	Windows
Disk space	• The Monitoring Agent for Windows OS requires 125 MB of disk space in the file system where it is to be installed through the local install method. See "Disk capacity planning for historical data" on page 241 for additional information about disk space for historical data collection.
Other requirements	• IBM Tivoli Monitoring v6.2.2 agents require at least a v6.2.2 hub monitoring server and portal server. IBM Tivoli Monitoring v6.2.1 hub monitoring servers and portal servers do not support v6.2.2 monitoring agents. IBM Tivoli Monitoring v6.2.1 monitoring agents work with both v6.2.1 and v6.2.2 environments. • Components to be monitored must be installed and configured • The minimum supported level of Microsoft.NET Framework is .NET Framework 1.1 SP1. For older releases of Windows OS that do not support 1.1 .NET, the minimum level is NET Framework 1.0 SP3. .NET Framework 3.5 is supported for 64-bit agents. • cscript version 5.6 or higher • The watchdog that is part of the Windows OS Agent calls scripts that require Windows Script Host 5.6 at a minimum

Note: If you install the agent on a 64-bit platform, the installer will default to 64-bit mode. If you are upgrading from an older version, the agent will continue to run in 32-bit mode.

Note: You cannot install two Windows OS Agents on the same system. This restriction also precludes installing a 32-bit Windows OS Agent and a 64-bit Windows OS Agent on the same system.

Note: For the most current information about the operating systems that are supported, see the following URL: http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity/index.html.

When you get to that site, click on the relevant link in the **Operating system reports** section.

Silent installation: If you are performing a silent installation using a response file, see the IBM Tivoli Monitoring Installation and Setup Guide, "Performing a silent installation of IBM Tivoli Monitoring."

Running as a non-Administrator user

You can run the Monitoring Agent for Windows OS as a non-Administrator user, however some functionality is unavailable.

When running as a non-Administrator user, you lose functionality in the following attribute groups if they are owned solely by the Administrator account:

- Registry

- File Trend
- File Change

Remote deployment of other agents is not available because administrator rights are required to install the new agents.

For Agent Management Services, the watchdog cannot stop or start any agent that it does not have privileges to stop or start.

To create a non-Administrator user, create a new Limited (non-Administrator) user and set up registry permissions as follows for the new user:

- full access to `HKEY_LOCAL_MACHINE\SOFTWARE\Candle`
- read access to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib`

The user that starts the Monitoring Agent for Windows OS – Primary service must have rights to manage the Monitoring Agent for Windows OS - Watchdog service. The user that starts the Monitoring Agent for Windows OS - Watchdog service must also have rights to manage any services that are managed by the Agent Management Services, including the Monitoring Agent for Windows OS – Primary service. Use Group Policy, Security Templates or Subinacl.exe to grant users the authority to manage system services in Windows. For detailed information, see the following Microsoft documentation athttp://support.microsoft.com/kb/325349.

The following example uses the security templates:

1. Click **Start** ->**Run**, enter `mmc` in the Open box, and then click **OK**.
2. On the File menu, click **Add/Remove Snap-in**.
3. Click **Add -> Security Configuration and Analysis**, and then click **Add** again.
4. Click **Close** and then click **OK**.
5. In the console tree, right-click **Security Configuration and Analysis**, and then click **Open Database**.
6. Specify a name and location for the database, and then click **Open**.
7. In the Import Template dialog box that is displayed, click the security template that you want to import, and then click **Open**.
8. In the console tree, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.
9. In the Perform Analysis dialog box that is displayed, accept the default path for the log file that is displayed in the Error log file path box or specify the location that you want, and then click **OK**.
10. After the analysis is complete, configure the service permissions as follows:
    a. In the console tree, click **System Services**.
    b. In the right pane, double-click the Monitoring Agent for Windows OS - Primary service.
    c. Select the **Define this policy in the database** check box, and then click **Edit Security**.
    d. To configure permissions for a new user or group, click **Add**.
    e. In the Select Users, Computers, or Groups dialog box, type the name of the user or group that you want to set permissions for, and then click **OK**. In the Permissions for User or Group list, select the **Allow** check box next to the **Start** button, stop and pause permission is selected by default. This setting permits the user or group to start, stop, and pause the service.

f. Click **OK** two times.

11. Repeat step 10 selecting the Monitoring Agent for Windows OS - Watchdog service.
12. To apply the new security settings to the local computer, right-click **Security Configuration and Analysis**, and then click **Configure Computer Now**.

Note: You can use also the Secedit command-line tool to configure and analyze system security. For more information about Secedit, click **Start** -> **Run**, enter `cmd` in the Open box, and then click **OK**. At the command prompt, type `secedit /?`, and then press **ENTER**. Note that when you use this method to apply settings, all the settings in the template are reapplied, and this may override other previously configured file, registry, or service permissions.

Use the Windows Services console to set the OS Agent and watchdog services to log on using the non Administrator user.

1. Click **Start** -> **Run**, enter `services.msc` in the Open box, and then click **OK**.
2. Select **Monitoring Agent for Windows OS - Primary**.
3. Right-click **Properties**.
4. Verify the startup type as being Automatic.
5. Select the **Log On** tab, and then select **Log on as "This account"** and supply the ID and password. Click **OK**.
6. Select **Monitoring Agent for Windows OS - Watchdog**.
7. Right-click **Properties**.
8. Verify the startup type as being Manual.
9. Select the **Log On** tab, and then select **Log on as "This account"** and supply the ID and password. Click **OK**.

Setting up the Monitoring Agent for Windows OS in a cluster environment

The *IBM Tivoli Monitoring Installation and Setup Guide* contains an overview of clustering. The information provided here is specifically for installing and setting up the Monitoring Agent for Windows OS in a Microsoft Cluster Server environment.

This agent monitors information that is both affected (shared disks, processes ...) and not affected (memory, CPU ...) by cluster resources as the resources are failed over from node to node in the cluster. Therefore, the agent actively runs on all nodes in the cluster. The agent was not modified to distinguish the differences between cluster affected and non-affected resources. History for those attributes that can move from node to node is only maintained for the time that the node owns the resource.

Resources not currently owned by the node might not show at all or may show with values of zero. In most cases the information is not shown on the node that does not own the resource. The physical disk attributes are examples of a monitored resource. The node that does not own the resource shows the disk but the attributes value as Zero while the logical disk information and attributes are only shown by the owning node. When the logical disk fails over, the system interface and the agent require an amount of time to discover the fail over.

Monitor the system log for cluster services entries by specifying the following values:

1. The Attribute Group equal to NT_Event_Log, for more information see “Event Log attributes” on page 76
2. Attribute Item: Log Name (Unicode) equal to System (case sensitive)
3. Attribute Item: Source equal to source of the log entry, for example ClusSvc
4. Attribute Item: Category equal to source of the log entry, for example Failover Mgr
5. Attribute Item: Event ID equal to the desired cluster eventID, for example:
   - 1201 - the cluster service brought the resource group online
   - 1204 - the cluster service brought the resource group offline

Using Agent Management Services

There are two watchdog monitors that run as part of the Monitoring Agent for Windows. One monitor runs as part of the OS Monitoring Agent process, which is referred to as the *Agent Watchdog*. The other watchdog monitor runs as a separate process named 'kcawd' (kcawd.exe on Windows). The kcawd process is also called the *Agent Management Services Watchdog*. This watchdog watches the OS Agent. It does this out-of-the-box, so as long as its Availability Status is showing 'Running' in the Agents' Runtime Status view of the Agent Management Services workspace. No setup or configuration is required.

The Agent Watchdog monitors agent processes other than the OS Agent. By using the communication facility of the OS Agent, this monitor can respond to Tivoli Enterprise Portal Desktop queries and Take Action commands that are performed against these other agent processes. The data is displayed in the Agent Management Services workspace. In the Tivoli Enterprise Portal Desktop, the Agent Management Services workspace lists the agents that can be monitored by this watchdog that is running as part of the OS Agent. These agents are non-OS agents, so the Monitoring Agent for Windows is not listed in the workspace, except for in the Agents' Management view. One of the agents listed in the workspace is the Agent Management Services Watchdog. Its purpose is to monitor the OS Agent's availability.

The Agent Management Services Watchdog monitor is responsible for watching just the OS Monitoring Agent and restarting it if it goes down. It is enabled by default and does not need to be configured. It is started automatically when the Monitoring Agent for Windows is started. This watchdog does not have a communication facility, so it cannot report information to the Tivoli Enterprise Portal or respond to Take Action commands. It is not an agent in itself, but a separate process that always monitors the OS Monitoring Agent.

You can temporarily disable the Agent Management Services Watchdog by using the *InstallDir*\tmaitm6_x64\disarmWatchdog.bat command if you have installed a 64-bit agent or by using the *InstallDir*\tmaitm6\disarmWatchdog.bat command if you have installed a 32-bit agent. These commands disable the Watchdog process for the OS Monitoring Agent and all Agent Management Services managed agents. If there is local administrative work to be performed, and you do not want the auto-restart of the agents to interfere with it, run appropriate command for your platform before proceeding. When the work is complete, recycle the OS Monitoring Agent to reenable Agent Management Services. Alternatively, use the

InstallDir\tmaitm6_x64\rearmWatchdog.bat command if you have installed a 64-bit agent or the *InstallDir*\tmaitm6\rearmWatchdog.bat command if you have installed a 32-bit agent.

If you use the Manage Tivoli Enterprise Monitoring Services interface to stop or start an Agent Management Services managed agent, its watchdog will be disabled if stopping the agent and enabled if starting the agent.

Processing missed Windows Event Log events

Whenever you have situations that monitor the Windows Event Log and you do not want to lose events that might occur when the Windows OS agent is stopped or situations are stopped, you can set environment variables to process the missed events. This function is by default disabled, so you must set one or more environment variables in the KNTENV file. These environment variables provide a mechanism for you to ensure that the monitoring server and portal server are not flooded with events if the agent is shut down or situations are stopped for long periods of time and then restarted:

- Missed Events by Time Interval

  Apply to all event logs:

  – NT_LOG_MAX_TIME=*x*

  Apply to each log separately:

  – NT_{*Event Log Name*}_LOG_MAX_TIME=*x*

  When *x* is a positive value in minutes:

  – *x* = 0, disabled, do not process missed events while the agent is shut down or a situation is stopped.

  – *x* = 1, process all missed events while the agent was shut down or a situation is stopped.

  – *x* > 1, process all missed events that are within the value specified in minutes.

  For example, if *x*=120, then at startup of the agent, only events that are within 120 minutes of the current machine time are processed that were received while the agent was shut down or a situation is stopped.

  You must specify the exact name of the event log you want to monitor. The Windows Registry Editor lists the event log name as a key in either of two paths:

  – *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog*

  – *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*

  The name of the event log is the key listed under the Eventlog or Channels key. For example, the Application event log has the key:

  – *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application*

  Applying the Event Log Name to the environment variable, NT_{*Event Log Name*}_LOG_MAX_TIME, requires the conversion of any invalid characters within the Event Log Name to a dash (-). Invalid characters include a space ( ), asterisk (*), pound sign (#), vertical bar (|), back slash (\), forward slash (/), colon (:), quotation mark ("), less than sumbol (<), greater than symbol (>), and question mark (?). For example, if the Event Log Name is Microsoft-Windows-TaskScheduler/Operational, then the environment variable to use in the KNTENV file would be NT_Microsoft-Windows-TaskScheduler-Operational_LOG_MAX_TIME=*x* where *x* is defined above and the forward slash (/) was changed to a dash (-).

- Missed Events by Maximum Count

  Apply to all event logs:

  – NT_LOG_MAX_EVTS=*x*

  Apply to each log separately:

  – NT_{*Event Log Name*}_LOG_MAX_EVTS=*x*

  Where *x* is a positive value specifying a maximum count of events to process.

  – *x* = 0, disabled, do not process missed events while the agent is shut down or a situation is stopped.
  – *x* = 1, process all missed events while the agent was shut down or a situation is stopped.
  – *x* > 1, process missed events while the agent was shut down or a situation is stopped for a maximum of *x* events.

  You must specify the exact name of the event log you want to monitor. The Windows Registry Editor lists the event log name as a key in either of two paths:

  – *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog*
  – *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*

  The name of the event log is the key listed under the Eventlog or Channels key. For example, the Application event log has the key:

  – *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application*

  Applying the Event Log Name to the above environment variable, NT_{*Event Log Name*}_MAX_EVTS, requires the conversion of any invalid characters within the Event Log Name to a dash (-). Invalid characters include a space ( ), asterisk (*), pound sign (#), vertical bar (|), back slash (\), forward slash (/), colon (:), quotation mark ("), less than sumbol (<), greater than symbol (>), and question mark (?). For example, if the Event Log Name is Microsoft-Windows-TaskScheduler/Operational, then the environment variable to use in the `KNTENV` file would be NT_Microsoft-Windows-TaskScheduler-Operational_LOG_MAX_EVTS=*x* where *x* is defined above and the forward slash (/) was changed to a dash (-).

Define one or more of the above environment variables with a non-zero value in the `KNTENV` file, and then restart the Windows OS agent. When the agent is restarted, you will see situation events triggered for Windows Event Log events that were missed because they occurred after the agent or the situation was last stopped.

Both sets of environment variables can be used together. In this way, you can process a maximum number of events received while the agent was shut down or a situation is stopped, along with the time interval that the event must fall within. Any of the environment variables that apply separately to the Windows Event Logs override the environment variables NT_LOG_MAX_TIME and NT_LOG_MAX_EVTS for that specified event log. The processing of missed events for a specific Windows Event Log while a situation is stopped requires that all situations running against the specific Windows Event Log be stopped along with historical data collection for the Event Log group.

Chapter 3. Workspaces reference

This chapter contains an overview of workspaces, references for detailed information about workspaces, and descriptions of the predefined workspaces included in this monitoring agent.

About workspaces

A workspace is the working area of the Tivoli Enterprise Portal application window. At the left of the workspace is a Navigator that you use to select the workspace you want to see.

As you select items in the Navigator, the workspace presents views pertinent to your selection. Each workspace has at least one view. Some views have links to other workspaces. Every workspace has a set of properties associated with it.

Some predefined workspaces are not available from the Navigator tree item, but are accessed by selecting the link indicator next to a row of data in a view. Left-clicking a link indicator selects the default workspace associated with that link. Right-clicking a link indicator displays all linked workspaces that can be selected.

Note: The Event Log workspace and the Print Job workspace are examples of linked workspaces.

This monitoring agent provides predefined workspaces. You cannot modify or delete the predefined workspaces, but you can create new workspaces by editing them and saving the changes with a different name.

More information about workspaces

For more information about creating, customizing, and working with workspaces, see the *IBM Tivoli Monitoring User's Guide*.

For a list of the predefined workspaces for this monitoring agent and a description of each workspace, refer to the Predefined workspaces section below and the information in that section for each individual workspace.

For additional information about workspaces for this monitoring agent, see Appendix B, "Workspaces additional information: requirements and scenarios," on page 367.

Predefined workspaces

The Monitoring Agent for Windows OS provides the following predefined workspaces, which are organized by Navigator item:

- "Disk workspace" on page 19
  - "Logical Disk workspace" on page 28
  - "Logical Disk I/O workspace" on page 28
  - "Physical Disk workspace" on page 33
  - "Mount Point workspace" on page 30

This agent also includes the following historical workspaces:

- Historical Summarized Availability
  - Historical Summarized Availability Daily
  - Historical Summarized Availability Hourly
  - Historical Summarized Availability Weekly
- Historical Summarized Capacity
  - Historical Summarized Capacity Daily
  - Historical Summarized Capacity Hourly
  - Historical Summarized Capacity Weekly
- Historical Summarized Performance
  - Historical Summarized Performance Daily
  - Historical Summarized Performance Hourly
  - Historical Summarized Performance Weekly

The following workspaces have a historical version:

- Active Server Pages
- Cache
- DHCP Server
- DNS Dynamic Update
- DNS Memory
- DNS Query
- DNS WINS
- DNS Zone Transfer
- FTP Server Statistics
- FTP Service
- Gopher Service
- HTTP Content Index
- HTTP Service
- ICMP Statistics
- IIS Statistics
- Indexing Service
- Indexing Service Filter
- IP Statistics
- Job Object
- Job Object Details
- Logical Disk
- Logical Disk I/O
- Memory Allocation
- MSMQ Information Store
- MSMQ Queue
- MSMQ Service
- MSMQ Sessions
- Network Interface
- Network Segment
- NNTP Commands
- NNTP Server
- Objects
- Paging
- Paging File
- Physical Disk
- Print Queue
- Process Overview
- Process Storage
- Processor Overview
- RAS Port
- RAS Total
- SMTP Server
- System I/O
- System Overview

- System Pools
- System Timings
- TCP Statistics
- UDP Statistics
- Web Service

The remaining sections of this chapter contain descriptions of each of these predefined workspaces.

IBM Tivoli Monitoring: Windows OS Agent workspaces

The IBM Tivoli Monitoring: Windows OS Agent workspaces contain the views you use to obtain information about the various aspects of Windows systems. The views within each workspace report attribute information you are monitoring. You can use them to do the following:

- Investigate attribute information relating to a change in state
- Monitor your system performance to identify bottlenecks and to evaluate tuning decisions
- Select the most effective threshold values for situations you create

A workspace might contain notepad views, browser sessions, event consoles, or a take action views that give you the ability to send commands to the operator console.

Note that the descriptions of each workspace apply to the default settings (the components of the workspace in its original configuration).

Active Server Pages workspace

The Active Server Pages workspace displays information on Active Server Pages requests, session data, and memory usage.

This workspace includes a Request Activity view, a Request Time Distribution view, and the Active Server Pages view. Use the view to obtain data about allocated memory, browser requests executing, request execution time, allocated memory in free list, and sessions timed out. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Agent Management Services workspace

The Agent Management Services workspace contains views of data collected by the Agent Management Services component of the Monitoring Agent for Windows.

This workspace includes an Agents' Management Status view, an Agents' Runtime Status view, an Agents' Alerts view, and an Agents' Management Definitions view.

Agents' Management Log workspace

The Agents' Management Log workspace contains a list of monitoring agent log entries filtered on the Agent Management Services component. Use this workspace to see the operations being executed by Agent Management Services and to have an audit trail of the operations that Agent Management Services is performing.

Log messages generated by the physical watchdog are displayed in the Agents' Management Log workspace view. By using these log messages, you can track OS Agent restarts and availability. The limitations of this function are that the physical watchdog must be running.

Alerts that are seen in the Alerts view in the default workspace are cached for 24 hours, by default. The time can be overridden by changing the environment variable KCA_CACHE_LIMIT found in the `kntcma.ini` file. The variable is specified in hours. This functionality is not available to previous versions of the agents.

The workspace includes the following operation messages:

- Agent added to system - CAP file found.
- Agent CAP file initialization completed.
- Agent daily restart count reset.
- Agent exceeded policy defined CPU threshold.
- Agent exceeded policy defined memory threshold.
- Agent exceeded restart tries.
- Agent initial start.
- Agent Management Services watchdog not reliable.
- Agent manual start failed.
- Agent manual stop failed.
- Agent not configured.
- Agent not found.
- Agent now managed.
- Agent now unmanaged.
- Agent recycle command received.
- Agent removed from system - CAP file removed.
- Agent restart disabled - disarm mode active
- Agent restart failed.
- Agent start command received.
- Agent started successfully.
- Agent stop command received.
- Agent stopped abnormally.
- Agent stopped successfully.
- Disarm completed successfully.
- Rearm completed successfully.

This workspace includes an Agents' Management Log view.

Cache workspace

The Cache workspace displays cache statistics. This helps you, along with the other Memory workspaces, to identify disk performance problems through slow rates of data transfer from disk to memory and high disk usage.

This workspace includes an Activity view and the Cache view. Use the view to obtain information about the number of times data is read in to the cache prior to writing the data back to disk, the frequency of reads from cache pages using a Memory Descriptor List (MDL) to access the pages, and the number of pages the

cache has flushed to disk. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Devices workspace

The Devices workspace displays status and configuration information about each device and file system driver installed on the server.

This workspace includes views of Automatic Start Type and Devices. Use the Devices view to obtain information about the name of the device driver, the current state of the device driver, and the name of the load ordering group to which this driver belongs. Use the Automatic Start Type view to obtain information about the state of the devices and the binary path. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Device Dependencies workspace

This workspace includes Dependencies and Devices views. The Dependencies view reports the device name and dependency type. The Devices view displays the device name, current state of device and the binary path.

DHCP Server workspace

The DHCP Server workspace helps you monitor all types of Dynamic Host Configuration Protocol (DHCP) messages sent and received by the server, the average amount of processing time spent by the server per message packet, and the number of message packets dropped because of internal delays at the server.

This workspace includes a Packet Traffic view and the DHCP Server view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Disk workspace

The Disk workspace information reflects the health of your storage components within your monitored systems. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus "superseded") with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). This workspace contains “at a glance” data associated with disk byte traffic, disk usage, and disk time distribution, including the following:

- Amount of disk byte traffic (reads and writes) expressed in bytes/second
- Percentage of disk space used and free
- Percentage of disk read time and disk write time

DNS Dynamic Update workspace

The DNS Dynamic Update workspace includes an Activity view and the DNS Dynamic Update view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the

information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

DNS Memory workspace

The DNS Memory workspace includes an Allocation view and the DNS Memory view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

DNS Query workspace

The DNS Query workspace includes a TCP Traffic view, a UDP Traffic view, and the DNS Query view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

DNS WINS workspace

The DNS WINS workspace includes a Lookup Traffic view, a Reverse Lookup view, and the DNS WINS view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

DNS Zone Transfer workspace

The DNS Zone Transfer workspace includes a Successes/Failures view and the DNS Zone Transfer view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Enterprise Services workspace

The Enterprise Services workspace contains information that reflects the health of your enterprise services systems. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). This workspace contains "at a glance" traffic data associated with ASP requests, FTP data, MSMQ messages, NNTP data, and web requests, including the following:

- ASP requests executed per second
- Rate of data bytes (per second) sent and received by the FTP service
- Rate of incoming and outgoing MSMQ messages handled by the MSMQ Service per second
- Rate of data bytes (per second) sent and received by the NNTP Server
- Rate of data bytes (per second) sent and received by the Web service

Event Log workspace

The Event Log workspace provides a summary of size and usage data for Windows event logs. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). This predefined workspace is not available from the Navigator tree item, but is accessed by selecting the link indicator next to a row of data in a System workspace view. Left-clicking a link indicator selects the default workspace associated with that link. Right-clicking a link indicator displays all linked workspaces that can be selected. This workspace includes the Monitored Logs view and the Event Log view.

When running ITM V6.2.3 Fix Pack 1 (or later), you have the capability to display events and event data from any event log you are monitoring. However, the Log Name and Log Name (Unicode) attributes represent input fields, not output fields. Filtering on the event log name is not supported. You must specify the exact name of the event log you want to monitor.

File Change workspace

The File Change workspace provides information on modifications to your file systems and to your directories. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

This workspace includes the File Change view. You can use this workspace to find out information such as when a file/directory was added, when a file/directory was removed, when a file/directory changed (in size, in attribute, or in the security for the file/directory), and when a file/directory was renamed. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

File Trend workspace

The File Trend workspace gives you a history of the recent activity of your file system. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

This workspace includes the File Trend view. Use the view to obtain information about the percent change over the last hour, percent change over the last interval, date created, size change over the last hour, and free space available. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

The File Trend view monitors the discrete files only and not subdirectories.

FTP Server Statistics workspace

The FTP Server Statistics workspace displays traffic statistics, session data, and connection activity for an FTP server.

This workspace includes a Connection Activity view, a File I/O view, a Byte Traffic view, and the FTP Server Statistics view. Use the view to obtain information about the number of bytes sent per second, connection attempts since startup, current

anonymous users, files sent per second, current connections, and logon attempts since startup. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

FTP Service workspace

The FTP Service workspace display traffic statistics, session data, and connection activity for an FTP server.

This workspace includes a Connection Activity view, a File I/O view, a Byte Traffic view, and the FTP Service view. Use the view to obtain information about the number of bytes sent per second, connection attempts since startup, current anonymous users, files sent per second, current connections, and logon attempts since startup. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Gopher Service workspace

The Gopher Service workspace provides traffic statistics, session data, and connection information for a Gopher server.

This workspace includes a Byte Traffic view and the Gopher Service view. Use the view to obtain information about total connection attempts, current connections, Kbytes received per second, Kbytes sent per second, maximum connections, directory listings sent, and logon attempts. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Historical Summarized Availability workspace

The Historical Summarized Availability workspace shows the managed resource availability (up time) data for the number of months that you specify in the Time Span dialog. This workspace consists of the following two graphical views:

- Availability by O/S Type, which shows the percentage of time that managed resources were up and available, grouped by operating system
- Availability by Server, which shows the percentage of time that each managed resource was up and available

Historical Summarized Availability Daily workspace

The Historical Summarized Availability Daily workspace shows the availability (up time) data by day, the sessions summary by day, and the system summary for a managed resource. This workspace consists of the following three graphical views:

- Availability (daily), which shows the average system up time, summarized by day
- Session Summary (daily), which shows session details such as the number sessions logged off and sessions timed out, summarized by day

- System Summary (daily), which shows system data such as the operating system type

Historical Summarized Availability Hourly workspace

The Historical Summarized Availability Hourly workspace shows the availability (up time) data by hour, the sessions summary by hour, and the system summary for a managed resource. This workspace consists of the following three graphical views:

- Availability (hourly), which shows the average system up time, summarized by hour
- Session Summary (hourly), which shows session details such as the number sessions logged off and sessions timed out, summarized by hour
- System Summary (hourly), which shows system data such as operating system type

Historical Summarized Availability Weekly workspace

The Historical Summarized Availability Weekly workspace shows the availability (up time) data by month, the sessions summary by week, and the system summary for a managed resource. This workspace consists of the following four graphical views:

- Availability (monthly), which shows the average system up time, summarized by month for the number of months that you specify in the Time Span dialog
- Availability (weekly), which shows the average managed resource up time, summarized by week
- Session Summary (weekly), which shows session details such as the number sessions logged off and sessions timed out, summarized by week
- System Summary (weekly), which shows system data such as the operating system type

Historical Summarized Capacity workspace

The Historical Summarized Capacity workspace shows the percentage of system resources used for the time span that you specify in the Time Span dialog. This workspace consists of the following four graphical views:

- Network Interface Activity (maximum over months), which shows the maximum percentage of network usage for the system during the time span that you specify in the Time Span dialog
- Processor Utilization (average over months), which shows the average processor utilization percentage during the specified time period
- Memory Utilization (average over months), which shows the average percentage of memory used during the specified time period
- Disk Capacity (average over months), which shows the maximum percentage of space used on all the system's logical disks during the specified time period

Historical Summarized Capacity Daily workspace

The Historical Summarized Capacity Daily workspace shows the percentage of system resources used for the time span that you specify in the Time Span dialog, summarized by day. This workspace consists of the following four graphical views:

- Network Interface Activity (daily), which shows the maximum percentage of network usage for the system during the time span that you specify in the Time Span dialog, summarized by day

- Processor Utilization (daily), which shows the average processor utilization percentage during the specified time period, summarized by day
- Memory Utilization (daily), which shows the average percentage of memory used during the specified time period, summarized by day
- Disk Capacity (daily), which shows the maximum percentage of space used on all the system's logical disks during the specified time period, summarized by day

Historical Summarized Capacity Hourly workspace

The Historical Summarized Capacity Hourly workspace shows the percentage of system resources used for the time span that you specify in the Time Span dialog, summarized by hour. This workspace consists of the following four graphical views:

- Network Interface Activity (hourly), which shows the maximum percentage of network usage for the system during the time span that you specify in the Time Span dialog, summarized by hour
- Processor Utilization (hourly), which shows the average processor utilization percentage during the specified time period, summarized by hour
- Memory Utilization (hourly), which shows the average percentage of memory used during the specified time period, summarized by hour
- Disk Capacity (hourly), which shows the maximum percentage of space used on all the system's logical disks during the specified time period, summarized by hour

Historical Summarized Capacity Weekly workspace

The Historical Summarized Capacity Weekly workspace shows the percentage of system resources used for the time span that you specify in the Time Span dialog, summarized by week. This workspace consists of the following four graphical views:

- Network Interface Activity (weekly), which shows the maximum percentage of network usage for the system during the time span that you specify in the Time Span dialog, summarized by week
- Processor Utilization (weekly), which shows the average processor utilization percentage during the specified time period, summarized by week
- Memory Utilization (weekly), which shows the average percentage of memory used during the specified time period, summarized by week
- Disk Capacity (weekly), which shows the maximum percentage of space used on all the system's logical disks during the specified time period, summarized by week

Historical Summarized Performance workspace

The Historical Summarized Performance workspace shows the average performance of system resources for the time span that you specify in the Time Span dialog. This workspace consists of the following four graphical views:

- Network Interface Performance (average over months), which shows the average rate of bytes transferred for the system during the time span that you specify in the Time Span dialog
- Processor Performance (average over months), which shows the average rate of interrupts for the system during the specified time period
- Memory Performance (average over months), which shows the average rate of page faults for the system during the specified time period

- Disk Performance (average over months), which shows the average percentage of disk time that the system used during the specified time period

Historical Summarized Performance Daily workspace

The Historical Summarized Performance Daily workspace shows the average performance of system resources for the time span that you specify in the Time Span dialog, summarized by day. This workspace consists of the following four graphical views:

- Network Interface Performance (daily), which shows the average rate of bytes transferred for the system during the time span that you specify in the Time Span dialog, summarized by day
- Processor Performance (daily), which shows the average rate of interrupts for the system during the specified time period, summarized by day
- Memory Performance (daily), which shows the average rate of page faults for the system during the specified time period, summarized by day
- Disk Performance (daily), which shows the average percentage of disk time that the system used during the specified time period, summarized by day

Historical Summarized Performance Hourly workspace

The Historical Summarized Performance Hourly workspace shows the average performance of system resources for the time span that you specify in the Time Span dialog, summarized by hour. This workspace consists of the following four graphical views:

- Network Interface Performance (hourly), which shows the average rate of bytes transferred for the system during the time span you specify in the Time Span dialog, summarized by hour
- Processor Performance (hourly), which shows the average rate of interrupts for the system during the specified time period, summarized by hour
- Memory Performance (hourly), which shows the average rate of page faults for the system during the specified time period, summarized by hour
- Disk Performance (hourly), which shows the average percentage of disk time that the system used during the specified time period, summarized by hour

Historical Summarized Performance Weekly workspace

The Historical Summarized Performance Weekly workspace shows the average performance of system resources for the time span that you specify in the Time Span dialog, summarized by week. This workspace consists of the following four graphical views:

- Network Interface Performance (weekly), which shows the average rate of bytes transferred for the system during the time span that you specify in the Time Span dialog, summarized by week
- Processor Performance (weekly), which shows the average rate of interrupts for the system during the specified time period, summarized by week
- Memory Performance (weekly), which shows the average rate of page faults for the system during the specified time period, summarized by week
- Disk Performance (weekly), which shows the average percentage of disk time that the system used during the specified time period, summarized by week

HTTP Content Index workspace

The HTTP Content Index workspace provides statistics for queries made to an HTTP server.

This workspace includes a Query Activity view and the HTTP Content Index view. Use the view to obtain information about the number of active queries, queries per minute, total requests rejected, and total queries. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

HTTP Service workspace

The HTTP Service workspace provides traffic data, connection statistics, and session data for an HTTP server.

This workspace includes a File I/O view, a Connection Activity view, and the HTTP Service view. Use the view to obtain information about the number of bytes received per second, bytes sent per second, current anonymous users, current connections, files received per second, files sent per second, and CGI requests. Additionally, IBM Tivoli Monitoring: Windows Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

ICMP Statistics workspace

The ICMP Statistics workspace provides message traffic information.

This workspace includes a Message Traffic view, a Message Errors view, and the ICMP Statistics view. Use the view to obtain information about the number of messages per second, messages received per second, received destination unreachable, messages sent per second, received time exceeded, and sent time exceeded. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

IIS Statistics workspace

The IIS Statistics workspace displays memory usage and connection data for the Internet Information Server.

This workspace includes a Request Activity view and the IIS Statistics view. Use the view to obtain information about the number of cache flushes, cache hits, cache misses, cache used, cached directory listings, total rejected asynchronous requests, and measured asynchronous I/O bandwidth usage. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Indexing Service workspace

The Indexing Service workspace collects statistics pertaining to the creation of indices and the merging of indices by the indexing service. A subordinate workspace, the Indexing Service Filter workspace, contains indexing speed and binding time information.

The Indexing Service workspace includes an Index Activity view, an Index Size view, and the Indexing Service view. Use the views to obtain information about the number of files indexed, the size of the content index, the number of active query client connections, the total number of documents in the index, the average time spent binding to indexing filters (Indexing Service Filter view), and the speed of indexing contents of files (Indexing Service Filter view). Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Indexing Service Filter workspace

The Indexing Service Filter workspace contains indexing speed and binding time information.

This workspace includes an Index Speed view and the Indexing Service Filter view. Use the view to determine the binding time, indexing speed, and the total indexing speed. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

IP Statistics workspace

The IP Statistics workspace provides traffic and fragmentation statistics for data using the IP protocol.

This workspace includes a Datagram Traffic view and the IP Statistics view. Use the view to obtain information about the number of datagrams forwarded per second, datagrams outbound that were discarded, datagrams received that had address errors, and fragmentation failures. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Job Object workspace

The Job Object workspace helps you monitor the name of a Windows Job Kernel Object, the system resources a job consumes, and the number of processes a job contains. The Job Object Detail workspace helps you to monitor details of individual Windows 2000 Job Kernel Objects including system resources a job consumes and the resources used by each of the processes that job contains.

The Job Object workspace includes a Processes view, a Time Distribution view, and the Job Object view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24

hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Both this workspace and its historical version have a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus "superseded") with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Job Object Details workspace

The Job Object workspace helps you monitor the name of a Windows 2000 Job Kernel Object, the system resources a job consumes, and the number of processes a job contains. The Job Object Detail workspace helps you to monitor details of individual Windows 2000 Job Kernel Objects including system resources a job consumes and the resources used by each of the processes that job contains.

The Job Object Details workspace includes a Memory Allocation view and the Job Object Details view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Logical Disk workspace

The Logical Disk workspace provides detailed information on swapping and paging activity and helps determine if system performance problems are caused by memory shortages.

This workspace includes a Usage view, a Time Distribution view, and a Logical Disk view. Use the view to obtain information about the total virtual memory, processes in run queue, processes waiting, page faults and page reclaims, and page ins and page outs. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Both this workspace and its historical version have a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus "superseded") with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Logical Disk I/O workspace

The Logical Disk I/O workspace provides detailed rate information for disk reads, disk writes, and transfers.

This workspace includes an Activity view, a Byte Traffic view, and a Logical Disk I/O view. Use the view to obtain information about the rate (in bytes/seconds) and total of disk reads, writes, and transfers. Additionally, IBM Tivoli Monitoring:

Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Both this workspace and its historical version have a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Memory workspace

The Memory workspace contains information that reflects the health of your memory components within your monitored systems. This workspace contains "at a glance" data associated with memory allocation, cache activity, and paging traffic, including the following:

- Available KBs, cache KBs, cache KBs peak, commit limit KBs, and committed KBs
- Percentage of copy read hits, data map hits, and pin read hits
- Pages input and output per second used to measure paging activity

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Memory Allocation workspace

The Memory Allocation workspace provides information on memory usage, virtual memory, reads and writes to the swap file, and page faults. This helps you, along with the other Memory workspaces, to identify disk performance problems through slow rates of data transfer from disk to memory and high disk usage.

This workspace includes an Allocation view and the Memory view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Monitored Logs workspace

The Monitored Logs workspace tells you when performance changes occur in Windows applications. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). You can access the information in any Windows Event logs. By using filters to view the log details, you can quickly pinpoint the problem.

This workspace includes a Records view, a Size view, and the Monitored Logs view. Use this view to obtain information about current size, record count, and % usage of the logs. In addition, the Event Log view associated with this workspace lets you monitor the actual records that are written to any Windows Event logs, such as the date and time of an event and event identification information. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

When running ITM V6.2.3 Fix Pack 1 (or later), you have the capability to display events and event data from any event log you are monitoring. However, the Log Name and Log Name (Unicode) attributes represent input fields, not output fields. Filtering on the event log name is not supported. You must specify the exact name of the event log you want to monitor.

Mount Point workspace

The Mount Point workspace includes a Usage view and a Mount Point Information view.

MSMQ Information Store workspace

The MSMQ Information Store workspace displays session information relating to the Information Store.

This workspace includes a Replication Activity view and the MSMQ Information Store view. Use the view to obtain information about the total number of MSMQ Information Store accesses that resulted in error replies by the Information Store, the total number of replication requests sent, and the total number of write requests sent. Additionally, IBM Tivoli Monitoring: Windows Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

MSMQ Queue workspace

The MSMQ Queue workspace displays message queue statistics.

This workspace includes a Message Activity view, a Byte Traffic view, and the MSMQ Queue view. Use the view to obtain information about the total number of bytes currently in the journal queue and the total number of messages in the journal queue. Additionally, IBM Tivoli Monitoring: Windows Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

MSMQ Service workspace

The MSMQ Service workspace displays session data and message traffic information.

This workspace includes a Message Traffic view, a Message Activity view, and the MSMQ Service view. Use the view to obtain information about the number of incoming messages, the number of outgoing messages, and the total number of open IPX sessions. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the

information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

MSMQ Sessions workspace

The MSMQ Sessions workspace displays session data and traffic flow information.

This workspace includes a Byte Traffic view, a Message Traffic view, and the MSMQ Sessions view. Use the view to obtain information about the rate of incoming MSMQ messages, the IP address of the computer in session with MSMQ, and the total number of bytes that were sent. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Network workspace

The Network workspace contains a variety of workspaces that reflect the health of the network components within your monitored systems. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). This workspace contains "at a glance" data associated with DHCP packet traffic, DNS memory allocation, IP datagram traffic, network packet traffic, and TCP connection activity, including the following:

- Rate of packets expired and received (packets per second)
- Total caching, TCP message, and UDP message memory used by the DNS server
- Rate (datagrams per second) of datagrams received and sent
- Rate (packets per second) of packets received and sent on the network interface
- Connection activity statistics, measured by the change in state of TCP connections

Network Interface workspace

The Network Interface workspace displays transmission rates and bandwidth utilization for data going over a TCP/IP connection.

This workspace includes a Byte Traffic view, a Packet traffic view, a Network Interface view, and a Network Interface IP Address view. Use the view to obtain information about the current bandwidth, packets outbound discarded, bytes total per second, packets received per second, and packets sent per second. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Network Ports workspace

The Network Port workspace includes a Network Port by State view and a Network Port Information view.

Network Segment workspace

The Network Segment workspace displays bandwidth utilization and traffic statistics for data in a network segment.

This workspace includes a Bandwidth Distribution view, a Frame Traffic view, and the Network Segment view. Use the view to obtain information about the percent broadcast frames, percent multicast frames, percent network utilization, broadcast frames received per second, and total bytes received per second. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

NNTP Commands workspace

The NNTP Commands workspace provides data to help you monitor a wide range of commands associated with the hosting of news group discussions.

This workspace includes a Command Activity view, a Logon Activity view, and the NNTP Commands view. Use the view to obtain information about a variety of commands received by the NNTP server, the rate at which these commands are received, and the number of logons per second that have failed. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

NNTP Server workspace

The NNTP Server workspace provides data to help you monitor a wide range of server activities associated with the hosting of news group discussions.

This workspace includes a Connection Activity view, an Article Traffic view, and the NNTP Server view. Use the view to obtain information about the rate of article deletion on the NNTP server, the total number of files sent per second by the NNTP server, the maximum number of simultaneous connections to the NNTP server, and the number of SSL connections made to the NNTP server. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Objects workspace

The Objects workspace identifies various system objects in Windows systems such as threads, processes, mutexes, semaphores, and various services, such as spoolers.

This workspace includes an Activity view and the Objects view. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this

workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Paging workspace

The Paging workspace provides detailed information on the efficiency of I/O operations using the paging file. This helps you, along with the other Memory workspaces, to identify disk performance problems through slow rates of data transfer from disk to memory and high disk usage.

This workspace includes an Activity view, an I/O view, and the Paging view. Use the view to obtain information about memory manager paging activity rates, including page reads, writes, and faults per second. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Paging File workspace

The Paging File workspace provides information about the system's paging file(s), particularly the % usage. This helps you, along with the other Memory workspaces, to identify disk performance problems through slow rates of data transfer from disk to memory and high disk usage.

This workspace includes a Usage view and the Paging File view. Use the view to obtain information about the % usage for each pagefile. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Physical Disk workspace

The Physical Disk workspace provides information on file system location and disk space usage. It identifies system performance problems caused by disk space shortages and uneven distribution of space across disks and file systems.

This workspace includes a Time Distribution view, a Byte Traffic view, and a Physical Disk view. Use the view to obtain information about the space available, space used, and space used percent. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Both this workspace and its historical version have a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version

with the same name (minus "superseded") with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Print Job workspace

The Print Job workspace displays information on the status of the jobs that you submitted to your printer. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). This predefined workspace is not available from the Navigator tree item, but is accessed by selecting the link indicator next to a row of data in a Printer workspace view. Left-clicking a link indicator selects the default workspace associated with that link. Right-clicking a link indicator displays all linked workspaces that can be selected.

Print Queue workspace

The Print Queue workspace displays information on performance and operation of printers locally attached to a computer using information from the Print Queue attribute group.

This workspace includes a Job Activity view, an Errors view, and the Print Queue view. Use the view to obtain information about the number of bytes per second printed on a print queue, the current number of jobs in a print queue, the current number of references (open handles) to the printer, and the total number of pages printed. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Printer workspace

The Printer workspace contains information that reflects the health of your printing systems. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). This workspace contains "at a glance" data associated with print queue job activity, printer jobs, and print job sizes, including the following:

- Data about jobs and jobs spooling in a queue, as well as total number of jobs printed (printers across the network)
- Number of jobs in the printer queue (specific printers)
- Size of specific print jobs

The Print Job workspace is a linked workspace from the Printer workspace. This workspace includes a Jobs view and a Print Job view. Right-click the link indicator in the Printer workspace to display the Print Job workspace and all linked workspaces that can be selected.

Printer Overview workspace

The Printer Overview workspace displays information on the status of the printers that are connected to your server. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

This workspace includes a Jobs view and the Printer Overview view. Use the view to obtain information about information about specific printers, including number of jobs, port name, location, and average pages per minute. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Process workspace

The Process workspace contains information that reflects the health of specific processes within your monitored systems. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). This workspace contains "at a glance" data associated with process time distribution, job object time distribution, and job object memory allocation, including the following:

- Percentage of elapsed time that a process has executed instructions in privileged mode vs. user mode
- Number of milliseconds of kernel mode processor time, processor time, and user mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the Job object was created
- Size (in KBs) of the page file, private bytes, and virtual bytes

Process I/O workspace

The Process I/O workspace includes an Activity by Process view and a Process I/O Information view.

Process Overview workspace

The Process workspace provides detailed information on each currently executing process, including identification, priority, command, and size data.

This workspace includes a Time Distribution view and the Process Overview view. Use the view to obtain information about the process ID, parent process ID, CPU utilization, priority, execution state, and time. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Process Storage workspace

The Process Storage workspace provides detailed information on virtual memory, page files, pool and nonpool bytes.

This workspace includes an Allocation view and the Process Storage view. Use the view to obtain information about the virtual bytes, page file bytes, pool paged and pool nonpaged bytes, as well as peak measurements of this data. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Processor workspace

The Processor workspace reflect the health of the processors within your monitored systems, containing "at a glance" data associated with process activity and process time distribution, including the following:

- Average number of interrupts a processor has processed per second, including totals.
- Percentage of elapsed time that a processor has been busy executing instructions in privileged time vs. user time, including totals.

Processor Overview workspace

The Processor Overview workspace displays percentages of processor activity taking place on each monitored Windows system.

Use this workspace to check for problems such as processes consuming abnormally large amounts of CPU time, imbalances between user and system CPU demands, and long CPU waits caused by I/O bottlenecks. This workspace includes a Time Distribution view and the Processor Overview view. Use the view to obtain information about the system name, user CPU and system CPU, idle CPU, and I/O wait time. Additionally, IBM Tivoli Monitoring: Windows Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Processor Summary workspace

The Processor Summary workspace includes a High/Low Processor Differences view, a High Process Information view, a High Processor Information view, and a Low Processor Information view.

RAS Port workspace

The RAS Port workspace displays transmission rates for the Remote Access Service.

This workspace includes an Errors view, a Byte Traffic view, and the RAS Port view. Use the view to obtain information about the total number of alignment

errors for a connection, the total number of data frames received for a particular connection, and the total number of bytes transmitted for a connection. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

RAS Total workspace

The RAS Total workspace displays transmission rates for the Total Remote Access Service.

This workspace includes an Errors view, a Compression I/O view, and the RAS Total view. Use the view to obtain information about the total number of alignment errors for a connection, the total number of buffer overrun errors, and the total number of bytes transmitted for a connection. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Redirector workspace

The Redirector workspace includes a Session Summary view and a Redirector Information view.

Server Overview workspace

This workspace displays server sessions details. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). This workspace includes a Security view, Throughput view and the Server Overview view.

Server Work Queues workspace

The Server Work Queues workspace includes a Work Summary by Queue view and a System Work Queue Information view.

Services workspace

The Services workspace displays status and configuration information about each service installed on the server.

This workspace includes views of Automatic Start Type and Services. Use the Services view to obtain information about the current state of the service and the name of the service. Use the Automatic Start Type view to obtain information about the state of the services and the binary path. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Service Dependencies workspace

The Services Dependencies workspace displays status and configuration information about each service installed on the server.

This workspace includes views of Dependencies and Services. Use the Services view to obtain information about the current state of the service and the name of the service. Use the Dependencies view to obtain information about dependencies of the services. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

SMTP Server workspace

The SMTP workspace helps you to monitor a wide range of activities associated with the hosting of an electronic mail server.

This workspace includes a Message Activity view, a Connection Activity view, and the SMTP Server view. Use the view to obtain information about the total number of bytes/KBs sent and received, the total number of messages delivered to local mailboxes, the number of non-delivery workspaces that have been generated, and the total number of connection errors. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

System I/O workspace

The System I/O workspace provides file read, write, and control information. This helps you, along with the other System workspaces, to identify the configuration of your systems and check their current activity levels.

This workspace includes an Operation Activity view, a Byte Traffic view, and the System I/O view. Use the view to obtain information about file control, file read, file write, and file data operations information. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

System workspace

The System workspace contains "at a glance" data associated with monitored logs, device states, and services, including the following:

- Log data, including name, modification date, max and current size (with percentage usage), and path.
- Device data, including display name, the current state of the device, and an indication of when to start the device (Automatic, Manual or Disabled, Boot, or System).
- Services data, including display name, the current state of the services, and an indication of when to start the services (Automatic, Manual or Disabled, Boot, or System)

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

The Event Log workspace is a linked workspace from the System workspace. This workspace includes an Event Log view and a Monitored Logs view. Right-click the link indicator in the System workspace to display the Event Log workspace and all linked workspaces that can be selected.

System Information workspace

The System Information workspace includes a Computer Information view, a BIOS Information view, and a Processor Information view.

System Overview workspace

The System Overview workspace supplies basic identification and system activity information on your monitored Windows Servers systems. Use this workspace to identify the configuration of your systems and check their current activity levels.

This workspace includes a Processor Queue Threads view and the System Overview view. Use the view to obtain information about system details, including the operating system type, the number of processors, and the network address. Additionally, IBM Tivoli Monitoring: Windows Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Both this workspace and its historical version have a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus "superseded") with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

System Pools workspace

The System Pools workspace provides detailed pool paged and non-paged information. This helps you, along with the other Memory workspaces, to identify disk performance problems through slow rates of data transfer from disk to memory and high disk usage.

This workspace includes an Allocation view, and the System Pools view. Use the view to obtain information about the number and size of system requests for space allocation in the paged and non-paged pool areas of memory. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

System Timings workspace

The System Timings workspace provides processor, user, privileged time, and context switch information. This helps you, along with the other System workspaces, to identify the configuration of your systems and check their current activity levels.

This workspace includes an Activity view and the System Timings view. Use the view to obtain information about % totals of privileged, processor, and user times, as well as the rate of context switches, system calls, and total interrupts per second. Additionally, IBM Tivoli Monitoring: Windows Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Both this workspace and its historical version have a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

TCP Statistics workspace

The TCP Statistics workspace displays connection data and segment traffic information for data using the TCP/IP protocol.

This workspace includes a Connection Activity view and the TCP Statistics view. Use the view to obtain information about active connections, connection failures, connections established, segments received per second, and segments per second. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Threads workspace

The Threads workspace includes a Processor Usage by Thread view and a Thread Information view.

UDP Statistics workspace

The UDP Statistics workspace provides datagram traffic statistics for data using the UDP protocol.

This workspace includes a Datagram Traffic view and the UDP Statistics view. Use the view to obtain information about the datagrams received per second, datagrams received that had errors, and datagrams sent per second. Additionally, IBM Tivoli Monitoring: Windows OS Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

Web Service workspace

The Web Service workspace provides traffic data, connection statistics, and session data for an HTTP server.

This workspace includes a File I/O view, a Connection Activity view and the Web Service view. Use the view to obtain information about the number of bytes received per second, bytes sent per second, current anonymous users, current connections, files received per second, files sent per second, and CGI requests. Additionally, IBM Tivoli Monitoring: Windows Agent provides a historical version of this workspace. You can request to view up to 24 hours of historical data for each component of this workspace. Based on the information that this workspace provides, you can recommend changes, set up situations, and verify that changes are improving performance.

This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807).

Windows OS workspace

The Windows OS workspace shows summary information for the computer being monitored by an instance of the Monitoring Agent for Windows OS. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). Views show the following:

- Names and usage statistics for each logical disk
- Memory usage
- Top ten processes using the most CPU
- Top ten processes using the most private memory
- Top ten processes using the most virtual memory

Windows OS Details workspace

The Windows OS Details workspace shows summary information for a computer being monitored by an instance of the Monitoring Agent for Windows OS. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). The views show the following:

- Names and usage statistics for each logical disk
- Memory usage
- Top ten processes using the most CPU
- Top ten processes using the most private memory
- Top ten processes using the most virtual memory

Windows Systems workspace

The Windows Systems workspace shows summary information for every Monitoring Agent for Windows OS instance. This workspace has a superseded version that displays queries with signed 32-bit maximum value (2,147,483,647) and a version with the same name (minus 'superseded') with queries that support values up to signed 64-bit max (9,223,372,036,854,775,807). The views show the following:

- Key characteristics about the Windows system, for example, operating system type and version, and the number of processors
- List of agents that are online

- List of agents that are offline
- For online agents, views show memory usage, disk usage and processor usage

Chapter 4. Attributes reference

This chapter contains an overview of attributes, references to detailed information about attributes, and descriptions of the attributes for each attribute group included in this monitoring agent.

IBM Tivoli Monitoring provides other attribute groups that are available to all monitoring agents, for example Universal Time and Local Time. The attributes in these common attribute groups are documented in the Tivoli Enterprise Portal Help.

About attributes

Attributes are the application properties being measured and reported by Monitoring Agent for Windows OS, such as the amount of memory usage or the message ID.

Attributes are organized in to groups according to their purpose. The attributes in a group can be used in the following two ways:

- Chart or table views

  Attributes are displayed in chart and table views. The chart and table views use queries to specify which attribute values to request from a monitoring agent. You use the Query editor to create a new query, modify an existing query, or apply filters and set styles to define the content and appearance of a view based on an existing query.
- Situations

  You use attributes to create situations that monitor the state of your operating system, database, or application. A situation describes a condition you want to test. When you start a situation, the Tivoli Enterprise Portal compares the values you have assigned to the situation attributes with the values collected by Monitoring Agent for Windows OS and registers an *event* if the condition is met. You are alerted to events by indicator icons that are displayed in the Navigator.

Some of the attributes in this chapter are listed twice, with the second attribute having a "(Unicode)" designation after the attribute name. These Unicode attributes were created to provide access to globalized data.

More information about attributes

For more information about using attributes and attribute groups, see the *IBM Tivoli Monitoring User's Guide*.

Groups of attributes

Each attribute belongs to an attribute group. The attribute group includes attributes that are related. Each attribute item stores data for a particular property of an attribute group.

The following are the attribute groups for IBM Tivoli Monitoring: Windows OS Agent. The groups are collected in attribute tables that are designated in brackets [ ] after the group name.

- Active Server Pages [ACTSRVPG]
- Agent Availability Management Status [KNTPASMGMT]
- Agent Active Runtime Status [KNTPASSTAT]
- Alerts Table [KNTPASALRT]
- BIOS Information [NTBIOSINFO]
- Cache [NTCACHE]
- Computer Information [NTCOMPINFO]
- Configuration Information [KNTPASCAP]
- Device Dependencies [NTDEVDEP]
- Devices [NTDEVICE]
- DHCP Server [DHCPSRV]
- DNS Dynamic Update [DNSDYNUPD]
- DNS Memory [DNSMEMORY]
- DNS Query [DNSQUERY]
- DNS WINS [DNSWINS]
- DNS Zone Transfer [DNSZONET]
- Event Log [NTEVTLOG]
- File Change [NTFLCHG]
- File Trend [NTFLTREND]
- FTP Server Statistics [FTPSTATS]
- FTP Service [FTPSVC]
- Gopher Service [GOPHRSVC]
- HTTP Content Index [HTTPCNDX]
- HTTP Service [HTTPSRVC]
- ICMP Statistics [ICMPSTAT]
- IIS Statistics [IISSTATS]
- Indexing Service [INDEXSVC]
- Indexing Service Filter [INDEXSVCF]
- IP Address [NTIPADDR]
- IP Statistics [IPSTATS]
- Job Object [JOBOBJ]
- Job Object Details [NTJOBOBJD]
- Job Object Details (superseded) [JOBOBJD]
- Logical Disk [WTLOGCLDSK]
- Mount Point [NTMNTPT]
- Memory [NTMEMORY]
- Memory (superseded) [WTMEMORY]
- Monitored Logs Report [NTLOGINFO]
- MSMQ Information Store [MSMQIS]
- MSMQ Queue [MSMQQUE]
- MSMQ Service [MSMQSVC]
- MSMQ Sessions [MSMQSESS]
- Network Interface [NTNETWRKIN]
- Network Interface (superseded) [NETWRKIN]
- Network Port [NTNETWPORT]

- Network Segment [NETSEGMT]
- NNTP Commands [NNTPCMD]
- NNTP Server [NNTPSRV]
- Objects [WTOBJECTS]
- Paging File [NTPAGEFILE]
- Physical Disk [WTPHYSDSK]
- Print Job [NTPRTJOB]
- Print Queue [PRINTQ]
- Printer [NTPRINTER]
- Process [NTPROCESS]
- Process (superseded) [WTPROCESS]
- Process IO [PROCESSIO]
- Processor [NTPROCSSR]
- Processor Information [NTPROCINFO]
- Processor Summary [NTPROCRSUM]
- RAS Port [KNTRASPT]
- RAS Total [KNTRASTOT]
- Redirector [NTREDIRECT]
- Registry [WTREGISTRY]
- Server [WTSERVER]
- Server Work Queue [NTSERVERQ]
- Server Work Queue (superseded) [WTSERVERQ]
- Service Dependencies [NTSVCDEP]
- Services [NTSERVICE]
- SMTP Server [SMTPSRV]
- System [WTSYSTEM]
- TCP Statistics [TCPSTATS]
- Thread [WTTHREAD]
- UDP Statistics [UDPSTATS]
- Web Service [WEBSVC]

IBM Tivoli Monitoring provides other attribute groups that are available to all monitoring agents, for example Universal Time and Local Time. The attributes in these common attribute groups are documented in the Tivoli Enterprise Portal Help.

Active Server Pages attributes

Use the Active Server Pages attributes to create situations to monitor Active Server Page requests, session information, and memory allocation. Active Server Pages is a single-instance attribute group. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

Allocated Memory The total amount of memory currently allocated by Active Server Pages. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Allocated Memory In Free List The number of bytes of allocated memory in the free memory list. Note that this attribute is only available on systems running with IIS installed and configured. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Allocated Memory In Used List The number of bytes of allocated memory in the used memory list. Note that this attribute is only available on systems running with IIS installed and configured. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Browser Requests Executing The number of browser requests currently executing. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Communication Failed The number of requests that failed due to communication failure. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Debugging Requests Number of debugging document requests. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Errors During Script Runtime Number of requests failed due to runtime errors. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Errors From ASP Preprocessor Number of requests failed due to preprocessor errors. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Errors From Script Compilers Number of requests failed due to script compilation errors. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Free Script Engines in Cache The number of free script engines in cache. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Request Errors/sec The number of errors per second, including connection errors, compile errors, and runtime errors. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Request Execution Time The number of milliseconds that it took to execute the most recent request. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Request Total Bytes In The total size, in bytes, of all the requests that have been enqueued. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Request Total Bytes Out The total size, in bytes, of responses sent to clients. This does not include standard HTTP headers. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Request Wait Time The number of milliseconds since the most recent request. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Requests Current The number of requests expecting service from the queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Requests Executed The total number of requests that have been dequeued and successfully executed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Requests Failed The total number of requests that had a compile time or runtime error. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Requests Not Authorized Number of requests failed due to insufficient access rights. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Requests Not Found The number of requests for files that were not found. Valid values are positive integers in the range 0 to 2147483647 and can include the use of

the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Requests Rejected The total number of requests not executed because the queue was full or there were insufficient resources to enqueue the requests. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Requests/sec The number of requests executed per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Requests Timed Out The number of requests that timed out. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Requests Total The total number of requests that have been enqueued since the service was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Session Duration The number of milliseconds that the most recent session persisted. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Session Timed Out Requests Executing The number of sessions timed out with requests currently executing. Note that this attribute is only available on systems running with IIS installed and configured. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Sessions Current The current number of sessions being serviced. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sessions Timed Out The number of sessions timed out. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sessions Timed Out Requests In Queue The number of sessions timed out with requests queued to execute. Note that this attribute is only available on systems

running with IIS installed and configured. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Sessions Total The total number of sessions since the service was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Template Cache Hit Rate Percent of requests found in template cache. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown.

Template Notifications The number of templates invalidated in the cache due to change notification. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Templates Cached The number of templates currently cached. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Thread Pool Current The current number of threads in the Active Server Pages thread pool. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Queue Length The total number of requests that are currently enqueued. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Transactions Aborted The number of transactions aborted. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Transactions Committed The number of transactions committed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Transactions Pending Number of transactions in progress. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Transactions Total The total number of transactions since the service was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Transactions/sec Transactions started per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Agent Availability Management Status attributes

Use Agent Availability Management Status attributes to view the current management status of an agent relative to Agent Management Services.

Agent Management Status The watched agent management status. The following values are valid: Unmanaged (0), Managed (1), Watchdog (2). A value of 'Managed' means that the agent is under the management of Agent Management Services. A value of 'Unmanaged' means it is known, but that the agent is not under the management of Agent Management Services.

Agent Name The watched agent name.

Agent Type The watched agent type. The following values are valid: Unknown (0), ITM_Unix (1), Console (2), Windows_Service (3), Discover_ITM (4), Discover_Bin (5), Linux_Service (6), ITM_Windows (7).

Agent Version The version, release, and modification information for the agent.

Build Date The build date information for the agent. Superseded by the Build Number attribute.

Build Number The build number information for the agent.

Manager Type The enum defining the manager type. The following are values are valid: Unknown (0), Not_Managed (1), Agent_Management Services (2), Watchdog (3), External (4). A value of 'Agent Management Services' means that Agent Management Services is responsible. A value of 'NotManaged' means that the agent is not under availability monitoring by any application. A value of 'Externally' means that some other application besides Agent Management Services is responsible for availability monitoring of the agent, for example Tivoli System Automation or Windows service control manager.

Operating System The operating system identification. The following are values are valid: Unknown (0), Windows (1), Linux (2).

Server Name The origin node of the collecting agent.

Service Name The service name.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Agent Active Runtime Status attributes

Use the Agents Active Runtime Status attributes to view the current availability status of an agent: Running, Not present, Unknown, Stopped, Manually Stopped. You can view the frequency at which the agent's availability and runtime properties are queried and also the agent's Daily Restart Count.

% Privileged Time The system CPU.

% Processor Time The CPU used by the process.

% User Time The user CPU time.

Agent Availability Status The watched agent availability status. The following are values are valid: Unknown (0), Not_found (1), Stopped (2), Start_Pending (3), Running (4), Manually_Stopped (5), Stop_Pending (6), Not_Configured (7). For agents that have an Availability Status of 'Running', use the attribute group to see runtime properties of the agent such as its Process ID and Thread Count.

Agent Host Name The host name of the agent.

Agent Name The watched agent name.

Agent Type The watched agent type. The following are values are valid: Unknown (0), ITM_Unix (1), Console (2), Win_Service (3), Discover_ITM (4), Discover_Bin (5), Linux_Service (6), ITM_Windows (7).

Check Frequency The frequency to check status in seconds.

Command Line The command line.

Daily Restart Count The restarts within a period of a day.

Handle Count The handle count.

Instance Name The instance name of the running IBM Tivoli Monitoring agent.

IP Address The IP address of the agent.

Last Health Check The last health check timestamp.

Operating System The operating system identification. The following values are valid: Unknown (0), Windows (1), Linux (2).

Page Faults sec The page faults per second.

Process ID The process ID.

Process Name The process name.

Server Name The origin node of the collecting agent.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Thread Count The thread count.

Total Working Set kBytes The working set size in kilobytes.

User Name The user name of the running managed agent.

Virtual kBytes The total size.

Alerts Table attributes

Use the Alerts Table attributes to view exceptional Warning and Critical level events surfaced by Agent Management Services. These events have to do with the operation of Agent Management Services or conditions affecting its ability to manage agents. The following alerts are included:

- Agent stopped abnormally.
- Agent restart failed.
- Agent exceeded restart tries.
- Agent not found.
- Agent exceeded policy defined memory threshold.
- Agent exceeded policy defined CPU threshold.
- Agent manual stop failed.
- Agent removed from system - CAP file removed.

Agent Name The watched agent name.

Agent Status The agent status. The following values are valid: Unknown (0), Not_found (1), Stopped (2), Start_Pending (3), Running (4), Manually_Stopped (5), Stop_Pending (6), Not_Configured (7).

Agent Type The watched agent type. The following values are valid: Unknown (0), ITM_Unix (1), Console (2), Windows_Service (3), Discover_ITM (4), Discover_Bin (5), Linux_Service (6), ITM_Windows (7).

Alert Details The alert message details.

Alert Message The alert message. The following values are valid: Availability_policy_removed (1), Managed_agent_removed_from_system (2), Unmanaged_agent_removed_from_system (3), Agent_abnormally_stopped (4), Agent_exceeded_restart_count (5), Agent_restart_failed (6), Agent_overutilizing_memory (7), Agent_overutilizing_CPU (8), Agent_manual_stop_failed (9), Agent_Management_Services_watchdog_not_reliable (11).

Operating System The operating system identification. The following values are valid: Unknown (0), Windows (1), Linux (2).

Process ID The process ID.

Process Name The process name.

Server Name The origin node of the collecting agent.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day

HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

BIOS Information attributes

Use BIOS Information attributes to monitor general information about the System BIOS. The data source for these attributes is WMI. To avoid throughput issues with the Microsoft WMI stack, you should limit the collection frequency to 5 minute intervals. This ensures that the Microsoft WMI Data queues have sufficient time to service the WMI queries made for collecting these attributes.

BIOS Description BIOS description of the manufacturer. The manufacturer of the BIOS sets this attribute value.

BIOS Manufacturer Manufacturer of the BIOS. The manufacturer of the BIOS sets this attribute value.

BIOS Release Date Release date of the Windows BIOS in the Coordinated Universal Time (UTC) format of YYYYMMDDHHMMSS.MMMMMM(+-)OOO.

BIOS Serial Number Serial Number of the BIOS. This attribute value can be equal to the Computer ID Number. Typically this occurs when the computer BIOS manufacturer and system manufacturer are the same. This attribute value is set by the BIOS manufacturer.

BIOS Version Version of the BIOS. This string is created by the BIOS manufacturer. The manufacturer of the BIOS sets this attribute value.

System Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Cache attributes

Use the Cache attributes to create situations to monitor cache activity, such as the frequency of reads from cache pages, the percentage of cache copy requests that were successful, and the number of pages the cache has flushed to disk. Cache is a single-instance attribute group.

Async Copy Reads/sec The frequency of reads from cache pages that involve a memory copy of the data from the cache to the buffer for the application. The application regains control immediately even if the disk must be accessed to retrieve the page. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Async Data Maps/sec The frequency that an application uses a file system, such as NTFS or HPFS, to map a page of a file in to the cache to read the page, and does not wish to wait for the cache to retrieve the page if it is not in main memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Async Fast Reads/sec The frequency of reads from cache pages that bypass the installed file system and retrieve the data directly from the cache. Normally, file I/O requests invoke the appropriate file system to retrieve data from a file, but this path permits direct retrieval of cache data without file system involvement if the data is in the cache. Even if the data is not in the cache, one invocation of the file system is avoided. If the data is not in the cache, the request (application program call) gets control immediately. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Async MDL Reads/sec The frequency of reads from cache pages using a Memory Descriptor List (MDL) to access the pages. The MDL contains the physical address of each page in the transfer, thus permitting Direct Memory Access (DMA) of the pages. If the accessed page(s) are not in main memory, the calling application program does not wait for the pages to fault in from disk. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Async Pin Reads/sec The frequency of reading data in to the cache prior to writing the data back to disk. Pages read in this fashion are pinned in memory at the completion of the read. The file system regains control immediately even if the disk must be accessed to retrieve the page. While pinned, the physical address for the page is not altered. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Copy Read Hits % The percentage of cache copy read requests that hit the cache, that is, that did not require a disk read to provide access to the page in the cache. A copy read is a file read operation that is satisfied by a memory copy from a cache page to the buffer for the application. The LAN Redirector uses this method to retrieve cache information, as does the LAN Server for small transfers. This is a method used by the disk file systems as well. Valid format is a numeric string in the range 0 to 100 (expressing a percentage). Note: the value -1 indicates Unavailable.

Copy Read Hits Dynamic Average A running average of the Copy Read Hits % attribute. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Copy Reads/sec The frequency of reads from cache pages that involve a memory copy of the data from the cache to the buffer for the application. The LAN Redirector uses this method to retrieve cache information, as does the LAN Server for small transfers. This is a method used by the disk file systems as well. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Data Flush Pages/sec The number of pages the cache has flushed to disk as a result of a request to flush or to satisfy a write-through file write request. More than one page can be transferred on each flush operation. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Data Flushes/sec The frequency with which the cache has flushed its contents to disk as the result of a request to flush or to satisfy a write-through file write request. More than one page can be transferred on each flush operation. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Data Map Hits % The percentage of data maps in the cache that could be resolved without having to retrieve a page from the disk, that is, the page was already in physical memory. Valid format is a numeric string in the range 0 to 100 (expressing a percentage).

Data Map Hits Dynamic Average A running average of the Data Map Hits % attribute. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Data Map Pins/sec The frequency of data maps in the cache that resulted in pinning a page in main memory, an action usually preparatory to writing to the file on disk. While pinned, the physical address for a page in main memory and the virtual address in the cache is not altered. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Data Maps/sec The number of times per second that a file system, such as NTFS or HPFS, maps a page of a file in to the cache to read the page. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fast Read Not Possibles/sec The frequency of attempts by an Application Program Interface (API) function call to bypass the file system to get at cache data that could not be honored without invoking the file system. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fast Read Resource Misses/sec The frequency of cache misses necessitated by the lack of available resources to satisfy the request. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fast Reads/sec The frequency of reads from cache pages that bypass the installed file system and retrieve the data directly from the cache. Normally, file I/O requests invoke the appropriate file system to retrieve data from a file, but this path permits direct retrieval of cache data without file system involvement if the data is in the cache. Even if the data is not in the cache, one invocation of the file system is avoided. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Lazy Write Flushes/sec The frequency with which the Lazy Write thread flushes its contents to disk. Lazy Writing is the process of updating the disk after the page has been changed in memory, so the application making the change to the file does not have to wait for the disk write to complete before proceeding. More than one page can be transferred on each write operation. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Lazy Write Pages/sec The frequency with which the Lazy Write thread for the cache writes to disk. Lazy Writing is the process of updating the disk after the page has been changed in memory, so the application making the change to the file does not have to wait for the disk write to complete before proceeding. More than one page can be transferred on a single disk write operation. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

MDL Read Hits % The percentage of cache Memory Descriptor List (MDL) read requests that hit the cache, that is, that did not require disk accesses to provide memory access to the page(s) in the cache. Valid format is a numeric string in the range 0 to 100 (expressing a percentage).

MDL Read Hits Dynamic Average A running average of the Memory Descriptor List (MDL) Read Hits % attribute. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

MDL Reads/sec The frequency of reads from cache pages that use a Memory Descriptor List (MDL) to access the data. The MDL contains the physical address of each page involved in the transfer, and thus can employ a hardware Direct Memory Access (DMA) device to effect the copy. The LAN Server uses this method for large transfers out of the server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pin Read Hits % The percentage of cache pin read requests that hit the cache, that is, that did not require a disk read to provide access to the page in the cache. While pinned, the physical address for the page in the cache is not altered. The LAN Redirector uses this method for retrieving cache information, as does the LAN Server for small transfers. This is usually the method used by the disk file systems as well. Valid format is a numeric string in the range 0 to 100 (expressing a percentage).

Pin Read Hits Dynamic Average A running average of the Pin Read Hits % attribute. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pin Reads/sec The frequency of reading data in to the cache preparatory to writing the data back to disk. Pages read in this fashion are pinned in memory at the completion of the read. While pinned, the physical address for a page in the cache is not altered. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Aheads/sec The frequency of cache reads where the cache detects sequential access to a file. The read aheads permit the data to be transferred in larger blocks than those being requested by the application, reducing the overhead per access. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sync Copy Reads/sec The frequency of reads from cache pages that involve a memory copy of the data from the cache to the buffer for the application. The file system does not regain control until the copy operation is complete, even if the disk must be accessed to retrieve the page. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sync Data Maps/sec The frequency with which a file system, such as NTFS or HPFS, maps a page of a file in to the cache to read the page, and wishes to wait for the cache to retrieve the page if it is not in main memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG,

*MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sync Fast Reads/sec The frequency of reads from cache pages that bypass the installed file system and retrieve the data directly from the cache. Normally, file I/O requests invoke the appropriate file system to retrieve data from a file, but this path permits direct retrieval of cache data without file system involvement if the data is in the cache. Even if the data is not in the cache, one invocation of the file system is avoided. If the data is not in the cache, the request (application program call) waits until the data is retrieved from disk. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sync MDL Reads/sec The frequency of reads from cache pages that use a Memory Descriptor List (MDL) to access the pages. The MDL contains the physical address of each page in the transfer, thus permitting Direct Memory Access (DMA) of the pages. If the accessed page(s) are not in main memory, the caller waits for the pages to fault in from the disk. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sync Pin Reads/sec The frequency of reading data in to the cache preparatory to writing the data back to disk. Pages read in this fashion are pinned in memory at the completion of the read. The file system does not regain control until the page is pinned in the cache, in particular if the disk must be accessed to retrieve the page. While pinned, the physical address for a page in the cache is not altered. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Computer Information attributes

Use Computer Information attributes to monitor general information about the computer system. The data source for these attributes is WMI. To avoid throughput issues with the Microsoft WMI stack, you should limit the collection frequency to 5 minute intervals. This ensures that the Microsoft WMI Data queues have sufficient time to service the WMI queries made for collecting these attributes.

Computer Domain Name The fully qualified domain name of the host computer. This value is resolved from the host IP address.

Computer Hostname The host name of the host computer. This value is resolved from the host IP address.

Computer ID Number This attribute value can be equal to the BIOS serial number for some Manufacturers. Typically this occurs when the computer system manufacturer and BIOS manufacturer are the same. This attribute value is set by the computer system manufacturer.

Computer Name Commonly used product name. This attribute value is set by the computer system manufacturer.

Computer System Description Computer system description. This attribute value is set by the computer system manufacturer.

Computer UUID Number Universally unique identifier (UUID) for this product. A UUID is a 128-bit identifier that is guaranteed to be different from other generated UUIDs. If a UUID is not available, a UUID of all zeros is used.

Computer Vendor Supplier name of the product. Corresponds to the Vendor property in the product object in the DMTF Solution Exchange Standard. This attribute value is set by the computer system manufacturer.

Computer Version Product version information. Corresponds to the Version property in the product object in the DMTF Solution Exchange Standard. This attribute value is set by the computer system manufacturer.

System Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month

DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Configuration Information attributes

Use Configuration Information attributes to monitor agent configuration such as Memory Threshold and Operating System.

Agent Name The sub agent name.

Agent Path The fully qualified path to agent.

Agent Type The watched agent type. The following values are valid: Unknown (0), ITM_Unix (1), Console (2), Windows_Service (3), Discover_ITM (4), Discover_Bin (5), Linux_Service (6), ITM_Windows (7).

Check Frequency The frequency to check status in seconds.

Configuration Script The agent configuration script.

% CPU Threshold The maximum CPU allowed.

Dependencies The dependent agents.

Manager Type The enum defining the manager type. The following values are valid: Unknown (0), Not_Managed (1), Agent_Management Services (2), Watchdog (3), External (4).

Maximum Daily Restarts The maximum number of restarts allowed. The clock begins at midnight.

Memory Threshold The maximum memory allowed.

Memory Unit The maximum memory allowed units. The following values are valid: Bytes (0), KB (1), MB (2), GB (3).

Operating System The operating system identification. The following values are valid: Unknown (0), Windows (1), Linux (2).

Operating System Name The operating system name.

Operating System Version The operating system version.

PAS_ID The PAS sub agent ID.

Policy File Timestamp The date and time of CAP file.

Process Name The process name of the managed agent.

Server Name The origin node of the collecting agent.

Service Name The service name.

Startup Script The agent startup script.

Status Script The agent status script.

Stop Script The agent stop script.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Device Dependencies attributes

Use the Device Dependencies attributes to obtain status and configuration information about all of the devices or load order groups that must start before a given device. Device Dependencies is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Dependency The name of a device or load order group that must start before the given device can start. If there are no dependencies for the given device, this field is blank. Valid format is a text string of up to 32 characters. For example, +SCSI miniport indicates the name of a device that must start before the given device can start.

Device Name The internal name of the device in the Service Control Manager database. The maximum size of the text string is 256 bytes, but here it is truncated to 64 bytes.

Display Name The name of the service as it is displayed in the Service Control Manager applet. Valid format is a text string of up to 64 characters. For example, Gateway Service indicates the name of the service.

Display Name (Unicode) The name of the device as it is displayed in the Service Control Manager applet in UTF8. Valid format is a text string of up to 388 bytes.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Devices attributes

Use the Devices attributes to create situations to obtain status and configuration information about all of the devices installed on the Windows Server. Devices is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Binary Path The fully qualified path to the device binary executable. Valid format is a text string of up to 64 characters. For example, `\SystemRoot\System32\drivers\afd.sys` indicates the path to the device binary executable.

Binary Path (Unicode) The fully qualified path to the device binary executable in UTF8. Valid format is a text string of up to 392 bytes.

Current State The current state of the device, which can be Stopped, Start Pending, Stop Pending, Running, Continue Pending, Paused Pending, or Paused. Valid format is a text string of up to 20 characters. For example, Running indicates that the device is currently running.

Device Name The internal name of the device in the Service Control Manager database. The maximum size of the text string is 256 bytes, but here it is truncated to 64 bytes.

Display Name The name of the driver as it is displayed in the Windows Service Control Manager applet. Valid format is a text string of up to 64 characters. For example, Cdrom is an example of a driver name.

Display Name (Unicode) The name of the driver as it is displayed in the Service Control Manager applet in UTF8. Valid format is a text string of up to 392 bytes.

Driver Object Name Specifies an object name. If the service is of type WIN32, this is the account name that the service uses to log on when it runs. If the service is

type Kernel Driver or File System Driver, this is the Windows Server's driver object name that the I/O Manager uses to load the device driver. Valid format is a text string of up to 32 characters.

Load Order Group The name of the load ordering group of which this device is a member. Devices can be placed in groups so other devices can have dependencies on a group of devices. If the device is not in a load ordering group, this field is blank. Valid format is a text string of up to 64 characters. For example, SCSI CDROM Class is an example of a load order group.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Start Type Specifies how to start the device. Valid format is a text string of up to 16 characters. The following values are valid:

- Automatic
- Manual
- Disabled
- Boot
- System
- Unknown

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

DHCP Server attributes

Use DHCP Server attributes to create situations to monitor Dynamic Host Configuration Protocol (DHCP) messages sent and received by the server, the average amount of processing time spent by the server per message packet, and the number of message packets dropped because of internal delays at the server. DHCP Server is a single-instance attribute group. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

Acks/sec Rate of DHCP Acks (acknowledgments) sent by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Active Queue Length The number of packets in the processing queue of the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Conflict Check Queue Length The number of packets in the DHCP server queue waiting on conflict detection (ping). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Declines/sec Rate of DHCP Declines received by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Discovers/sec Rate of DHCP Discovers received by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Duplicates Dropped/sec Rate at which the DHCP server received duplicate packets. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Informs/sec Rate of DHCP Informs received by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Milliseconds Per Packet Average The average time per packet taken by the DHCP server to send a response. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Nacks/sec Rate of DHCP Nacks (negative acknowledgments) sent by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Offers/sec Rate of DHCP Offers sent out by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG,

*MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Expired/sec Rate at which packets get expired in the DHCP server message queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Received/sec Rate at which packets are received by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Releases/sec Rate of DHCP Releases received by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Requests/sec Rate of DHCP Requests received by the DHCP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

DNS Dynamic Update attributes

Use DNS attributes to create situations to monitor DNS (Domain Name Server) server activity and performance. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

DNS Dynamic Update is a single-instance attribute group.

Dynamic Update NoOperation The total number of No-operation/Empty dynamic update requests received by the DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Dynamic Update NoOperation/sec The average number of No-operation/Empty dynamic update requests received by the DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Dynamic Update Queued The total number of dynamic updates queued by the DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Dynamic Update Received The total number of dynamic update requests received by the DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Dynamic Update Received/sec The average number of dynamic update requests received by the DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Dynamic Update Rejected The total number of dynamic updates rejected by the DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Dynamic Update TimeOuts The total number of dynamic update timeouts of the DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Dynamic Update Written to Database The total number of dynamic updates written to the database by the DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Dynamic Update Written to Database/sec The average number of dynamic updates written to the database by the DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Secure Update Failure The total number of secure updates failed of the DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Secure Update Received The total number of secure update requests received by the DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Secure Update Received/sec The average number of secure update requests received by the DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

DNS Memory attributes

Use DNS attributes to create situations to monitor DNS (Domain Name Server) server activity and performance. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

DNS Memory is a single-instance attribute group.

Caching Memory The total caching memory used by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Database Node Memory The total database node memory used by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Nbstat Memory The total Nbstat memory used by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Record Flow Memory The total record flow memory used by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

TCP Message Memory The total TCP message memory used by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour

MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

UDP Message Memory The total UDP message memory used by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

DNS Query attributes

Use DNS attributes to create situations to monitor DNS (Domain Name Server) server activity and performance. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

DNS Query is a single-instance attribute group.

Recursive Queries The total number of recursive queries received by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Recursive Queries/sec The average number of recursive queries received by DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Recursive Query Failure The total number of recursive query failures. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Recursive Query Failure/sec The average number of recursive query failures in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Recursive Send TimeOuts The total number of recursive query sending timeouts. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Recursive TimeOut/sec The average number of recursive query sending timeouts in each second. Valid values are positive integers in the range 0 to 2147483647 and

can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

TCP Query Received The total number of TCP queries received by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

TCP Query Received/sec The average number of TCP queries received by DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

TCP Response Sent The total number of TCP responses sent by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

TCP Response Sent/sec The average number of TCP responses sent by DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Query Received The total number of queries received by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of

the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Query Received/sec The average number of queries received by DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Response Sent The total number of responses sent by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Response Sent/sec The average number of responses sent by DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

UDP Query Received The total number of UDP queries received by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

UDP Query Received/sec The average number of UDP queries received by DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

UDP Response Sent The total number of UDP responses sent by DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

UDP Response Sent/sec The average number of UDP responses sent by DNS server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

DNS WINS attributes

Use DNS attributes to create situations to monitor DNS (Domain Name Server) server activity and performance.

DNS WINS is a single-instance attribute group.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

WINS Lookup Received The total number of WINS lookup requests received by the server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

WINS Lookup Received/sec The average number of WINS lookup requests received by the server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

WINS Response Sent The total number of WINS lookup responses sent by the server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

WINS Response Sent/sec The average number of WINS lookup responses sent by the server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

WINS Reverse Lookup Received The total number of WINS reverse lookup requests received by the server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

WINS Reverse Lookup Received/sec The average number of WINS reverse lookup requests received by the server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or

*SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

WINS Reverse Response Sent The total number of WINS Reverse lookup responses sent by the server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

WINS Reverse Response Sent/sec The average number of WINS Reverse lookup responses sent by the server in each second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

DNS Zone Transfer attributes

Use DNS attributes to create situations to monitor DNS (Domain Name Server) server activity and performance. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

DNS Zone Transfer is a single-instance attribute group.

AXFR Request Received The total number of full zone transfer requests received by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

AXFR Request Sent The total number of full zone transfer requests sent by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

AXFR Response Received The total number of full zone transfer responses received by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

AXFR Success Received The total number of successful full zone transfers received by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

AXFR Success Sent The total number of successful full zone transfers of the master DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IXFR Request Received The total number of incremental zone transfer requests received by the master DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM

functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IXFR Request Sent The total number of incremental zone transfer requests sent by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IXFR Response Received The total number of incremental zone transfer responses received by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IXFR Success Received The total number of successful incremental zone transfers received by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IXFR Success Sent The total number of successful incremental zone transfers of the master DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IXFR TCP Success Received The total number of successful TCP incremental zone transfers received by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IXFR UDP Success Received The total number of successful UDP incremental zone transfers received by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Notify Received The total number of notifies received by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Notify Sent The total number of notifies sent by the master DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Zone Transfer Failure The total number of failed zone transfers of the master DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Zone Transfer Request Received The total number of zone transfer requests received by the master DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Zone Transfer SOA Request Sent The total number of zone transfer SOA requests sent by the secondary DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Zone Transfer Success The total number of successful zone transfers of the master DNS server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Event Log attributes

Use Event Log attributes to create situations about actual records that are written to any Windows Event logs, such as date and time of the event and event identification information. Event Log is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

When building a query to collect log entries, the following applies:

- The operator is checked for ULogName and LogName. If ULogName and LogName are specified for the same clause (AND) ULogName is used. This is not recommended since the normal filter will likely throw away the results (no log will have ULogName == Application and LogName = Security, for example). The operator is checked for ULogName and LogName. If it is anything other than ==, the query fails, error entries are written to the log and no results are returned.
- EntryTime allows specification using >, >=, <, <=. Any other operators cause an error to be written to the log, and no results are returned.
- The agent returns up to 500 entries from each log identified in the query.
- The agent processes all of the logs identified in OR clauses using ULogName and LogName.
- Any filter elements other than U/LogName and EntryTime are handled by the agent infrastructure, so the results are filtered correctly.

Category The classification of the event as defined by the source. Valid format is a text string of up to 32 characters.

Category (Unicode) The classification of the event as defined by the source in UTF8. Valid format is a text string of up to 52 bytes.

Computer The name of the computer where the event occurs. Valid format is a text string of up to 16 characters.

Description A description of the event you are monitoring. Valid format is a text string of up to 64 characters.

Description (Unicode) The event detailed description in UTF8. Valid format is a text string of up to 1128 bytes.

Duplicate Record Count The number of duplicate records in the NT Event Log. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum. Controlled by these agent environment settings:

- NT_LOG_THROTTLE
- NT_{*Event Log Name*}_LOG_THROTTLE
- NT_APPLICATION_LOG_THROTTLE
- NT_SYSTEM_LOG_THROTTLE
- NT_SECURITY_LOG_THROTTLE
- NT_DNS_LOG_THROTTLE
- NT_DIRSERVICE_LOG_THROTTLE
- NT_FILEREPSRV_LOG_THROTTLE

For information on how to use environment variables to resolve high CPU usage due to situation behavior and to reduce the amount of records displayed in query views, see "Specific situation troubleshooting" on page 345.

Entry Time The date and time the event you are monitoring is logged. This is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C Century (0 for 20th, 1 for 21st)
YY Year

MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Event ID The identification code of the event you are monitoring. Valid format is a numeric string.

Event ID (String) Event ID represented as a string.

Log Name The name of a log. Valid format is a text string of up to 32 characters. The log names are case sensitive. Application is an example of a valid log name.

Log Name (Unicode) Log Name in UTF8. Valid format is a text string of up to 392 bytes. The log names are case sensitive. Application is an example of a valid log name.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Source The name of the application or component that logged the event you are monitoring. Valid format is a text string of up to 32 characters.

Source (Unicode) The software that logged the event, which can be an application name or a component of the system in UTF8. Valid format is a text string of up to 52 bytes.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Type The severity level of the event you are monitoring. Valid format is a case-sensitive text string of up to 16 characters (as described in the Event Type column). Possible values are:

Event Type	Description
Error	Serious, such as 'device driver not loading'
Warning	Cautionary, but not serious, such as 'low on disk space'
Information	Noteworthy, but not serious, such as 'successful operation achieved by an application'
Success	Indicates a successful procedure, such as 'an attachment to a shared printer'
Failure Audit	Failure of a procedure, such as 'a user attempting a procedure without correct privileges'

For example, Error indicates the severity level of the event you are monitoring is serious.

User The name of the user whose information you are monitoring. Valid format is a text string of up to 32 characters.

User (Unicode) The user name in UTF8. Valid format is a text string of up to 52 bytes.

File Change attributes

Use File Change attributes to monitor changes to your file system and to request notification when resources change. File Change is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Note: When defining a situation, the function *SCAN or wildcards (such as "*") are not supported in attributes containing the name or the path of the files.

When creating situations using the File Change attribute group you must supply values for the following attributes to restrict the monitoring for the situation:

- Watch Directory (Unicode)
- Watch File (Unicode) optional

The use of this attribute group requires that you set one or more filter conditions. The attributes that can be used in the filters are the following:

- Change File Name
- Change Directory Name
- Change Attributes
- Change Size
- Change Last Write
- Change Last Access
- Change Create
- Change Security
- Monitor all Conditions (activates all of the above)

Any query and situation must contain only one row of filter data in the situations formula. If more than one row is provided the results are undefined.

Note: The product provided File Change query does not produce data unless a situation is defined against this attribute group.

Action The type of change that occurred most recently to the directory or to the file. Valid values are positive integers in the range 0 to 5 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. The numbers 1 through 5 determine the type of change that recently occurred.

Number	Description
1	File/directory was added
2	File/directory was removed
3	File/directory changed (in size, in attribute, or in the security for the file/directory)
4	File/directory was renamed - the old name displays
5	File/directory was renamed - the new name displays

For example, to determine whether a file/directory was removed, enter 2.

Attributes The current attributes for the file. When used in a situation, this value does not act as a trigger condition for the situation. This value can be used as a filter condition after the situation has already been triggered by one of the predefined monitor conditions. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Change Attributes Selects monitoring for attribute changes. Valid value is a single character (y=Yes or n=No).

Change Create Selects monitoring for Create Date/Time changes. Valid value is a single character (y=Yes or n=No).

Change Directory Name Selects monitoring for directory name changes. Valid value is a single character (Y=yes or n=No).

Change File Name Selects monitoring for file name changes. Valid value is a single character (y=Yes or n=No).

Change Last Access Selects monitoring for Last Access date/time changes. Valid value is a single character (y=Yes or n=No).

Change Last Write Selects monitoring for Last Write date/time changes. Valid value is a single character (y=Yes or n=No).

Change Security Selects monitoring for security code changes. Valid value is a single character (y=Yes or n=No).

Change Size Selects monitoring for size changes. Valid value is a single character (y=Yes or n=No).

Current Size The current size of the file. When used in a situation, this value does not act as a trigger condition for the situation. This value can be used as a filter condition after the situation has already been triggered by one of the predefined monitor conditions. This attribute is the 64-bit version of Current_Size. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Current Size (Superseded) The current size of the file. When used in a situation, this value does not act as a trigger condition for the situation. This value can be used as a filter condition after the situation has already been triggered by one of the predefined monitor conditions. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Date Time Created The date and time at which the file was created. This information is displayed in the standard 16-character date/time format CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Date Time Last Modified The date and time the file was last modified. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Monitor all Conditions This attribute combines different types of filter criteria, allowing you to monitor the most recent file changes. You can use this attribute to trigger monitoring for all of the following attributes: Change Attributes, Change Create, Change Directory Name, Change File Name, Change Last Access, Change Last Write, Change Security, and Change Size. You can also use the above-listed attributes in individual situations to monitor for one or more conditions, such as the latest change to the file name or the last time a file was accessed. Valid value is a single character (y=Yes or n=No).

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Hits The total number of file/directory changes since monitoring began. This attribute is the 64-bit version of Total_Hits. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Total Hits (Superseded) The total number of file/directory changes since monitoring began. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Watch Directory The full path of the watched directory. Any changes to any files in the directory will be detected. Valid format is a text string of up to 260 characters. For example, `C:\FILESYS\USAGE`. A filter value is required for this attribute in situations using either the File Change attribute group or the File Trend attribute group.

Watch Directory (Unicode) The full path of the watched directory in UTF8. Any changes to any files in the directory will be detected. Valid format is a text string of up to 392 bytes. A filter value is required for this attribute in situations using either the File Change attribute group or the File Trend attribute group.

Watch File The name of the watched file. Valid format is a text string of up to 260 characters. For example, usage.log. A filter value is required for this attribute in situations using either the File Change attribute group or the File Trend attribute group.

Watch File (Unicode) The name of watched File in UTF8. Valid format is a text string of up to 392 bytes. A filter value is required for this attribute in situations using either the File Change attribute group or the File Trend attribute group.

Watch Tree The entire watch tree or only the directory. Valid value is a single character (y=Yes or n=No). y = to select monitoring for the entire watch tree. n = to select monitoring for the directory only. For example, y indicates that you are monitoring the entire watch tree.

File Trend attributes

Use File Trend attributes to monitor the growth rate in file space usage, by both change and absolute size change, over various monitoring periods. File Trend is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Note: When defining a situation, the function *SCAN or wildcards (such as "*") are not supported in attributes containing the name or the path of the files.

The File Trend attributes monitor the discrete files only and not subdirectories.

When creating situations using the File Trend attribute group you must supply values for the following attributes to restrict the monitoring for the situation:

- Watch Directory (Unicode)
- Watch File (Unicode) optional

Situations must contain only one row of filter data in the situations formula. If more than one row is provided the results are undefined.

Note: The product provided File Trend query does not produce data unless a situation is defined against this attribute group.

Attributes The file attributes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown.

% Change Average The percentage of change for the averaging take sample interval. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

% Change Last Hour The percentage rate of growth over the last hour. Valid format is a numeric string in the range 0 to 100 (expressing a percentage). Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

% Change Last Interval The percentage rate of growth over the last interval. Valid format is a numeric string in the range 0 to 100 (expressing a percentage). Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

% Change Total The percentage rate of growth change since monitoring began. Valid format is a numeric string in the range 0 to 100 (expressing a percentage). Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

% Used The percentage of the entire disk resource that a particular file takes. Valid format is a numeric string in the range 0 to 100 (expressing a percentage). Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Current Size The current size of the file. This attribute is the 64-bit version of Current Size. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Current Size (Superseded) The current size of the file. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Date Time Created The date and time the file was created. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Date Time Last Modified The date and time the file was last modified. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Free Space Exhausted Hours The time until current free space on the volume is exhausted based on the size change rate over the last hour. If there is no size change detected over the last hour then the Free Space Exhausted Hours value is zero(0). Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum. Standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm. Note: -1 indicates Unknown.

Sampling Interval The time between successive samples. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Sampling Number The number of intervals that are sampled to get an average. Valid values are positive integers in the range 2 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Size Change Average The average absolute file size change. This attribute is the 64-bit version of Size Change Average. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Size Change Average (Superseded) The average absolute file size change. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Size Change Last Hour The average absolute file size change over the last hour. This attribute is the 64-bit version of Size Change LastHour. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Size Change Last Hour (Superseded) The average absolute file size change over the last hour. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Size Change Last Interval The average absolute file size change over the last interval. This attribute is the 64-bit version of Size_Change_LastInterval. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Size Change Last Interval (Superseded) The average absolute file size change over the last interval. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Size Change Total The absolute file size change since monitoring began expressed as a percentage. This attribute is the 64-bit version of Size Change Total. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Size Change Total (Superseded) The absolute file size change since monitoring began expressed as a percentage. Valid values are positive integers in the range of

0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Watch Directory The full path of the watched directory. Any changes to any files in the directory will be detected. Valid format is a text string of up to 260 characters. For example, C:\ADMIN\USAGE. A filter value is required for this attribute in situations using either the File Change attribute group or the File Trend attribute group. This attribute monitors the discrete files only and not subdirectories.

Watch Directory (Unicode) The full path of the watched directory. Any changes to any files in the directory will be detected. Valid format is a text string of up to 392 bytes. A filter value is required for this attribute in situations using either the File Change attribute group or the File Trend attribute group. This attribute monitors the discrete files only and not subdirectories.

Watch File The name of the watched file. Valid format is a text string of up to 260 characters. For example, `usage.log`. A filter value is required for this attribute in situations using either the File Change attribute group or the File Trend attribute group. This attribute monitors the discrete files only and not subdirectories.

Watch File (Unicode) The name of watched file. Valid format is a text string of up to 392 bytes. A filter value is required for this attribute in situations using either the File Change attribute group or the File Trend attribute group. This attribute monitors the discrete files only and not subdirectories.

FTP Server Statistics attributes

Use FTP Server Statistics attributes to monitor traffic and connection activity about the FTP (File Transfer Protocol) Server, such as the current connections, the bytes received per second, and the total non-anonymous users connected. FTP Server Statistics is a single-instance attribute group. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

Bytes Received/sec The number of bytes received per second by the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the

use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The number of data bytes sent per second by the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connection Attempts Since FTP Start The number of connection attempts since the FTP server was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Anonymous Users The number of anonymous users currently connected to the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Connections The current number of connections to the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Non-Anonymous Users The number of non-anonymous users currently connected to the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Received The number of files received by the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Sent The number of files sent by the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Logon Attempts Since FTP Start The number of logon attempts since the FTP server was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum Anonymous Users The maximum number of anonymous users simultaneously connected to the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or

*SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum Connections The maximum number of simultaneous connections to the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum NonAnonymous Users The maximum number of non-anonymous users simultaneously connected to the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Anonymous Users Since FTP Start The total number of anonymous users connected since the FTP server was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Bytes/sec The total number of Kbytes flowing through the FTP server per second. This includes both incoming and outgoing bytes. This number is a good indicator of how heavily your FTP server is loaded. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Files The total number of files sent and received by the FTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Non-Anonymous Users Since FTP Start The total number of non-anonymous users connected since the FTP server was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

FTP Service attributes

Use FTP Service attributes to create situations that monitor traffic and connection activity for an FTP (File Transfer Protocol) server. FTP Service is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Bytes Received/sec The rate that data bytes are received by the FTP service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate that data bytes are sent by the FTP service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Total/sec The sum of Bytes Sent/sec and Bytes Received/sec. This is the total rate of bytes transferred by the FTP service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Anonymous Users The number of users who currently have an anonymous connection using the FTP service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Connections The current number of connections established with the FTP service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current NonAnonymous Users The number of users who currently have a non-anonymous connection using the FTP service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

FTP Site Name of File Transfer Protocol site. Valid format is a text string of up to 64 characters.

Maximum Anonymous Users The maximum number of users who established concurrent anonymous connections using the FTP service (since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum Connections The maximum number of simultaneous connections established with the FTP service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum Non Anonymous Users The maximum number of users who established concurrent non-anonymous connections using the FTP service (since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Anonymous Users The total number of users who established an anonymous connection with the FTP service (since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Connection Attempts The number of connections that have been attempted using the FTP service (since service startup). This counter is for all instances listed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Files Received The total number of files received by the FTP service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Files Sent The total number of files sent by the FTP service since service startup. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Files Transferred The sum of Files Sent and Files Received. This is the total number of files transferred by the FTP service since service startup. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Logon Attempts The number of logons that have been attempted using the FTP service (since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Non Anonymous Users The total number of users who established a non-anonymous connection with the FTP service (since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Gopher Service attributes

Use Gopher Service attributes to monitor traffic and connection activity for a Gopher server, such as the current connections, the bytes received per second, and the total non-anonymous users connected. Gopher Service is a single-instance attribute group. Gopher Service attributes are only supported for Windows NT and earlier.

Aborted Connections Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The rate that bytes are received by the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

BYTSNTSE

Bytes Sent/sec The rate that bytes are sent by the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

BYTTOTSE

Bytes Total/sec The total number of KBs flowing through the Gopher server per second. This includes both incoming and outgoing bytes. This number is a good indicator of how heavily your Gopher server is loaded. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

CONNATMP

Connection Attempts The number of connections that had errors when processed by the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

CONNERR

Connections in Error The number of connections that had errors when processed by the Gopher Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

CURANUSR

Current Anonymous Users The number of anonymous users currently connected to the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

CURRCONN

Current Connections The current number of connections to the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

CURNAUSR

Current NonAnonymous Users The number of non-anonymous users currently connected to the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

DIRLSTSE

Directory Listings Sent The total number of directory listings sent by the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can

include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

FILESENT

Files Sent The total number of files sent by the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

GPHRPREQ

Gopher Plus Requests The number of Gopher Plus requests received by the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

LOGATMPS

Logon Attempts The number of logon attempts that have been made by the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

MAXANUSR

Maximum Anonymous Users The maximum number of anonymous users simultaneously connected to the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

MAXCONN

Maximum Connections The number of connection attempts that have been made to the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

MAXNAUSR

Maximum NonAnonymous Users The maximum number of non-anonymous users simultaneously connected to the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

SRCHSENT

Searches Sent The total number of searches performed by the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

ORIGINNODE

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

`TIMESTAMP`

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

`TOTANUSR`

Total Anonymous Users The total number of anonymous users that have ever connected to the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

`TOTNAUSR`

Total NonAnonymous Users The total number of non-anonymous users that have ever connected to the Gopher server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

HTTP Content Index attributes

Use HTTP Content Index attributes to monitor queries made to an HTTP (HyperText Transport Protocol) server, such as the number of active queries, the current requests queued, and the percentage of queries found in the query cache. HTTP Content Index is a single-instance attribute group. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

Active Queries The current number of running queries. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

% Cache Hits The percentage of queries found in the query cache. Valid format is a numeric string in the range 0 to 100 (expressing a percentage).

Cache Items The number of completed queries in cache. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

% Cache Misses The percentage of queries not found in the query cache. Valid format is a numeric string in the range 0 to 100 (expressing a percentage).

Current Requests Queued The current number of query requests queued. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Queries Per Minute The number of queries per minute. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Queries The total number of queries since the server started up. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Requests Rejected The total number of query requests rejected. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

HTTP Service attributes

Use HTTP Service attributes to monitor traffic and connection activity for an HTTP (HyperText Transport Protocol) server, such as the current connections, the bytes received per second, and the total anonymous users connected. HTTP Service is a single-instance attribute group.

Bytes Received/sec The rate that data bytes are received by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate that data bytes are sent by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Total/sec The sum of bytes sent per second and bytes received per second. This is the total rate of bytes transferred by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

CGI Requests Common Gateway Interface (CGI) requests are custom gateway executables (exe). An administrator can install these executables to add forms processing or other dynamic data sources. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connection Attempts The number of connection attempts that have been made to the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connections/sec The number of HTTP requests being handled per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Anonymous Users The number of anonymous users currently connected to the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current CGI Requests The current number of CGI requests that are simultaneously being processed by the HTTP server. This includes WAIS index queries. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Connections The current number of connections to the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current ISAPI Extension Requests The number of ISAPI (Internet Server API) Extension requests that are simultaneously being processed by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current NonAnonymous Users The number of non-anonymous users currently connected to the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Received The total number of files received by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Sent The total number of files sent by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Total The sum of files sent and files received. This is the total number of files transferred by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Get Requests The number of HTTP requests using the GET method. Get requests are generally used for basic file retrievals or image maps, though they can be used with forms. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Head Requests The number of HTTP requests using the HEAD method. Head requests generally indicate a client is querying the state of a document they already have to see if it needs to be refreshed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or

*SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ISAPI Extension Requests The number of ISAPI Extension requests. ISAPI Extension requests are custom gateway Dynamic Link Libraries (.dll) an administrator can install to add forms processing to other dynamic data sources. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Logon Attempts The number of logon attempts that have been made by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum Anonymous Users The maximum number of anonymous users simultaneously connected to the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum CGI Requests The maximum number of CGI requests that have been simultaneously processed by the HTTP server. This includes WAIS index queries. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum Connections The maximum number of simultaneous connections to the HTTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum ISAPI Extension Requests The maximum number of ISAPI Extension requests that have been simultaneously processed by the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum NonAnonymous Users The maximum number of non-anonymous users simultaneously connected to the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Not Found Errors The number of requests that could not be satisfied by the server because the requested document could not be found. These are generally reported as an HTTP 404 error code to the client. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Other Requests The number of HTTP requests that are not GET, POST, or HEAD methods. These might include PUT, DELETE, LINK, or other methods supported by gateway applications. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Post Requests The number of HTTP requests using the POST method. Post requests are generally used for forms or gateway requests. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Anonymous Users The total number of anonymous users that have ever connected to the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total NonAnonymous Users The total number of non-anonymous users that have ever connected to the HTTP server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ICMP Statistics attributes

Use ICMP Statistics attributes to monitor message traffic. ICMP (Internet Control Message Protocol) messages are used to convey the results of network commands, such as the PING command. ICMP Statistics is a single-instance attribute group.

Messages/sec The total rate that ICMP messages that are received and sent by the entity. The rate includes those messages received or sent in error. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Outbound Errors The number of ICMP messages that this entity did not send due to problems discovered within ICMP, such as lack of buffers. This value must not include errors discovered outside the ICMP layer, such as the inability of IP to rout the resultant datagram. In some implementations, there might not be any types of error that contribute to the value of the counter. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Received Errors The number of ICMP messages that the entity received but determined as having errors (bad ICMP checksums, bad length, and so on). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Received/sec The rate that ICMP messages are received by the entity. The rate includes those messages received in error. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Sent/sec The rate that ICMP messages are attempted to be sent by the entity. The rate includes those messages sent in error. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Address Mask The number of ICMP Address Mask Request messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Received Address Mask Reply The number of ICMP Address Mask Reply messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Destination Unreachable The number of ICMP Destination Unreachable messages received. Valid values are positive integers in the range 0 to 2147483647

and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Echo/sec The rate of ICMP Echo messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Received Echo Reply/sec The rate of ICMP Echo Reply messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Parameter Problem The number of ICMP Parameter Problem messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Redirect/sec The rate of ICMP Redirect messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Source Quench The number of ICMP Source Quench messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Time Exceeded The number of ICMP Time Exceeded messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Timestamp/sec The rate of ICMP Timestamp (request) messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Received Timestamp Reply/sec The rate of ICMP Timestamp Reply messages received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Address Mask The number of ICMP Address Mask Request message sent. Valid values are positive integers in the range 0 to 2147483647 and can include the

use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Address Mask Reply The number of ICMP Address Mask Reply messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Sent Destination Unreachable The number of ICMP Destination Unreachable messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Echo/sec The rate of ICMP Echo messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Echo Reply/sec The rate of ICMP Echo Reply messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Parameter Problem The number of ICMP Parameter Problem messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Redirect/sec The rate of ICMP Redirect messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Source Quench The number of ICMP Source Quench messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Time Exceeded The number of ICMP Time Exceeded messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Timestamp/sec The rate of ICMP Timestamp (request) messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sent Timestamp Reply/sec The rate of ICMP Timestamp Reply messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

IIS Statistics attributes

Use IIS Statistics attributes to monitor memory usage and connection data. IIS (Internet Information Server) Statistics is a single-instance attribute group. If the service being monitored is not installed or if the service is minimally loaded most attributes report 0 values.

Cache Flushes The number of times a portion of the memory cache has expired due to the file or directory changes in an IIS directory tree. Note that this attribute is not available on systems running Windows 2000 with IIS 5.0. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cache Hits The total number of times a file open, a directory listing, or a service-specific object request was found in the cache. Note that this attribute is not available on systems running Windows 2000 with IIS 5.0. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cache Hits % The ratio of cache hits to all cache requests. Note that this attribute is not available on systems running Windows 2000 with IIS 5.0. Valid values are

positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown.

Cache Misses The total number of times a file open, a directory listing, or a service-specific object request was not found in the cache. Note that this attribute is not available on systems running Windows 2000 with IIS 5.0. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cache Size The configured maximum size of the shared HTTP, FTP, and Gopher memory cache. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cache Used The total number of bytes currently containing cached data in the shared memory cache. This includes directory listings, file handle tracking, and service-specific objects. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cached Directory Listings The number of directory listing objects cached by all of the IIS. Note that this attribute is not available on systems running Windows 2000 with IIS 5.0. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cached File Handles The number of open file handles cached by all of the IIS. Note that this attribute is not available on systems running Windows 2000 with IIS 5.0. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cached Objects The number of objects cached by all of the IIS. The objects include file handle tracking objects, directory listing objects, and service-specific objects. Note that this attribute is not available on systems running Windows 2000 with IIS 5.0. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Current Blocked Async I/O Requests The current number of asynchronous I/O requests blocked by the bandwidth throttler. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Measured Async I/O Bandwidth Usage The number of measured bandwidth of asynchronous I/O averaged over a minute. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM

functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Allowed Async Requests The total number of asynchronous I/O requests allowed by the bandwidth throttler. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Blocked Async I/O Requests The total number of asynchronous I/O requests blocked by the bandwidth throttler. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Rejected Async Requests The total number of asynchronous I/O requests rejected by the bandwidth throttler. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Indexing Service attributes

Use Index Service attributes to monitor the creation of indices and the merging of indices by the indexing service. Indexing Service is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Deferred for Indexing Number of files not available and deferred for indexing. Note that this attribute is not available in IIS 4.0. Valid values are positive integers

in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Files to be Indexed Number of files to be filtered and added to the index. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Index A collection of all index information and stored properties for a particular group of file system directories. Valid format is a text string of up to 64 characters.

Index (Unicode) A collection of all index information and stored properties for a particular group of file system directories. Valid format is a text string of up to 392 bytes.

Index Size MB Size of the content index (ci files only) in MBs. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Merge Progress Percent merge complete for the current merge. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Number of Documents Indexed Number of documents indexed since the current indexing session started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Running Queries Number of active query client connections. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Saved Indexes Number of saved indexes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Number of Documents Total number of documents in the index. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Number of Queries Total number of queries since the index was mounted. Note that this attribute is not available in IIS 4.0. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Unique Keys Number of unique keys (words, etc) in the index. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Word Lists Number of word lists. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Indexing Service Filter attributes

Use Index Service Filter attributes to monitor indexing speed and binding time. Indexing Service Filter is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Binding Time mSec Average time spent binding to indexing filters. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Index A collection of all index information and stored properties for a particular group of file system directories. Valid format is a text string of up to 64 characters.

Index (Unicode) A collection of all index information and stored properties for a particular group of file system directories. Valid format is a text string of up to 392 bytes.

Indexing Speed MB/hr Speed of the indexing of file contents in MBs per hour. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Indexing Speed MB/hr Speed of indexing file contents and properties in MBs per hour. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IP Address attributes

Use IP Address attributes to obtain IP (Internet Protocol) address information.

DNS Name The Domain Name Server entry associated with the IP network address.

IP Address An IP address associated with the network interface.

IP Version An indicator as to whether the IP address is version 4 or version 6. Valid values include IPv4 (4), IPv6 (6), and IPv4_IPv6 (10). The value for IPv4_IPv6 relates to the Automatic Tunneling Pseudo Interface for the Windows Server 2003 and Windows XP operating systems. These pseudo processes include, System, Idle, and _Total.

MAC Address The MAC address of the network interface.

Network Interface Name The name of the network interface. The value Not Available indicates Not Available for Windows 2000.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

IP Statistics attributes

Use IP Statistics attributes to monitor traffic and fragmentation statistics for data using the IP (Internet Protocol) protocol. IP Statistics is a single-instance attribute group.

Note: IBM Tivoli Monitoring v.6.x does not support IPV6.

Datagram Fragmentation Percentage Measure of datagram fragmentation. Calculated as 100 * (Fragments Received/sec ÷ Datagrams Received/sec). Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Datagrams/sec The rate that IP datagrams are received from or sent to the interfaces, including those in error. Any forwarded datagrams are not included. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Forwarded/sec The rate of input datagrams for this entity was not their final IP destination. An attempt was made to find a route to forward the datagrams to their final destination. In entities that do not act as IP gateways, this rate includes only those packets that were Source-Routed via this entity, and the Source-Route option processing was successful. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Outbound Discarded The number of output IP datagrams for which no problems were encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space). This counter includes datagrams counted in Datagrams Forwarded, if any such packets met this (discretionary) discard criterion. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Outbound No Route The number of IP datagrams discarded because no route could be found to transmit them to their destination. This counter includes any packets counted in Datagrams Forwarded that meet this 'no route' criterion. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Received Address Errors The number of input datagrams discarded because the IP address in their IP header destination field was not a valid address to be received at this entity. This count includes addresses that are not valid (for example, 0.0.0.0) and addresses for classes that are not supported (such as Class E). For entities that are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Received Delivered/sec The rate that input datagrams are successfully delivered to IP user-protocols (including ICMP). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Received Discarded The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). This counter does not include any datagrams discarded while awaiting re-assembly. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Received Header Errors The number of input datagrams discarded due to errors in their IP headers, such as bad checksums, version mismatch, other format errors, time-to-live exceeded, and errors discovered in processing their IP options. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Received/sec The rate that IP datagrams are received from the interfaces, including those in error. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Received Unknown Protocol The number of locally-addressed datagrams received successfully, but discarded because of an unknown or unsupported protocol. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Sent/sec The rate that IP datagrams are supplied to IP for transmission by the local IP user-protocols (including ICMP). This counter does not include any datagrams counted in Datagrams Forwarded. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fragment Re-assembly Failures The number of failures detected by the IP re-assembly algorithm (such as time out, errors, and so on). This is not necessarily a count of discarded IP fragments since some algorithms (notably RFC 815) can lose track of the number of fragments by combining them as they are received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fragmentation Failures The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be. This happens due to setting the Don't Fragment flag. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fragmented Datagrams/sec The rate that datagrams are successfully fragmented at this entity. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fragments Created/sec The rate that datagrams are successfully fragmented at this entity. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fragments Re-assembled/sec The rate that IP fragments are successfully re-assembled. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Fragments Received/sec The rate that IP fragments that need to be re-assembled at this entity are received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Job Object attributes

Use Job Object attributes to create situations that monitor job kernel objects, the system resources a job consumes, and the number of processes a job contains. Job Object is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Current % Kernel Mode Time Shows the percentage of the monitoring interval that the processes in the Job object spent executing code in kernel or privileged mode. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Current % Processor Time Shows the percentage of the monitoring interval that the process in the Job object spent executing code. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Current % User Mode Time Shows the percentage of the monitoring interval that the processes in the Job object spent executing code in user mode. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Name Name of Job kernel object. Valid format is a text string of up to 64 characters.

Name (Unicode) Instance name (Job Object) in UTF8. The maximum job object name size is defined by MAX_PATH. Valid format is a text string of up to 392 bytes.

Pages/sec Shows the page fault rate of all the processes in the Job object. Valid values are positive integers in the range 0 to 2147483647 and can include the use of

the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Process Count Active Shows the number of processes that are currently associated with the Job object. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Process Count Terminated Shows the number of processes that have been terminated because of a limit violation. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Process Count Total Shows the number of processes, both active and terminated, that are or have been associated with the Job object. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

This Period mSec Kernel Mode Shows the number of milliseconds of kernel mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the last time a time limit on the Job was established. This attribute is the 64-bit version of This Period mSec Kernel Mode. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

This Period mSec Kernel Mode (Superseded) Shows the number of milliseconds of kernel mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the last time a time limit on the Job was established. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

This Period mSec Processor Shows the number of milliseconds of processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the last time a time limit on the Job was established. This attribute is the 64-bit version of This Period mSec Processor. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

This Period mSec Processor (Superseded) Shows the number of milliseconds of processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the last time a time limit on the Job was established. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

This Period mSec User Mode Shows the number of milliseconds of user mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the last time a time limit on the Job was established. This attribute is the 64-bit version of This Period mSec User Mode. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

This Period mSec User Mode (Superseded) Shows the number of milliseconds of user mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the last time a time limit on the Job was established. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total mSec Kernel Mode Shows the number of milliseconds of kernel mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the Job object was created. This attribute is the 64-bit version of Total mSec Kernel Mode. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Total mSec Kernel Mode (Superseded) Shows the number of milliseconds of kernel mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the Job object was created. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Total mSec Processor Shows the number of milliseconds of processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the Job object was created. This attribute is the 64-bit version of Total mSec Processor. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Total mSec Processor (Superseded) Shows the number of milliseconds of processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the Job object was created. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Total mSec User Mode Shows the number of milliseconds of user mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the Job object was created. This attribute is the 64-bit version of Total_mSec_User_Mode. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Total mSec User Mode (Superseded) Shows the number of milliseconds of user mode processor time used by all the processes in the Job object, including those that have terminated or that are no longer associated with the Job object, since the Job object was created. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Job Object Details Attributes

Use Job Object Details attributes to create situations that monitor details of individual job kernel objects, including system resources a job consumes and the processes that job contains. Job Object Details is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Privileged Time The percentage of elapsed time that the threads of the process have spent executing code in privileged mode. When a Windows Server's service is called, the service often runs in Privileged Mode to gain access to system-private data. Such data is protected from access by threads executing in user Mode.

Calls to the system can be explicit or implicit, such as page faults or interrupts. Unlike some early operating systems, Windows NT and higher versions of Windows Servers use process boundaries for subsystem protection in addition to the traditional protection of user and privileged modes. These subsystem processes provide additional protection. Therefore, some work done by Windows Server on behalf of your application might appear in other subsystem processes in addition to the privileged time in your process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Processor Time The percentage of elapsed time that all of the threads of this process used the processor to execute instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a

process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions are included in this count. On Multi-processor systems the maximum value of the counter is 100 % times the number of processors. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% User Time The percentage of elapsed time that this threads of this process have spent executing code in user mode. Applications, environment subsystems and integral subsystems execute in user mode. Code executing in user mode cannot damage the integrity of the Windows Server Executive, Kernel, and device drivers. Unlike some early operating systems, Windows NT and higher versions of Windows Servers use process boundaries for subsystem protection in addition to the traditional protection of user and privileged modes. These subsystem processes provide additional protection. Therefore, some work done by Windows Server on behalf of your application might appear in other subsystem processes in addition to the privileged time in your process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Creating Process ID The Process ID of the creating process. Note that the creating process might have terminated since this process was created, and so this value might no longer identify a running process. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Elapsed Time The total elapsed time (in seconds) this process has been running. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Handle Count The total number of handles currently open by this process. This number is the sum of the handles currently open by each thread in this process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ID Process The unique identifier of this process. ID Process numbers are reused, so they only identify a process for the lifetime of that process. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

IO Data Bytes/sec The rate the process is reading and writing bytes in I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

IO Data Operations/sec The rate the process is issuing read and write I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

IO Other Bytes/sec The rate the process is issuing bytes to I/O operations that do not involve data such as control operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Note: the value

9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

IO Other Operations/sec The rate the process is issuing I/O operations that are neither a read or a write operation. An example of this type of operation would be a control function. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

IO Read Bytes/sec The rate the process is reading bytes from I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

IO Read Operations/sec The rate the process is issuing read I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

IO Write Bytes/sec The rate the process is writing bytes to I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

IO Write Operations/sec The rate the process is issuing write I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Page Faults/sec The rate Page Faults occur in the threads executing in this process. A page fault occurs when a thread refers to a virtual memory page that is not in its working set in main memory. This does not cause the page to be fetched from disk if it is on the standby list and hence already in main memory, or if it is in use by another process with whom the page is shared. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Page File Bytes The current number of bytes this process has used in the paging file(s). Paging files are used to store pages of memory used by the process that are not contained in other files. Paging files are shared by all processes, and lack of space in paging files can prevent other processes from allocating memory. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Page File Bytes Peak The maximum number of bytes this process has used in the paging file(s). Paging files are used to store pages of memory used by the process that are not contained in other files. Paging files are shared by all processes, and lack of space in paging files can prevent other processes from allocating memory. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Page File kBytes Page File Bytes in KBs. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Page File kBytes Peak Page File Bytes Peak in KBs. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Pool Nonpaged Bytes The number of bytes in the nonpaged pool, an area of system memory (physical memory used by the operating system) for objects that cannot be written to disk, but must remain in physical memory as long as they are allocated. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Bytes The number of bytes in the paged pool, an area of system memory (physical memory used by the operating system) for objects that can be written to disk when they are not being used. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Priority Base The current base priority of this process. Threads within a process can raise and lower their own base priority relative to the process' base priority. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Private Bytes The current number of bytes this process has allocated that cannot be shared with other processes. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Private kBytes Private Bytes in KBs. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Process Name of process in UTF8. The maximum process name size is defined by MAX_PATH.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Thread Count The number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Virtual Bytes The current size in bytes of the virtual address space the process is using. Use of virtual address space does not necessarily imply corresponding use of either disk or main memory pages. Virtual space is finite, and by using too much, the process can limit its ability to load libraries. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Virtual Bytes Peak Virtual Bytes Peak is the maximum number of bytes of virtual address space the process has used at any one time. Use of virtual address space does not necessarily imply corresponding use of either disk or main memory pages. Virtual space is however finite, and by using too much, the process might limit its ability to load libraries. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Virtual kBytes Virtual Bytes in KBs. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Virtual kBytes Peak Virtual Bytes Peak in KBs. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Working Set The current number of bytes in the Working Set of this process. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed, they are soft-faulted back in to the Working Set before they leave main memory. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Working Set Peak The maximum number of bytes in the Working Set of this process at any point in time. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed, they are soft-faulted back in to the Working Set before they

leave main memory. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Job Object Details Attributes (32-bit - Superseded)

Use Job Object Details attributes to create situations that monitor details of individual job kernel objects, including system resources a job consumes and the processes that job contains. Job Object Details is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group. This attribute group is superseded. There is a new attribute group with the same name that replaces it.

% Privileged Time The percentage of elapsed time that the threads of the process have spent executing code in privileged mode. When a Windows Server's service is called, the service often runs in Privileged Mode to gain access to system-private data. Such data is protected from access by threads executing in user Mode. (Superseded.)

Calls to the system can be explicit or implicit, such as page faults or interrupts. Unlike some early operating systems, Windows NT and higher versions of Windows Servers use process boundaries for subsystem protection in addition to the traditional protection of user and privileged modes. These subsystem processes provide additional protection. Therefore, some work done by Windows Server on behalf of your application might appear in other subsystem processes in addition to the privileged time in your process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Processor Time The percentage of elapsed time that all of the threads of this process used the processor to execute instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions are included in this count. On Multi-processor systems the maximum value of the counter is 100 % times the number of processors. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.)

% User Time The percentage of elapsed time that this threads of this process have spent executing code in user mode. Applications, environment subsystems and integral subsystems execute in user mode. Code executing in user mode cannot damage the integrity of the Windows Server Executive, Kernel, and device drivers. Unlike some early operating systems, Windows NT and higher versions of Windows Servers use process boundaries for subsystem protection in addition to the traditional protection of user and privileged modes. These subsystem processes provide additional protection. Therefore, some work done by Windows Server on behalf of your application might appear in other subsystem processes in addition to the privileged time in your process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.)

Creating Process ID The Process ID of the creating process. Note that the creating process might have terminated since this process was created, and so this value might no longer identify a running process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or

*SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Elapsed Time The total elapsed time (in seconds) this process has been running. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Handle Count The total number of handles currently open by this process. This number is the sum of the handles currently open by each thread in this process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ID Process The unique identifier of this process. ID Process numbers are reused, so they only identify a process for the lifetime of that process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

IO Data Bytes/sec The rate the process is reading and writing bytes in I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IO Data Operations/sec The rate the process is issuing read and write I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IO Other Bytes/sec The rate the process is issuing bytes to I/O operations that do not involve data such as control operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IO Other Operations/sec The rate the process is issuing I/O operations that are neither a read or a write operation. An example of this type of operation would be a control function. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IO Read Bytes/sec The rate the process is reading bytes from I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IO Read Operations/sec The rate the process is issuing read I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IO Write Bytes/sec The rate the process is writing bytes to I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IO Write Operations/sec The rate the process is issuing write I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/O's. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page Faults/sec The rate Page Faults occur in the threads executing in this process. A page fault occurs when a thread refers to a virtual memory page that is not in its working set in main memory. This does not cause the page to be fetched from disk if it is on the standby list and hence already in main memory, or if it is in use by another process with whom the page is shared. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page File Bytes The current number of bytes this process has used in the paging file(s). Paging files are used to store pages of memory used by the process that are not contained in other files. Paging files are shared by all processes, and lack of space in paging files can prevent other processes from allocating memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page File Bytes Peak The maximum number of bytes this process has used in the paging file(s). Paging files are used to store pages of memory used by the process that are not contained in other files. Paging files are shared by all processes, and lack of space in paging files can prevent other processes from allocating memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page File kBytes Page File Bytes in KBs. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page File kBytes Peak Page File Bytes Peak in KBs. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged Bytes The number of bytes in the nonpaged pool, an area of system memory (physical memory used by the operating system) for objects that cannot be written to disk, but must remain in physical memory as long as they are allocated. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Bytes The number of bytes in the paged pool, an area of system memory (physical memory used by the operating system) for objects that can be written to disk when they are not being used. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Priority Base The current base priority of this process. Threads within a process can raise and lower their own base priority relative to the process' base priority. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.)

Private Bytes The current number of bytes this process has allocated that cannot be shared with other processes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Private kBytes Private Bytes in KBs. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Process Name of process. Valid format is a text string of up to 64 characters. (Superseded.)

Process (Unicode) Instance name (Process) in UTF8. The maximum process name size is defined by MAX_PATH. Valid format is a text string of up to 392 bytes. (Superseded.)

Server Name The managed system name. The form should be *hostname:agent_code*. (Superseded.)

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Thread Count The number of threads currently active in this process. An instruction is the basic unit of execution in a processor, and a thread is the object that executes instructions. Every running process has at least one thread. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data (Superseded). This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Virtual Bytes The current size in bytes of the virtual address space the process is using. Use of virtual address space does not necessarily imply corresponding use of either disk or main memory pages. Virtual space is finite, and by using too much, the process can limit its ability to load libraries. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Virtual Bytes Peak Virtual Bytes Peak is the maximum number of bytes of virtual address space the process has used at any one time. Use of virtual address space does not necessarily imply corresponding use of either disk or main memory pages. Virtual space is however finite, and by using too much, the process might limit its ability to load libraries. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Virtual kBytes Virtual Bytes in KBs. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Virtual kBytes Peak Virtual Bytes Peak in KBs. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or

*SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Working Set The current number of bytes in the Working Set of this process. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed, they are soft-faulted back in to the Working Set before they leave main memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Working Set Peak The maximum number of bytes in the Working Set of this process at any point in time. The Working Set is the set of memory pages touched recently by the threads in the process. If free memory in the computer is above a threshold, pages are left in the Working Set of a process even if they are not in use. When free memory falls below a threshold, pages are trimmed from Working Sets. If they are needed, they are soft-faulted back in to the Working Set before they leave main memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Logical Disk attributes

Use Logical Disk attributes to create situations that monitor information about disk drive partitions that have been assigned a drive letter. Logical disk is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Disk Read Time The percentage of elapsed time a logical disk has been busy servicing read requests. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. The value -1 indicates Unavailable.

% Disk Time The percentage of elapsed time that a logical disk has been busy servicing read and write requests. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. The value -1 indicates Unavailable.

% Disk Write Time The percentage of elapsed time that a logical disk drive has been busy servicing write requests. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. The value -1 indicates Unavailable.

% Free The percentage of the volume that is free space. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. The value -1 indicates Unavailable.

% Used The percentage of the volume that is used. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. The value -1 indicates Unavailable.

Avg Disk ms/Read The average amount of time for a read of data from a logical disk. Valid values are positive integers in the range 0 to 2147483647 (expressing milliseconds) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Average Disk Queue Length The average number of both read and write requests that were queued for the selected disk during the sample interval. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Average Disk Read Queue Length The average number of read requests that were queued for the selected disk during the sample interval. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Average Disk Write Queue Length The average number of write requests that were queued for the selected disk during the sample interval. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Bytes/sec The rate at which the system has transferred bytes to and from a logical disk during write or read operations. This attribute is the 64-bit version of Disk Bytes/ sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum, the value -9223372036854775808 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Bytes/sec (Superseded) The rate at which the system has transferred bytes to and from a logical disk during write or read operations. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes/second) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Queue Length (Requests) The number of requests outstanding on a logical disk. This number includes requests in service when the data is collected. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Read Bytes/sec The rate at which the system has transferred bytes from a logical disk during read operations. This attribute is the 64-bit version of Disk Read Bytes/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum, the value -9223372036854775808 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Read Bytes/sec (Superseded) The rate at which the system has transferred bytes from a logical disk during read operations. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes/second) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Reads/sec The rate of read operations from a logical disk. Valid values are positive integers in the range 0 to 2147483647 (expressing reads/second) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Transfers/sec The rate of read and write operations on a logical disk. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Write Bytes/sec The rate at which the system has transferred bytes to a logical disk during write operations. This attribute is the 64-bit version of Disk Write Bytes/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum, the value -9223372036854775808 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Write Bytes/sec (Superseded) The rate at which the system has transferred bytes to a logical disk during write operations. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes/second) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Disk Writes/sec The rate of write operations to a logical disk. Valid values are positive integers in the range 0 to 2147483647 (expressing writes/second) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Free Megabytes The number of MBs of unallocated space on a logical drive. Note: 1 MB = 1,048,576 bytes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Logical Disk Name The name of a logical disk. Valid format is a text string of up to 64 characters.

Logical Disk Name (Long) The long name of the logical disk. Valid format is a text string of up to 268 characters.

Physical Disk Number The number of the physical disk that contains this logical disk. This value is only provided for drives assigned as drive letters. If the logical disk is a mounted volume, this value will be "Mounted". Note: Mnt = Mounted.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Size The size of the logical disk, in MBs. 1 MB = 1,048,576 bytes. Note: -1 indicates Unavailable.

Mount Point attributes

The Mount Point attribute group provides a list of mounted volumes.

Drive Name The drive name.

Mounted Volume Name The volume name.

Mount Point The mount point where the volume is mounted.

Mount Point State The mount point state.

System Name The network name of the source of this information.

Timestamp The data timestamp.

Memory attributes

Use Memory attributes to create situations that monitor counter information for real and virtual memory. Real memory is allocated in units of pages. Virtual memory may exceed real memory size, causing page traffic as virtual pages are moved between disk and real memory. Memory is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Committed Bytes In Use The ratio of Committed Bytes to the Commit Limit. Committed memory is the physical memory in use for which space has been reserved in the paging file should it need to be written to disk. The commit limit is determined by the size of the paging file. If the paging file is enlarged, commit limit is enlarged, the commit limit increases, and the ratio is reduced. This counter displays the current percentage value only; it is not an average.

Available Bytes The size of the virtual memory currently on the Zeroed, Free and Standby lists. Zeroed and Free memory is ready for use, with Zeroed memory cleared to zeros. Standby memory is memory removed from a process Working Set but still available. Notice that this is an instantaneous count, not an average over

the time interval. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Available kBytes The amount of available real memory, in KBs. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Available Usage Percentage The percent of bytes of real memory available. Calculated as 100 * (Available Bytes divided by Total Memory Bytes). Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cache Bytes The number of bytes currently in use by the system cache. The system cache is used to buffer data retrieved from disk or LAN. The system cache uses memory not in use by active processes in the computer. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Cache Bytes Peak The maximum number of bytes used by the system cache. The system cache is used to buffer data retrieved from disk or LAN. The system cache uses memory not in use by active processes in the computer. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Cache Faults/sec The average number of cache faults that have occurred on a system per second. Cache faults occur whenever the cache manager does not find a file's page in the immediate cache and must ask the memory manager to locate the page elsewhere in memory or on the disk so that it can be loaded in to the immediate cache. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Cache kBytes The amount of cache memory, in KBs, the system is currently using. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Cache kBytes Peak The maximum number of KBs the system cache has used since startup. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Cache Usage Percentage The percent of bytes of real memory allocated to the system cache. Calculated as 100 * (Cache Bytes divided by Total Memory Bytes). Note: -1 indicates Unknown.

Commit Avail kBytes The number of KBs until the commit limit is reached. Calculated as Commit Limit kB - Committed kBytes. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Commit Limit (Bytes) The number of bytes of virtual memory that can be committed on a system without extending the paging files. Commit limit is the size (in bytes) of virtual memory that can be committed without having to extend the paging files. If the paging files can be extended, this is a soft limit. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Commit Limit (Kilobytes) The number of KBs of virtual memory that can be committed on a system without extending the paging files. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Committed Bytes The number of bytes of virtual memory that have been committed on a system. Committed memory must have disk storage available, or must be assured never to need disk storage (because main memory is large enough to hold it). Notice that this is an instantaneous count, not an average over the time interval. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Committed kBytes The number of KBs of virtual memory that have been committed on a system. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Demand Zero Faults/sec The rate at which a zeroed page is required to satisfy the fault. Zeroed pages are pages emptied of previously stored data and filled with zeros. These are a security feature of Windows that prevent processes from seeing data stored by earlier processes that used the memory space. Windows maintains a list of zeroed pages to accelerate this process. This counter shows the number of faults, without regard to the number of pages retrieved to satisfy the fault. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Free System Page Table Entries The number of page table entries a system is not currently using. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Memory Usage Percentage The percent of bytes of real memory in use. Calculated as 100 * (Committed Bytes divided by Total Memory Bytes). Note that this value can exceed 100 since Committed Bytes is a measure of virtual memory while Total Memory Bytes is a measure of real memory. A value greater than 100 indicates that the computer is paging. Note: -1 indicates Unknown.

Page Faults/sec The number of page faults in the processor. Note that page faults occur when a process refers to a page that is not in its Working Set in main memory. A Page Fault will not cause the page to be fetched from disk if that page is on the standby list, and hence already in main memory, or if it is in use by another process with whom the page is shared. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page Reads/sec The number of times the disk was read to retrieve pages of virtual memory necessary to resolve page faults. Multiple pages can be read during a disk read operation. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page Writes/sec The count of the number of times pages have been written to the disk because they were changed since last retrieved. Each such write operation

may transfer a number of pages. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pages/sec The number of pages read from the disk or written to the disk to resolve memory references to pages that were not in memory at the time of the reference. This is the sum of Pages Input/Sec and Pages Output/Sec attributes. This counter includes paging traffic on behalf of the system cache to access file data for applications. This is the primary counter to observe if you are concerned about excessive memory pressure (that is, thrashing), and the excessive paging that may result. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pages Input/sec The number of pages read from the disk to resolve memory references to pages that were not in memory at the time of the reference. This counter includes paging traffic on behalf of the system cache to access file data for applications. This is an important counter to observe if you are concerned about excessive memory pressure (that is, thrashing), and the excessive paging that may result. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pages Output/sec The count of the number of pages that are written to disk because the pages have been modified in main memory. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged Allocs The number of calls to allocate space in the system nonpaged pool. Nonpaged pool is a system memory area where space is acquired by operating system components as they accomplish their appointed tasks. nonpaged pool pages cannot be paged out to the paging file, but instead remain in main memory as long as they are allocated. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged Bytes The number of bytes in the nonpaged pool, a system memory area where space is acquired by operating system components as they accomplish their appointed tasks. Nonpaged pool pages cannot be paged out to the paging file, but instead remain in main memory as long as they are allocated. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Pool Nonpaged kBytes The number of KBs in the nonpaged pool area of memory. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Pool Paged Allocs The number of calls to allocate space in the system paged pool. Paged pool is a system memory area where space is acquired by operating system components as they accomplish their appointed tasks. Paged pool pages can be paged out to the paging file when not accessed by the system for sustained periods of time. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Bytes The number of bytes in the paged pool area, a system memory area where space is acquired by operating system components as they accomplish their appointed tasks. Paged pool pages can be paged out to the paging file when

not accessed by the system for sustained periods of time. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Pool Paged kBytes The number of KBs in the paged pool area of memory. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Pool Paged Resident Bytes The current size of the paged pool. The paged pool is an area of physical memory acquired by the operating system for objects that can be paged out to the paging file when not accessed by the system for sustained periods of time. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

System Cache Resident Bytes The number of bytes from the system cache that are resident in physical memory. This does not include virtual memory not currently resident. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

System Code Total Bytes The number of bytes of pageable operating system code that is currently in virtual memory. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

System Driver Resident Bytes The number of bytes of pageable physical memory being used by device drivers. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

System Driver Total Bytes The number of bytes of pageable virtual memory that is currently being used by device drivers. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Memory Size (Bytes) The number of bytes of installed random access memory (RAM) in the computer. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Total Memory Size (KB) The number of kilobytes of installed random access memory (RAM) in the computer. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Total Memory Size (MB) The number of megabytes of installed random access memory (RAM) in the computer. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Transition Faults/sec The number of page faults resolved by recovering pages that were in transition, that is, being written to disk at the time of the page fault. The pages were recovered without additional disk activity. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Working Set Total Bytes The number of bytes of real memory allocated to currently running processes. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Working Set Total kBytes The number of KBs of real memory allocated to currently running processes. Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Working Set Total Usage Percentage The percent of bytes of real memory allocated to currently running processes. Calculated as 100 * (Total Working Set Bytes divided by Total Memory Bytes). Note: -1 indicates Unknown.

Write Copies/sec The number of page faults that have been satisfied by making a copy of a page when an attempt to write to the page is made. This is an economical way of sharing data since the copy of the page is only made on an attempt to write to the page; otherwise, the page is shared. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Memory attributes (32-bit - Superseded)

Use Memory attributes to create situations that monitor counter information for real and virtual memory. Memory is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group. This attribute group is superseded. There is a new attribute group with the same name that replaces it.

% Committed Bytes In Use The ratio of Committed Bytes to the Commit Limit. Committed memory is the physical memory in use for which space has been reserved in the paging file should it need to be written to disk. The commit limit is determined by the size of the paging file. If the paging file is enlarged, commit limit is enlarged, the commit limit increases, and the ratio is reduced. This counter displays the current percentage value only; it is not an average. (Superseded.)

Available Bytes The amount of available real memory, in bytes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Available kBytes The amount of available real memory, in KBs. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Available Usage Percentage The percent of bytes of real memory available. Calculated as 100 * (Available Bytes ÷ Total Memory Bytes). (Superseded.) Note: -1 indicates Unknown.

Cache Bytes The amount of cache memory, in bytes, the system is currently using. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cache Bytes Peak The maximum number of bytes the system cache has used since startup. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Cache Faults/sec The average number of cache faults that have occurred on a system per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Cache kBytes The amount of cache memory, in KBs, the system is currently using. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Cache kBytes Peak The maximum number of KBs the system cache has used since startup. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Cache Usage Percentage The percent of bytes of real memory allocated to the system cache. Calculated as 100 * (Cache Bytes ÷ Total Memory Bytes). (Superseded.) Note: -1 indicates Unknown.

Commit Avail kBytes The number of KBs until the commit limit is reached. Calculated as Commit Limit kB - Committed kBytes. Valid values are positive integers in the range 0 to 2147483647, and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Commit Limit (Bytes) The number of bytes of virtual memory that can be committed on a system without extending the paging files. Valid values are positive integers in the range 0 to 2147483647 that vary depending on your system and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Commit Limit (Kilobytes) The number of KBs of virtual memory that can be committed on a system without extending the paging files. Valid values are positive integers in the range 0 to 2147483647 that vary depending on your system and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Committed Bytes The number of bytes of virtual memory that have been committed on a system. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Committed kBytes The number of KBs of virtual memory that have been committed on a system. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Demand Zero Faults/sec The average number of demand zero page faults that have occurred on a system per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Free System Page Table Entries The number of page table entries a system is not currently using. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Memory Usage Percentage The percent of bytes of real memory in use. Calculated as 100 * (Committed Bytes ÷ Total Memory Bytes). Note that this value can exceed 100 since Committed Bytes is a measure of virtual memory while Total Memory Bytes is a measure of real memory. A value greater than 100 indicates that the computer is paging. (Superseded.) Note: -1 indicates Unknown.

Page Faults/sec The number of page faults in the processor. Note that page faults occur when a process refers to a page that is not in its Working Set in main memory. Valid values are positive integers in the range that varies depending on your system and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page Reads/sec The rate at which the memory manager reads from the disk. Valid values are positive integers in the range 0 to 2147483647 and can include the use of

the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page Writes/sec The rate at which the memory manager writes changed pages to a disk. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pages/sec The average number of pages per second the memory manager reads from or writes to a disk. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pages Input/sec The rate at which the memory manager reads pages from the disk to update memory references to pages that were not previously referenced. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pages Output/sec The number of modified pages that are written to the disk. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged Allocs The number of system requests for space allocation in the nonpaged pool area of memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged Bytes The number of bytes in the nonpaged pool area of memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged kBytes The number of KBs in the nonpaged pool area of memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Allocs The number of system requests for space allocation in the paged pool area of memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Bytes The number of bytes in the paged pool area of memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown.

(Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged kBytes The number of KBs in the paged pool area of memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Resident Bytes The current size of the paged pool. The paged pool is an area of physical memory acquired by the operating system for objects that can be paged out to the paging file when not accessed by the system for sustained periods of time. Valid values are positive integers in the range 0 to 2147483647, and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system. (Superseded.)

System Cache Resident Bytes The number of bytes from the system cache that are resident in physical memory. This does not include virtual memory not currently resident. Valid values are positive integers in the range 0 to 2147483647, and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Code Total Bytes The number of bytes of pageable operating system code that is currently in virtual memory. Valid values are positive integers in the range 0 to 2147483647, and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Driver Resident Bytes The number of bytes of pageable physical memory being used by device drivers. Valid values are positive integers in the range 0 to 2147483647, and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Driver Total Bytes The number of bytes of pageable virtual memory that is currently being used by device drivers. Valid values are positive integers in the range 0 to 2147483647, and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data (Superseded). This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Memory Size (Bytes) The number of bytes of installed random access memory (RAM) in the computer. (Superseded.) Note: -1 indicates Unavailable.

Total Memory Size (KB) The number of kilobytes of installed random access memory (RAM) in the computer. (Superseded.) Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Total Memory Size (MB) The number of megabytes of installed random access memory (RAM) in the computer. (Superseded.) Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Transition Faults/sec The number of transition faults the system has resolved per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Working Set Total Bytes The number of bytes of real memory allocated to currently running processes. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Working Set Total kBytes The number of KBs of real memory allocated to currently running processes. (Superseded.) Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Working Set Total Usage Percentage The percent of bytes of real memory allocated to currently running processes. Calculated as 100 * (Total Working Set Bytes ÷ Total Memory Bytes). (Superseded.) Note: -1 indicates Unknown.

Write Copies/sec The rate at which the memory manager has resolved page faults associated with write attempts by making page copies. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Monitored Logs Report attributes

Monitored Logs Report attributes represent log settings that affect future log entries, such as the maximum log size and when old entries should be deleted. Monitored Logs Report is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Usage The percentage of the log used. Valid values are positive integers in the range of 0 to 100 (expressing a percentage).

Usage: The following situation notifies you when the Security Log reaches 50% of the capacity you set as a maximum:

*VALUE *Log Name *EQ Security *AND *VALUE *Capacity *EQ 50

Current Size The current size of a specific log in bytes. This attribute reflects the size of the file on disk, and it might not match the value displayed by the event log viewer. This attribute is the 64-bit version of Current Size. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Current Size (Superseded) The current size of a specific log in bytes. This attribute reflects the size of the file on disk, and it might not match the value displayed by the event log viewer. Valid values are positive integers in the range 0 to 2147483647 (expressing an integer). Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Usage: The following situation notifies you when the size of the Application Log is greater than 512 bytes:

*VALUE *Log Name *EQ Application *AND *VALUE *Current Size *GT 512

Date Time Last Modified The date and time when the file was last modified.

Log Name Use this attribute to create a situation where you want to specify a specific log to monitor or exclude events written to a specific log. Valid format is a text without case-sensitivity with a range from 1 to 32 characters.

Log Name (Unicode) Use this attribute to create a situation where you want to specify a specific log to monitor or exclude events written to a specific log. Valid format is a text string of up to 392 bytes.

Maximum Size The maximum size of the log file in bytes. This attribute is the 64-bit version of Max Size. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Maximum Size (Superseded) The maximum size of the log file in bytes. Valid values are positive integers in the range 0 to 4194240 (expressing an integer). Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Usage: The follow situation notifies you when the Application Log reaches 512 bytes:

VALUE *Log Name *EQ *Application *AND *VALUE *Max Size *EQ 512

Path A location on a disk drive. Valid format is a text string without case-sensitivity in the range from 1 to 256 characters.

Note: Do not use to create situations.

Path (Unicode) A location on a disk drive. Valid format is a text string without case-sensitivity in the range from 1 to 392 bytes.

Note: Do not use to create situations.

Record Count The number of records in a log. This attribute is the 64-bit version of Record Count. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Record Count (Superseded) The number of records in a log. Valid values are positive integers in the range 0 to 4194240 (expressing an integer). Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Usage: The following situation notifies you when the System Log contains 55 or more records:

*VALUE *Log Name *EQ *System *AND *Record Count *GE 55

Retention Use this attribute when you want to be notified when a specific log reaches the number of days you specified in the Overwrite Event Older Than section of the Event Log Settings panel. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

To specify this number on the Event Log Settings panel, perform the procedure that follows.

1. Click Start from the menu bar.

The Start menu displays.

2. Select Programs and then Administrative Tools.

3. Open the Event Viewer.

4. Select Log, then Log Settings.

5. Click the Overwrite Events Older Than button and enter a number.

To verify this number, check the Retention field in the Monitored Logs report.

Usage: The following situation notifies you when the events logged to the Application Log reach the seven day maximum retention:

*VALUE *Log Name *EQ *Application *AND *VALUE *Retention *EQ 7

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

MSMQ Information Store attributes

Use MSMQ Information Store attributes to monitor session information relating to the MSMQ (Microsoft Message Queue) Information Store. MSMQ Information Store is a single-instance attribute group.

Access to the Server The total number of times the MSMQ Information Store was accessed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Errors Returned to Application The total number of MSMQ Information Store accesses that resulted in error replies by the Information Store. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Replication Requests Received The total number of replication requests received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Replication Requests Sent The total number of replication requests sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sync Replies The total number of sync requests that were answered. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sync Requests The total number of sync requests received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG,

*MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Write Requests Sent The total number of write requests sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

MSMQ Queue attributes

Use MSMQ Queue attributes to monitor MSMQ (Microsoft Message Queue) statistics. MSMQ Queue is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Bytes in Journal Queue The total number of bytes that currently reside in the journal queue. For the Computer Queues instance, this represents the computer journal queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes in Queue The total number of bytes that currently reside in the queue. For the Computer Queues instance, this represents the dead letter queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages in Journal Queue The total number of messages that currently reside in the journal queue. For the Computer Queues instance, this represents the dead letter queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages in Queue The total number of messages that currently reside in the queue. For the Computer Queues instance, this represents the dead letter queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Queue Instance The instance name of the queue. Valid format is a text string of up to 64 characters. For example, LMAIL.

Queue Instance (Unicode) The instance name of the queue. Valid format is a text string of up to 256 characters. INACTIVE=Queue_is_Inactive is a valid value. Queue_is_Inactive is displayed for this attribute if there are no messages in the queue.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

MSMQ Service attributes

Use MSMQ (Microsoft Message Queue) Service attributes to monitor session data and the flow of messages through the system. MSMQ Service is a single-instance attribute group.

IP Sessions The total number of open IP sessions. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN,

*MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IPX Sessions The total number of open IPX sessions. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Incoming Messages/sec The rate of incoming MSMQ messages handled by the MSMQ Service per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

MSMQ Incoming Messages The total number of incoming messages handled by the MSMQ service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

MSMQ Outgoing Messages The total number of outgoing messages handled by the MSMQ service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Outgoing Messages/sec The rate of outgoing MSMQ messages handled by the MSMQ Service per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sessions The total number of open network sessions. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month

DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Bytes in all Queues The total number of bytes in all active queues under the MSMQ Service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Messages in all Queues The total number of messages in all active queues under the MSMQ Service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

MSMQ Sessions attributes

Use MSMQ Sessions attributes to monitor session statistics. MSMQ (Microsoft Message Queue) Sessions is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Incoming Bytes The total number of bytes that were received through the selected session. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Incoming Bytes/sec The rate that MSMQ messages are entering through the selected session. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Incoming Messages The total number of messages that were received through the selected session. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Incoming Messages/sec The rate that MSMQ messages are entering per second through the selected session. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Outgoing Bytes The total number of bytes that were sent through the selected session. Valid values are positive integers in the range 0 to 2147483647 and can

include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Outgoing Bytes/sec The rate that MSMQ messages are leaving per second through the selected session. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Outgoing Messages The total number of messages that were sent through the selected session. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Outgoing Messages/sec The rate that MSMQ messages are leaving per second through the selected session. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Session The IP address of the computer in session with MSMQ. Valid format is a text string of up to 64 characters. For example, MBROWN2

System Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Network Interface attributes

Use Network Interface attributes to monitor the rates at which bytes and packets are sent and received over the named network interface. Network Interface is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Bandwidth Utilization Percentage Measure of network interface bandwidth utilization. Calculated as 100 * ((8 * Bytes Total/sec) ÷ Current Bandwidth). Note: -1 indicates Unknown and 9223372036854775807 indicates Value_Exceeds_Maximum.

Bytes Received/sec The rate that bytes are received on the interface, including framing characters. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate that bytes are sent on the interface, including framing characters. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Total/sec The rate that bytes are sent and received on the interface, including framing characters. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Current Bandwidth An estimate of the current bandwidth for the interface in bits per second (bps). For interfaces that do not vary in bandwidth, or for those where no accurate estimation can be made, this value is the nominal bandwidth. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

IPv4 Address The IPv4 interface address. Note that the value No_DNS_Entry is a valid value.

IPv6 Global Address The IPv6 Global interface address. Note that the value No_DNS_Entry is a valid value.

IPv6 Link Local Address The IPv6 Link Local interface address. Note that the value No_DNS_Entry is a valid value.

Network Interface Instance (Unicode) The instance name of the Network Interface object (Connection Name) in unicode. The valid format is a text string of up to 128 characters.

Network Interface Instance The instance name of the Network Interface object (Connection Name). The valid format is a text string of up to 128 characters.

Output Queue Length The length of the output packet queue (in packets). If this is longer than 2, delays are being experienced and the bottleneck must be found and eliminated, if possible. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum, and -9223372036854775808 indicates Value_Exceeds_Minimum.

Output Queue Length kPackets The length of the output packet queue in packets (in thousands). If this is longer than 2, delays are being experienced and the bottleneck must be found and eliminated, if possible. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Outbound Discarded The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Outbound Errors The number of outbound packets that could not be transmitted because of errors. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Received Discarded The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol.

One possible reason for discarding such a packet could be to free up buffer space. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Received Errors The number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Received Non-Unicast/sec The rate that non-unicast, that is, subnet broadcast or subnet multicast packets, are delivered to a higher-layer protocol. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Received/sec The rate that packets are received on the network interface. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Received Unicast/sec The rate that (subnet) unicast packets are delivered to a higher-layer protocol. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Received Unknown The number of packets received via the interface that were discarded because of an unknown or unsupported protocol. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets/sec The rate that packets are sent and received per second on the network interface. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Sent/sec The rate that packets are sent on the network interface. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Sent Non-Unicast/sec The rate that packets are requested to be transmitted to non-unicast, that is, subnet broadcast or subnet multicast, addresses by higher-layer protocols. The rate includes the packets that were discarded or not sent. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Sent Unicast/sec The rate that packets are requested to be transmitted to subnet-unicast addresses by higher-layer protocols. The rate includes the packets that were discarded or not sent. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Network Interface attributes (32-bit - Superseded)

Use Network Interface attributes to monitor the rates at which bytes and packets are sent and received over the named network interface. Network Interface is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group. This attribute group is superseded. There is a new attribute group with the same name that replaces it.

Bandwidth Utilization Percentage Measure of network interface bandwidth utilization. Calculated as 100 * ((8 * Bytes Total/sec) ÷ Current Bandwidth). (Superseded.)

Bytes Received/sec The rate that bytes are received on the interface, including framing characters. Valid values are positive integers in the range 0 to 2147483647

and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate that bytes are sent on the interface, including framing characters. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Total/sec The rate that bytes are sent and received on the interface, including framing characters. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Bandwidth An estimate of the current bandwidth for the interface in bits per second (bps). For interfaces that do not vary in bandwidth, or for those where no accurate estimation can be made, this value is the nominal bandwidth. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IPv4 Address The IPv4 interface address. Note that the value No_DNS_Entry is a valid value. (Superseded.)

IPv6 Global Address The IPv6 Global interface address. Note that the value No_DNS_Entry is a valid value. (Superseded.)

IPv6 Link Local Address The IPv6 Link Local interface address. Note that the value No_DNS_Entry is a valid value. (Superseded.)

Network Interface Instance The instance name of the Network Interface object (Connection Name). Valid format is a text string of up to 64 characters. For example, "Broadcom TetXtreme Gigabit Ethernet - Pocket Scheduler Miniport". (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Network Interface Instance (Unicode) The instance name of the Network Interface object (Connection Name) in UTF-8. Valid format is a text string of up to 128 characters. (Superseded.)

Output Queue Length The length of the output packet queue (in packets). If this is longer than 2, delays are being experienced and the bottleneck must be found and eliminated, if possible. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum, and -2147483648 indicates Value_Exceeds_Minimum.

Output Queue Length kPackets The length of the output packet queue in packets (in thousands). If this is longer than 2, delays are being experienced and the bottleneck must be found and eliminated, if possible. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN,

*MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Outbound Discarded The number of outbound packets that were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Outbound Errors The number of outbound packets that could not be transmitted because of errors. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Received Discarded The number of inbound packets that were chosen to be discarded even though no errors had been detected to prevent their being delivered to a higher-layer protocol.

One possible reason for discarding such a packet could be to free up buffer space. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Received Errors The number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Received Non-Unicast/sec The rate that non-unicast, that is, subnet broadcast or subnet multicast packets, are delivered to a higher-layer protocol. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Received/sec The rate that packets are received on the network interface. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Received Unicast/sec The rate that (subnet) unicast packets are delivered to a higher-layer protocol. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Received Unknown The number of packets received via the interface that were discarded because of an unknown or unsupported protocol. Valid values are

positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets/sec The rate that packets are sent and received per second on the network interface. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Sent/sec The rate that packets are sent on the network interface. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Sent Non-Unicast/sec The rate that packets are requested to be transmitted to non-unicast, that is, subnet broadcast or subnet multicast, addresses by higher-layer protocols. The rate includes the packets that were discarded or not sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Sent Unicast/sec The rate that packets are requested to be transmitted to subnet-unicast addresses by higher-layer protocols. The rate includes the packets that were discarded or not sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname*:*agent_code*. (Superseded.)

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. (Superseded). This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Network Port attributes

Use Network Port attributes to monitor connection information about network ports.

Local Host IP Address The IP address of the local host.

Local Host Name The host name of the local host. This name can either be the simple host name or the fully qualified host name.

Local Port The local port number.

Local Port Name The local port name.

Protocol The port protocol.

Remote Host IP Address The IP address of the remote host when the protocol is TCP. This value is blank if the protocol is UDP.

Remote Host Name The host name of the remote host when the protocol is TCP. This value is blank if the protocol is UDP. This name can either be the simple host name or the fully qualified host name.

Remote Port The remote port number. Note: 0 indicates Unavailable. On the Tivoli Enterprise Portal, for sessions that are established with a protocol of UDP and for sessions that are in a Listening state, a value of Unavailable is indicated for the remote port attribute.

State The port state. The valid values include Closed, Listening, SYN_Sent, SYN_Received, Established, Waiting_for_FIN__WAIT1, Waiting_for_FIN__WAIT2, Waiting_for_Close, Closing, Last_ACK, Time_Wait, TCB_deleted, Unknown_status, and Unavailable. For sessions that are established with a protocol of UDP, the remote port and state attributes will have a value of Unavailable.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute

SS Second
mmm Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Network Segment attributes

Use Network Segment attributes to monitor utilization and traffic statistics for data in a network segment. Data for this report is from the Microsoft Network Monitor. Network Segment is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group. Network Segment attributes are only supported for Windows NT and earlier. They exist in this release for backward compatibility only.

% Broadcast Frames The percentage of network bandwidth that is made up of broadcast traffic on this network segment. Valid values are positive integers in the range 0 to 100 (expressing a percentage).

% Multicast Frames The percentage of network bandwidth that is made up of multicast traffic on this network segment. Valid values are positive integers in the range 0 to 100 (expressing a percentage).

% Network Utilization The percentage of network bandwidth in use of this network segment. Valid values are positive integers in the range 0 to 100 (expressing a percentage).

Broadcast Frames Received/sec The number of broadcast frames received per second on this network segment. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Multicast Frames Received/sec The number of multicast frames received per second on this network segment. Valid format is a text string of up to 64 characters. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Network Segment Instance The instance name of the Network Interface object (Connection Name). Valid format is a text string of up to 64 characters.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C Century (0 for 20th, 1 for 21st)

YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Bytes Received/sec The number of bytes received per second on this network segment. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Total Frames Received/sec The total number of frames received per second on this network segment. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

NNTP Commands attributes

Use NNTP (Network News Transport Protocol) Commands attributes to create situations that monitor a variety of commands associated with the hosting of news group discussions. NNTP Commands is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Article Commands The number of ARTICLE commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Article Commands/sec The number of ARTICLE commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Check Commands The number of CHECK commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Check Commands/sec The number of CHECK commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Group Commands The number of GROUP commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to

2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Group Commands/sec The number of GROUP commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Help Commands The number of HELP commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Help Commands/sec The number of HELP commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IHave Commands The number of IHAVE commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

IHave Commands/sec The number of IHAVE commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Last Commands The number of LAST commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Last Commands/sec The number of LAST commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

List Commands The number of LIST commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

List Commands/sec The number of LIST commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Logon Attempts The number of logon attempts that have been made to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Logon Attempts/sec The number of logon attempts per second that have been made to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Logon Failures The number of logons that had failed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Logon Failures/sec The number of logons per second that had failed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Mode Commands The number of MODE commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Mode Commands/sec The number of MODE commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Newgroups Commands The number of NEWGROUPS commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Newgroups Commands/sec The number of NEWGROUPS commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Newnews Commands The number of NEWNEWS commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Newnews Commands/sec The number of NEWNEWS commands per second received by the NNTP Server since it was started. Valid values are positive integers

in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Next Commands The number of NEXT commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Next Commands/sec The number of NEXT commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

NNTP Server Instance number of NNTP virtual server. Valid format is a text string of up to 64 characters.

Post Commands The number of POST commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Post Commands/sec The number of POST commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Quit Commands The number of QUIT commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Quit Commands/sec The number of QUIT commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Search Commands The number of SEARCH commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Search Commands/sec The number of SEARCH commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Stat Commands The number of STAT commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Stat Commands/sec The number of STAT commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Takethis Commands The number of TAKETHIS commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Takethis Commands/sec The number of TAKETHIS commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

XHdr Commands The number of XHDR commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

XHdr Commands/sec The number of XHDR commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

XOver Commands The number of XOVER commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

XOver Commands/Sec The number of XOVER commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

XPat Commands The number of XPAT commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

XPat Commands/sec The number of XPAT commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

XReplic Commands The number of XREPLIC commands received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

XReplic Commands/sec The number of XREPLIC commands per second received by the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

NNTP Server attributes

Use NNTP (Network News Transport Protocol) Server attributes to create situations that monitor a wide range of server activities associated with the hosting of news group discussions. NNTP Server is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Article Map Entries The entries inserted in to the article mapping table of the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Article Map Entries/sec The entries inserted per second in to the article mapping table of the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Deleted The number of articles deleted on the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Deleted/sec The number of articles deleted per second on the NNTP Server since it was started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Posted The number of articles posted to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Posted/sec The number of articles posted per second to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Received The total number of files received by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Received/sec The total number of files per second received by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Sent The total number of files sent by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Sent/sec The total number of files sent per second by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Articles Total The sum of Articles Sent and Articles Received. This is the total number of files transferred by the NNTP Server. Valid values are positive integers

in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The rate that data bytes are received by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate that data bytes are sent by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Total/sec The sum of Bytes Sent/sec and Bytes Received/sec. This is the total rate of bytes transferred by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Control Messages Failed The total number of control messages failed or not applied by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Control Messages Received The total number of control messages received by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Anonymous Users The number of anonymous users currently connected to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Connections The current number of connections to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current NonAnonymous Users The number of nonanonymous users currently connected to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Outbound Connections The number of current outbound connections being made by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM

functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Failed Outbound Logons The number of failed outbound logons made by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

History Map Entries The entries inserted in to the history mapping table of the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

History Map Entries/sec The entries inserted per second in to the history mapping table of the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum Anonymous Users The maximum number of anonymous users simultaneously connected to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Maximum Connections The maximum number of simultaneous connections to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Maximum NonAnonymous Users The maximum number of nonanonymous users simultaneously connected to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Moderated Postings Failed The total number of moderated postings the NNTP Server fails to send to an SMTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Moderated Postings Sent The total number of moderated postings the NNTP Server attempts to send to an SMTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

NNTP Server Instance number of NNTP virtual server. Valid format is a text string of up to 64 characters.

Sessions Flow Controlled The number of client sessions currently in a flow controlled state in the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM

functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Anonymous Users The total number of anonymous users that have ever connected to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Connections The number of connections that have been made to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total NonAnonymous Users The total number of nonanonymous users that have ever connected to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Outbound Connections The number of outbound connections that have been made by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Outbound Connections Failed The number of unsuccessful outbound connections that have been made by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN,

*MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Passive Feeds The number of passive feeds accepted by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Pull Feeds The number of pull feeds made by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Push Feeds The number of push feeds made by the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total SSL Connections The number of SSL connections that have been made to the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Xover Entries The number of xover entries in the xover table of the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Xover Entries/sec The number of xover entries inserted per second in the xover table of the NNTP Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Objects attributes

Use Objects attributes to create situations that monitor the number of events, mutexes, processes, sections, semaphores, and threads. Objects is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Events The number of events on a system at the time of monitoring. Note that an event is any system or user action that causes notification or a log entry. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Mutexes The number of mutexes on a system at the time of monitoring. This is an instantaneous count, not an average. The system uses mutexes to assure that only

one section of code is executing per thread. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Processes The number of active processes on a system at the time of monitoring. This is an instantaneous count, not an average. A process is a running program. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sections The number of sections on a system at the time of monitoring. A process creates sections in memory to store data. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Semaphores The number of semaphores on a system at the time of monitoring. Semaphores allow threads access to data structures that they share with other threads. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Threads The number of threads on a system at the time of monitoring. Valid values are positive integers in the range 0 to 9999 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Paging File attributes

Use Paging File attributes to create situations that monitor information about the page files of the system. Paging File is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Usage The amount of a paging file in use. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Usage Peak The peak amount of the Page File instance used in percent. Valid values are positive integers.

Pagefile Name The name of a page file. Valid format is a text string of up to 64 characters. For example, PAGING.

Pagefile Name (Unicode) The instance name in UTF8. Valid format is a text string of up to 392 bytes.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Physical Disk attributes

Use Physical Disk attributes to create situations that monitor information about fixed and hard disk drives. Physical disk is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Disk Idle Time The percentage of elapsed time that the selected disk drive is not servicing any read or write requests. Valid values are positive integers in the range 0 to 100 (expressing a percentage).

% Disk Read Time The percentage of elapsed time a disk drive been busy servicing read requests. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Disk Time The percentage of elapsed time a disk drive has been busy servicing read or write requests. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Disk Write Time The percentage of elapsed time that a disk drive has been busy servicing write requests. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Avg Disk Bytes/Read The average number of bytes transferred from a disk during read operations. This attribute is the 64-bit version of Avg Disk Bytes/Read. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Avg Disk Bytes/Read (Superseded) The average number of bytes transferred from a disk per read operation. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes per read) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Avg Disk Bytes/Transfer Average number of bytes transferred to or from the disk during write or read operations. This attribute is the 64-bit version of Avg Disk Bytes/Transfer. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Avg Disk Bytes/Transfer (Superseded) Average number of bytes transferred to or from the disk during write or read operations. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Avg Disk Bytes/Write Average number of bytes transferred to the disk during write operations. This attribute is the 64-bit version of Avg Disk Bytes/Write. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Avg Disk Bytes/Write (Superseded) Average number of bytes transferred to the disk during write operations. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Avg Disk ms/Read Average time in milliseconds of a read of data from the disk. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Avg Disk ms/Transfer Time in milliseconds of the average disk transfer. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Avg Disk ms/Write Average time in milliseconds of a write of data to the disk. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Average Disk Queue Length The average number of both read and write requests that were queued for the selected disk during the sample interval. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Average Disk Read Queue Length The average number of read requests that were queued for the selected disk during the sample interval. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Average Disk Write Queue Length The average number of write requests that were queued for the selected disk during the sample interval. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Disk Bytes/sec The rate at which bytes are transferred to or from a disk during write or read operations. This attribute is the 64-bit version of Disk Bytes/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Disk Bytes/sec (Superseded) The rate at which bytes are transferred to or from a disk during write or read operations. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes/second) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Disk Number The number of a physical disk. Calculated as the left part of the Disk Name.

Disk Queue Length The number of requests outstanding on a disk the instant the data is collected, including requests currently in service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Disk Read Bytes/sec The rate bytes are transferred from the disk during read operations. This attribute is the 64-bit version of Disk Read Bytes/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Disk Read Bytes/sec (Superseded) The rate bytes are transferred from the disk during read operations. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes/second) and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Disk Reads/sec The average number of read operations that have occurred on a disk per second. Valid values are positive integers in the range 0 to 2147483647 and

can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Disk Transfers/sec The average number of read and write operations that have occurred on a disk per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Disk Write Bytes/sec The rate bytes are transferred to the disk during write operations. This attribute is the 64-bit version of Disk Write Bytes/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Disk Write Bytes/sec (Superseded) The rate bytes are transferred to the disk during write operations. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes/second) and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Disk Writes/sec The average number of write operations that have occurred on a disk per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Physical Disk Name The name of a physical disk. Valid format is a text string of up to 64 characters.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Print Job attributes

Use the Print Job attributes to create situations that monitor information about each print job owned by a specific printer that is attached to your server. Print Job is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Data Type The data type used to record print jobs. Valid format is a text string of up to 32 characters. For example, tEXT is an example of a data type.

Document Name The name of the document in print. Valid format is a text string of up to 64 characters. For example, KNTDOC is an example of a document name.

Document Name (Unicode) The name of the document in print in UTF8. Valid format is a text string of up to 392 bytes.

Driver Name The print driver that is being used. Valid format is a text string of up to 64 characters. For example, to HP Laserjet III is an example of a print driver name.

Machine Name The machine that created the job. Valid format is a text string of up to 32 characters. For example, AGHQ01 is an example of a machine name.

Notify Name The user to notify about the job. Valid format is a text string of up to 32 characters. For example, MBROWN is an example of a user name.

Notify Name (Unicode) The user to notify about the job in UTF8.

Pages Printed The number of pages that have printed. This attribute is the 64-bit version of Pages Printed. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Pages Printed (Superseded) The number of pages that have printed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Parameters The parameters of the print processor. Valid format is a text string of up to 64 characters. For example, MARGIN is an example of a parameter setting.

Position The position of the job in the print queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Print Processor The print processor that must be used. Valid format is a text string of up to 64 characters. For example, WINPRINT is an example of a print processor.

Printer Name The name of the printer. Valid format is a text string of up to 64 characters. For example, to LPT1 specifies the name of the printer.

Printer Name (Unicode) The name of the printer in UTF8. Valid format is a text string of up to 336 bytes.

Priority The priority of the job. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Size The size of the print job. This attribute is the 64-bit version of Size. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Size (Superseded) The size of the print job. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Status The status of the job. Valid format is a text string of up to 20 characters. For example, to PRINTING indicates the status of the job.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Time Elapsed The time elapsed, in seconds, that has elapsed since the job began printing. This attribute is the 64-bit version of Time Elapsed. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Time Elapsed (Superseded) The time elapsed, in seconds, that has elapsed since the job began printing. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Time Submitted The time when the job was submitted. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Pages The number of pages of the job. This attribute is the 64-bit version of Total Pages. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Total Pages (Superseded) The number of pages of the job. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

User Name The user who owns the job. Valid format is a text string of up to 32 characters. For example, SMITH is an example of a user name.

User Name (Unicode) The user who owns the job in UTF8. Valid format is a text string of up to 40 bytes.

Print Queue attributes

Use the Print Queue attributes to create situations that monitor the performance and operation of printers locally attached to a computer. Print Queue is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group. Attribute values in this table are obtained from PerfMon. All attribute values are provided for printers locally attached to the computer. Network printers, file printers, and printers attached to remote print servers do not have all their values shown in the local computer's PerfMon database. For these printers, some metrics, such as Job Errors, Out of Paper Errors, Not Ready Errors, are reported as zero.

Add Network Printer Calls Total number of calls from other print servers to add shared network printers to this server since last restart. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Average Job Errors/Day Average number of job errors per day, where a day is a complete 24 hour period, since the system was last started. Calculated as Job Errors ÷ System Up Time Days. If the system has been running less than 1 day, this value is the same as Job Errors. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Average Not Ready Errors/Day Average number of not ready errors per day, where a day is a complete 24 hour period, since the system was last started. Calculated as Not Ready Errors ÷ System Up Time Days. If the system has been running less than 1 day, this value is the same as Not Ready Errors. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Average Out Of Paper Errors/Day Average number of out of paper errors per day, where a day is a complete 24 hour period, since the system was last started. Calculated as Out Of Paper Errors ÷ System Up Time Days. If the system has been running less than 1 day, this value is the same as Out Of Paper Errors. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Printed/sec Number of bytes per second printed on a print queue. This attribute is the 64-bit version of Bytes Printed/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Printed/sec (Superseded) Number of bytes per second printed on a print queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Enumerate Network Printer Calls Total number of calls from browse clients to this print server to request network browse lists since last restart. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Job Errors Total number of job errors in a print queue since last restart. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Jobs Current number of jobs in a print queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Jobs Spooling Current number of spooling jobs in a print queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Max Jobs Spooling Maximum number of spooling jobs in a print queue since last restart. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Max References Peak number of references (open handles) to this printer. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Name Name of the print queue object for monitoring print server activity. Valid format is a text string of up to 64 characters.

Name (Unicode) Name of the print queue object for monitoring print server activity. Valid format is a text string of up to 336 bytes.

Not Ready Errors Total number of printer not ready errors in a print queue since the last restart. Valid values are positive integers in the range 0 to 2147483647 and

can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Out of Paper Errors Total number of out of paper errors in a print queue since the last restart. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

References Current number of references (open handles) to this printer. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Jobs Printed Total number of jobs printed on a print queue since the last restart. This attribute is the 64-bit version of Total Jobs Printed. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Total Jobs Printed (Superseded) Total number of jobs printed on a print queue since the last restart. This attribute is the 64-bit version of Total Pages Printed. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Pages Printed Total number of pages printed through GDI on a print queue since the last restart. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Total Pages Printed (Superseded) Total number of pages printed through GDI on a print queue since the last restart. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Printer attributes

Use the Printer attributes to create situations that monitor information about each printer that is attached to your server. Printer is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Average Pages Per Minute The average pages printed per minute of the printer. This attribute is the 64-bit version of Average Pages Per Minute. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Average Pages Per Minute (Superseded) The average pages printed per minute of the printer. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Comment The comment. Valid format is a text string of up to 64 characters. For example, SUBMITTED is an example of a comment.

Comment (Unicode) Comment in UTF8. Valid format is a text string of up to 388 bytes.

Data Type The data type used to record print jobs Valid format is a text string of up to 32 characters.

Default Priority The default priority value assigned to each print job. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Driver Name The print driver that is being used. Valid format is a text string of up to 64 characters. For example, to HP Laserjet III is an example of a print driver.

Location The location where the printer resides. Valid format is a text string of up to 64 characters. For example, to AGH specifies a location where the printer resides.

Location (Unicode) The location of the printer in UTF8. Valid format is a text string of up to 388 bytes.

Number of Jobs The number of jobs in the queue. This attribute is the 64-bit version of Number of Jobs. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Number of Jobs (Superseded) The number of jobs in the queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG,

*MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Parameters The parameters of the print processor. Valid format is a text string of up to 64 characters. For example, to MARGIN indicates a parameter.

Port Name The port name that the printer is connected to. Valid format is a text string of up to 64 characters. For example, to LDEV1 specifies the port name for the printer.

Print Processor The print processor that must be used. Valid format is a text string of up to 64 characters. For example, to WINPRINT indicates the print processor used.

Printer Name The name of the printer. Valid format is a text string of up to 64 characters. For example, to LPT1 is the name of the printer.

Printer Name (Unicode) The name of the printer in UTF8. Valid format is a text string of up to 336 bytes.

Priority The priority of the job. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Separator File The file that contains the job separator page. Valid format is a text string of up to 64 characters. For example, to JSEP indicates the file that contains the job separator page.

Separator File (Unicode) The file that contains the job separator page in UTF8. Valid format is a text string of up to 392 bytes.

Share Name The share name of the printer. Valid format is a text string of up to 32 characters. For example, to AGHQ01 specifies the share name of the printer.

Share Name (Unicode) The share name of the printer.

Start Time The start time of the printer operation.

Status The status of the job. Valid format is a text string of up to 20 characters. For example, to PRINTING specifies the status of the print job.

System Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C Century (0 for 20th, 1 for 21st)
YY Year

MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Until Time The end time of the printer operation.

Process attributes

Use Process attributes to monitor information about a specific process, such as the amount of time the process runs, its thread count, and how it uses real and virtual memory. Process is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Privileged Time The percentage of elapsed time that a process has executed instructions in privileged mode. Valid values are positive integers that can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Processor Time The percentage of elapsed time that a process has used the processor to execute instructions. Valid values are positive integers that can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

There is an inconsistency between the way that the Process report calculates the percentage of processor time used by a process, and the way that the Windows Performance Monitor calculates this percentage.

The Process report displays the percentage of processor time used for a single process on all processors. The total is based on 100 times P, where P is equal to the number of processors in use.

% User Time The percentage of elapsed time that a process has executed instructions in user mode. Valid values are positive integers that can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Avg % Processor Time Percentage of processor use, as an average across all processors in the system.

Binary Path The fully qualified path to the device binary executable running in the process in UTF-8.

Elapsed Time (Seconds) The total amount of time, in seconds, a process has been running. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Handle Count The total number of handles currently open through this process. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

ID Process The unique identifier of a process. Note that this number applies only while the process is running. After the process ends, the same number might be

used to represent a different process. Valid values are positive integers and can include the use of the *MIN, *MAX, or *SUM functions.

Page Faults/sec The average number of page faults that have occurred for a process per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Page File Bytes The number of bytes of page file space a process uses. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Page File Bytes Peak The maximum number of bytes of page file space a process has used since starting. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Page File kBytes The number of KBs of page file space a process uses. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Page File kBytes Peak The maximum number of KBs of page file space a process has used since starting. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Pool Nonpaged Bytes The number of bytes of pool nonpaged memory a process uses. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Bytes The number of bytes of pool paged memory a process uses. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Priority Base The current base priority of a process. Valid values are positive integers in the range 1 to 31 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Private Bytes The number of bytes of memory space a process has allocated that cannot be shared with other processes. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Private kBytes The number of KBs of memory space a process has allocated that cannot be shared with other processes. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Process Count The count of process executable instances. The process count is the duplicate occurrences of the binary path data. Valid values can include the value Undefined (0).

Process Name The process instance name. Valid format is a text string of up to 64 characters. For example, SYS1.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Thread Count The number of threads currently active in a process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

User The user ID associated with the running process.

Virtual Bytes The number of bytes of virtual address space that a process uses. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Virtual Bytes Peak The maximum number of bytes of virtual address space a process has used since starting. Note: -1 indicates Unknown, 9223372036854775807 indicates Value_Exceeds_Maximum and -9223372036854775808 indicates Value_Exceeds_Minimum.

Virtual kBytes The number of KBs of virtual address space that a process uses. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Virtual kBytes Peak The maximum number of KBs of virtual address space a process has used since starting. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Working Set The size of the current working set of a process in bytes. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Working Set kBytes The size of the current working set of a process in KBs. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Working Set kBytes Peak The maximum number of KBs of a working set. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Working Set Peak The maximum working set of a process in bytes since the process started. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Process attributes (32-bit - Superseded)

Use Process attributes to monitor information about a specific process, such as the amount of time the process runs, its thread count, and how it uses real and virtual memory. Process is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group. This attribute group is superseded. There is a new attribute group with the same name that replaces it.

% Privileged Time The percentage of elapsed time that a process has executed instructions in privileged mode. Valid values are positive integers that can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.)

% Processor Time The percentage of elapsed time that a process has used the processor to execute instructions. Valid values are positive integers that can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.)

There is an inconsistency between the way that the Process report calculates the percentage of processor time used by a process, and the way that the Windows Performance Monitor calculates this percentage.

The Process report displays the percentage of processor time used for a single process on all processors. The total is based on 100 times P, where P is equal to the number of processors in use.

% User Time The percentage of elapsed time that a process has executed instructions in user mode. Valid values are positive integers that can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.)

Avg % Processor Time Percentage of processor use, as an average across all processors in the system. (Superseded.)

Binary Path The fully qualified path to the device binary executable running in the process in UTF-8. (Superseded.)

Elapsed Time (Seconds) The total amount of time, in seconds, a process has been running. Valid values are positive integers in the range 0 to 2147483647 (expressing seconds) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Handle Count The total number of handles currently open through this process. Valid values are positive integers in the range 0 to 2147483647 (expressing seconds) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ID Process The unique identifier of a process. Note that this number applies only while the process is running. After the process ends, the same number might be used to represent a different process. Valid values are positive integers and can include the use of the *MIN, *MAX, or *SUM functions. (Superseded.)

Page Faults/sec The average number of page faults that have occurred for a process per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Page File Bytes The number of bytes of page file space a process uses. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Page File Bytes Peak The maximum number of bytes of page file space a process has used since starting. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Page File kBytes The number of KBs of page file space a process uses. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Page File kBytes Peak The maximum number of KBs of page file space a process has used since starting. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Pool Nonpaged Bytes The number of bytes of pool nonpaged memory a process uses. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Pool Paged Bytes The number of bytes of pool paged memory a process uses. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the

value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Priority Base The current base priority of a process. Valid values are positive integers in the range 1 to 31 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Private Bytes The number of bytes of memory space a process has allocated that cannot be shared with other processes. Valid values are positive integers in the range 0 to 2147483647 (expressing bytes) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Private kBytes The number of KBs of memory space a process has allocated that cannot be shared with other processes. Valid values are positive integers in the range 0 to 2147483647 (expressing KBs) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Process Count The count of process executable instances. The process count is the duplicate occurrences of the binary path data. Note: valid values can include the value Undefined (0) and the value Value_Exceeds_Maximum (2147483647). (Superseded.)

Process Name The process instance name. Valid format is a text string of up to 64 characters. For example, SYS1. (Superseded.)

Server Name The managed system name. The form should be *hostname*:*agent_code*. (Superseded.)

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Thread Count The number of threads currently active in a process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. (Superseded). This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute

SS Second
mmm Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

User The user ID associated with the running process. (Superseded.)

Virtual Bytes The number of bytes of virtual address space that a process uses. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Virtual Bytes Peak The maximum number of bytes of virtual address space a process has used since starting. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Virtual kBytes The number of KBs of virtual address space that a process uses. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Virtual kBytes Peak The maximum number of KBs of virtual address space a process has used since starting. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Working Set The size of the current working set of a process in bytes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Working Set kBytes The size of the current working set of a process in KBs. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Working Set Peak The maximum working set of a process in bytes since the process started. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum. (Superseded.)

Process IO attributes

Use the Processes IO attributes to monitor process statistics.

Binary Path The fully qualified path to the device binary executable running in the process in UTF-8.

ID Process The unique identifier of this process. ID Process numbers are reused, so they only identify a process for the lifetime of that process. Valid values are positive integers.

IO Data Bytes per Sec The rate the process is reading and writing bytes in I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

IO Data Operations per Sec The rate the process is issuing read and write I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

IO Other Bytes per Sec The rate the process is issuing bytes to I/O operations that do not involve data such as control operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

IO Other Operations per Sec The rate the process is issuing I/O operations that are neither a read or a write operation. An example of this type of operation would be a control function. This counter counts all I/O activity generated by the process to include file, network and device I/Os. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

IO Read Bytes per Sec The rate the process is reading bytes from I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

IO Read Operations per Sec The rate the process is issuing read I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

IO Write Bytes per Sec The rate the process is writing bytes to I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

IO Write Operations per Sec The rate the process is issuing write I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum, the value -2147483648 indicates Value_Exceeds_Minimum, and the value -1 indicates Unavailable.

Process Name Instance Name. Valid format is a text string of up to 64 characters.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Processor attributes

Use Processor attributes to create situations that monitor information about each processor on the computer. Processor is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% DPC Time The percentage of processor time spent processing Deferred Procedure Calls (DPCs) during the sample interval. Valid values are positive integers.

% Interrupt Time The percentage of processor time spent processing hardware interrupts during the sample interval.

% Privileged Time The percentage of elapsed time that a processor has been busy executing instructions in non-idle privileged mode. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Processor Time The percentage of elapsed time that a processor has been busy executing non-idle threads. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. The percent value might exceed 100 on multiple processor systems.

% User Time The percentage of elapsed time a processor has been busy executing instructions in non-idle user mode. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. The percent value might exceed 100 on multiple processor systems.

APC Bypasses/sec The rate at which Kernel APC interrupts were avoided. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

DPC Bypasses/sec The rate at which Deferred Procedure Calls (DPCs) on all processors were avoided. (DPCs are interrupts that run at a lower priority than standard interrupts). This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

DPC Queued/sec The overall rate at which Deferred Procedure Calls (DPCs) are added to the DPC queue for the processor. This is not the number of DPCs in the queue. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

DPC Rate The rate at which Deferred Procedure Calls (DPCs) are added to the DPC queue for the processor between the timer ticks of the processor clock. This is not the number of DPCs in the queue. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Interrupts/sec The average number of interrupts a processor has processed per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Processor The processor instance name. Valid format is a text string of up to 64 characters. For example, SYS1.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Processor Information attributes

Use the Process Information attributes to monitor system processors. The data source for these attributes is WMI. To avoid throughput issues with the Microsoft WMI stack, you should limit the collection frequency to 5 minute intervals. This ensures that the Microsoft WMI Data queues have sufficient time to service the WMI queries made for collecting these attributes.

Current Clock Speed Current speed of the processor, in MHz.

L2 Cache Size L2 cache size of the processor. This value is presented in KB.

Load Percentage Load capacity of each processor, averaged to the last second. Processor loading refers to the total computing burden for each processor at one time.

Maximum Clock Speed Maximum speed of the processor, in MHz.

Power Management Support If TRUE, the power of the device can be managed, which means that it can be put in to suspend mode, and so on. The property does not indicate that power management features are enabled, but it does indicate that the logical device power can be managed.

Processor Address Width Processor address width, in bits. This represents the size of a pointer type on the processor. On a 32-bit processor, the value is 32 and on a 64-bit processor it is 64.

Processor Data Width Processor data width, in bits.

Processor Description Processor description.

Processor Device ID Unique identifier of a processor on the system.

Processor ID Processor information that describes the processor features. For an x86 class CPU, the field format depends on the processor support of the CPUID instruction. If the instruction is supported, the property contains 2 (two) DWORD formatted values. The first is an offset of 08h-0Bh, which is the EAX value that a CPUID instruction returns with input EAX set to 1. The second is an offset of 0Ch-0Fh, which is the EDX value that the instruction returns. Only the first two bytes of the property are significant and contain the contents of the DX register at CPU reset all others are set to 0 (zero), and the contents are in DWORD format.

Processor Manufacturer Name of the processor manufacturer.

Processor Name Processor name.

Processor Version Processor revision number that depends on the architecture.

Socket Designation Type of chip socket used on the circuit card.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Processor Summary attributes

Use the Processor Summary attributes to monitor high and low processor information for one server.

High % Interrupt Time Percent of interrupt time for the High Processor.

High % Privileged Time Percent of privileged time for the High Processor.

High % Processor Time Percent of total processor time for the High Processor.

High % User Time Percent of user time for the High Processor.

High Interrupts/sec Number of interrupts per second for the High Processor.

High Process Average Utilization The average processor utilization of the process with the highest processor utilization on this server. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

High Process ID The process ID of the process with the highest processor utilization on this server.

High Process Name The name of the process with the highest processor utilization on this server.

High Processor Name of the processor with the highest utilization.

High Process Utilization The total processor utilization of the process with the highest processor utilization on this server. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Low % Interrupt Time Percent of interrupt time for the Low Processor.

Low % Privileged Time Percent of privileged time for the Low Processor.

Low % Processor Time Percent of total processor time for the Low Processor.

Low % User Time Percent of user time for the Low Processor.

Low Interrupts/sec Number of interrupts per second for the Low Processor. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Low Processor Name of the processor with the lowest utilization.

Processor Interrupt Difference On a multi-processor computer, the difference in processor utilization for interrupt handling between the processor with the highest total utilization percentage and the processor with the lowest total utilization percentage. Note that the processor with the lower total utilization might have an interrupt processing time higher than the higher processor. When this occurs, this attribute has a negative value. On a single processor computer this value is 0. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Processor Privileged Difference On a multi-processor computer, the difference in processor utilization for privileged handling between the processor with the highest total utilization percentage and the processor with the lowest total utilization percentage. Note that the processor with the lower total utilization might have a privileged processing time higher than the higher processor. When this occurs, this attribute has a negative value. On a single processor computer this value is 0. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Processor User Difference On a multi-processor computer, the difference in processor utilization for user handling between the processor with the highest total utilization percentage and the processor with the lowest total utilization percentage. Note that the processor with the lower total utilization has a user processing time higher than the higher processor. When this occurs, this attribute

has a negative value. On a single processor computer this value is 0. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Processor Utilization Difference On a multi-processor computer, the difference in processor total utilization between the processor with the highest total utilization percentage and the processor with the lowest total utilization percentage. On a single processor computer this value is 0. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

RAS Port attributes

Use RAS Port attributes to monitor Remote Access Service Port activity. RAS Port is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Alignment Errors The total number of alignment errors for this connection. Alignment errors occur when a byte received is different from the byte expected. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Buffer Overrun Errors The total number of buffer overrun errors for this connection. Buffer overrun errors occur when the software cannot handle the rate at which data is received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received The total number of bytes received for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The number of bytes received per second for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Transmitted The total number of bytes transmitted for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Transmitted/sec The number of bytes transmitted per second for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

CRC Errors The total number of CRC errors for this connection. CRC errors occur when the frame received contains erroneous data. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Frames Received The total number of data frames received for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Frames Received/sec The number of data frames received per second for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Frames Transmitted The total number of data frames transmitted for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Frames Transmitted/sec The number of data frames transmitted per second for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Percent Compression In The compression ratio for bytes being received. Valid values are positive integers in the range 0 to 100 (expressing a percentage).

Percent Compression Out The compression ratio for bytes being transmitted. Valid values are positive integers in the range 0 to 100 (expressing a percentage).

Port Instance The instance name of the queue. Valid format is a text string of up to 64 characters. For example, tAM1.

Serial Overrun Errors The total number of serial overrun errors for this connection. Serial overrun errors occur when the hardware cannot handle the rate at which data is received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.**Timeout Errors** The total number of timeout errors for this connection. Timeout errors occur when an expected response is not received in time. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Errors The total number of CRC, Timeout, Serial Overrun, Alignment, and Buffer Overrun errors for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Errors/sec The total number of CRC, Timeout, Serial Overrun, Alignment, and Buffer Overrun errors per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

RAS Total attributes

Use RAS Total attributes to monitor Total Remote Access Service activity. RAS Total is a single-instance attribute group.

Alignment Errors The total number of alignment errors for this connection. Alignment errors occur when a byte received is different from the byte expected. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Buffer Overrun Errors The total number of buffer overrun errors for this connection. Buffer overrun errors occur when the software cannot handle the rate at which data is received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received The total number of bytes received for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The number of bytes received per second for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Transmitted The total number of bytes transmitted for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Transmitted/sec The number of bytes transmitted per second for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

CRC Errors The total number of CRC errors for this connection. CRC errors occur when the frame received contains erroneous data. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Frames Received The total number of data frames received for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Frames Received/sec The number of data frames received per second for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Frames Transmitted The total number of data frames transmitted for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Frames Transmitted/sec The number of data frames transmitted per second for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Percent Compression In The compression ratio for bytes being received. Valid values are positive integers in the range 0 to 100 (expressing a percentage).

Percent Compression Out The compression ratio for bytes being transmitted. Valid values are positive integers in the range 0 to 100 (expressing a percentage).

Serial Overrun Errors The total number of serial overrun errors for this connection. Serial overrun errors occur when the hardware cannot handle the rate at which data is received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timeout Errors The total number of timeout errors for this connection. Timeout errors occur when an expected response is not received in time. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour

MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Connections The total number of Remote Access connections. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Errors The total number of CRC, Timeout, Serial Overrun, Alignment, and Buffer Overrun errors for this connection. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Errors/sec The total number of CRC, Timeout, Serial Overrun, Alignment, and Buffer Overrun errors per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Redirector attributes

Use Redirector attributes to monitor IO Statistics of Processes.

Bytes Received/sec The rate of bytes coming in to the redirector from the network. It includes all application data as well as network protocol information (such as packet headers). This attribute is the 64-bit version of Bytes Received/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Received/sec (Superseded) The rate of bytes coming in to the redirector from the network. It includes all application data as well as network protocol information (such as packet headers). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Total/sec The rate the redirector is processing data bytes. This includes all application and file data in addition to protocol information such as packet headers. This attribute is the 64-bit version of Bytes Total/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Total/sec (Superseded) The rate the redirector is processing data bytes. This includes all application and file data in addition to protocol information such as packet headers. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Transmitted/sec The rate at which bytes are leaving the redirector to the network. It includes all application data as well as network protocol information (such as packet headers). This attribute is the 64-bit version of Bytes Transmitted/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Transmitted/sec (Superseded) The rate at which bytes are leaving the redirector to the network. It includes all application data as well as network protocol information (such as packet headers). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connects Core The number of connections you have to servers running the original MS-Net SMB protocol, including MS-Net itself, Xenix, and VAXs. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connects LAN Manager 2.0 Counts connections to LAN Manager 2(dot)0 servers, including LMX servers. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connects LAN Manager 2.1 Counts connections to LAN Manager 2(dot)1 servers, including LMX servers. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connects Windows NT Counts the connections to Windows 2000 or earlier computers. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Commands Counts the number of requests to the redirector that are currently queued for service. If this number is much larger than the number of network adapter cards installed in the computer, then the networks and the servers being accessed are bottlenecked. Valid values are positive integers. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Data Operations/sec The rate at which the redirector is processing data operations. One operation can include many bytes, since each operation has overhead. The efficiency of this path can be determined by dividing the Bytes/sec by this counter to obtain the average number of bytes transferred per operation. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Read Operations/sec The rate at which applications are asking the redirector for data. Each call to a file system or similar Application Program Interface (API) call counts as one operation. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Write Operations/sec The rate at which applications are sending data to the redirector. Each call to a file system or similar Application Program Interface (API) call counts as one operation. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

High % Bytes/Sec The percentage of network card bandwidth that is used by the redirector (workstation) service. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

High Current Mod The average number of requests, per network interface card, to the redirector that are currently queued for service. This value is calculated as Current Commands ÷ NIC Count. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Network Errors/sec The rate at which serious unexpected errors are occurring. Such errors generally indicate that the redirector and one or more servers are having communication difficulties. For example, an SMB (Server Manager Block) protocol error is a Network Error. An entry is written to the System Event Log and provide details. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Received/sec The rate at which the redirector is receiving packets (also called SMBs or Server Message Blocks). Network transmissions are divided in to packets. The average number of bytes received in a packet can be obtained by dividing Bytes Received/sec by this counter. Some packets received might not contain incoming data (for example, an acknowledgment to a write made by the redirector counts as an incoming packet). This attribute is the 64-bit version of Packets Received/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Received/sec (Superseded) The rate at which the redirector is receiving packets (also called SMBs or Server Message Blocks). Network transmissions are divided in to packets. The average number of bytes received in a packet can be obtained by dividing Bytes Received/sec by this counter. Some packets received might not contain incoming data (for example, an acknowledgment to a write made by the redirector counts as an incoming packet). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets Transmitted/sec The rate at which the redirector is sending packets (also called SMBs or Server Message Blocks). Network transmissions are divided in to packets. The average number of bytes transmitted in a packet can be obtained by dividing Bytes Transmitted/sec by this counter. This attribute is the 64-bit version of Packets_Transmitted/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets Transmitted/sec (Superseded) The rate at which the redirector is sending packets (also called SMBs or Server Message Blocks). Network transmissions are divided in to packets. The average number of bytes transmitted in a packet can be obtained by dividing Bytes Transmitted/sec by this counter. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Packets/sec The rate the redirector is processing data packets. One packet includes many bytes, but each packet has protocol overhead. You can determine the efficiency of this path by dividing the Bytes/sec by this counter to determine the average number of bytes transferred/packet. You can also divide this counter by Operations/sec to determine the average number of packets per operation, another measure of efficiency. This attribute is the 64-bit version of Packets/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Packets/sec (Superseded) The rate the redirector is processing data packets. One packet includes many bytes, but each packet has protocol overhead. You can determine the efficiency of this path by dividing the Bytes/sec by this counter to determine the average number of bytes transferred/packet. You can also divide this counter by Operations/sec to determine the average number of packets per operation, another measure of efficiency. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Bytes Cache/sec The rate at which applications are accessing the file system cache by using the redirector. Some of these data requests are satisfied by retrieving the data from the cache. Requests that miss the cache cause a page fault (see Read Bytes Paging/sec). This attribute is the 64-bit version of Read Bytes Cache/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Read Bytes Cache/sec (Superseded) The rate at which applications are accessing the file system cache by using the redirector. Some of these data requests are satisfied by retrieving the data from the cache. Requests that miss the cache cause a page fault (see Read Bytes Paging/sec). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Bytes Network/sec The rate at which applications are reading data across the network. This occurs when data sought in the file system cache is not found there and must be retrieved from the network. Dividing this value by Bytes Received/sec indicates the proportion of application data traveling across the network (see Bytes Received/sec). This attribute is the 64-bit version of Read Bytes Network/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Read Bytes Network/sec (Superseded) The rate at which applications are reading data across the network. This occurs when data sought in the file system cache is not found there and must be retrieved from the network. Dividing this value by

Bytes Received/sec indicates the proportion of application data traveling across the network (see Bytes Received/sec). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Bytes Non-Paging/sec The bytes read by the redirector in response to normal file requests by an application when they are redirected to come from another computer. In addition to file requests, this counter includes other methods of reading across the network such as Named Pipes and Transactions. This counter does not count network protocol information, just application data. This attribute is the 64-bit version of Read Bytes Non-Paging/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Read Bytes Non-Paging/sec (Superseded) The bytes read by the redirector in response to normal file requests by an application when they are redirected to come from another computer. In addition to file requests, this counter includes other methods of reading across the network such as Named Pipes and Transactions. This counter does not count network protocol information, just application data. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Bytes Paging/sec The rate at which the redirector is attempting to read bytes in response to page faults. Page faults are caused by loading of modules (such as programs and libraries), by a miss in the cache (see Read Bytes Cache/sec), or by files directly mapped in to the address space of applications. This attribute is the 64-bit version of Read Bytes Paging/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Read Bytes Paging/sec (Superseded) The rate at which the redirector is attempting to read bytes in response to page faults. Page faults are caused by loading of modules (such as programs and libraries), by a miss in the cache (see Read Bytes Cache/sec), or by files directly mapped in to the address space of applications. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Operations Random/sec The rate at which, on a file-by-file basis, reads are made that are not sequential. If a read is made using a particular file handle, and then is followed by another read that is not immediately the contiguous next byte, this counter is incremented by one. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Packets Small/sec The rate at which reads less than one-fourth of the server negotiated buffer size are made by applications. Too many of these could indicate a waste of buffers on the server. This counter is incremented once for each read. It does not count packets. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Packets/sec The rate at which read packets are being placed on the network. Each time a single packet is sent with a request to read data remotely, this counter is incremented by one. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Reads Denied/sec The rate at which the server is unable to accommodate requests for raw reads. When a read is much larger than the server's negotiated buffer size, the redirector requests a raw read which, if granted, would permit the transfer of the data without a lot of protocol overhead on each packet. To accomplish this, the server must lock out other requests, therefore the request is denied if the server is very busy. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Reads Large/sec The rate at which reads more than twice the negotiated buffer size of the server are made by applications. Too many of these could place a strain on server resources. This counter is incremented once for each read. It does not count packets. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Disconnects The number of times a server has disconnected your redirector. (See also Server Reconnects.) Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Reconnects The number of times your redirector has had to reconnect to a server in order to complete a new active request. You can be disconnected by the server if you remain inactive for too long. Locally even if all your remote files are closed, the redirector keeps your connections intact for (nominally) 10 minutes. Such inactive connections are called Dormant Connections. Reconnecting is expensive in time. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Sessions The total number of security objects the redirector has managed. For example, a logon to a server followed by a network access to the same server establishes one connection, but two sessions. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Sessions Hung The number of active sessions that are timed out and unable to proceed due to a lack of response from the remote server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the

*AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Write Bytes Cache/sec The rate at which applications on your computer are writing to the file system cache by using the redirector. The data might not leave your computer immediately; it can be retained in the cache for further modification before being written to the network. This saves network traffic. Each write of a byte in to the cache is counted here. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Write Bytes Cache/sec (Superseded) The rate at which applications on your computer are writing to the file system cache by using the Redirector. The data might not leave your computer immediately; it can be retained in the cache for further modification before being written to the network. This saves network traffic. Each write of a byte in to the cache is counted here. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Write Bytes Network/sec The rate at which applications are writing data across the network. This occurs when the file system cache is bypassed, such as for Named Pipes or Transactions, or when the cache writes the bytes to disk to make room for other data. Dividing this counter by Bytes Transmitted/sec indicates the proportion of application data being to the network (see Transmitted Bytes/sec). This attribute is the 64-bit version of Write Bytes Network/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Write Bytes Network/sec (Superseded) The rate at which applications are writing data across the network. This occurs when the file system cache is bypassed, such as for Named Pipes or Transactions, or when the cache writes the bytes to disk to make room for other data. Dividing this counter by Bytes Transmitted/sec indicates the proportion of application data being to the network (see Transmitted Bytes/sec). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Write Bytes Non-Paging/sec The rate at which bytes are written by the redirector in response to normal file outputs by an application when they are redirected to another computer. In addition to file requests, this count includes other methods of writing across the network, such as Named Pipes and Transactions. This counter does not count network protocol information, just application data. This attribute is the 64-bit version of Write Bytes Non-Paging/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Write Bytes Non-Paging/sec (Superseded) The rate at which bytes are written by the redirector in response to normal file outputs by an application when they are redirected to another computer. In addition to file requests, this count includes other methods of writing across the network, such as Named Pipes and Transactions. This counter does not count network protocol information, just application data. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Write Bytes Paging/sec The rate at which the redirector is attempting to write bytes changed in the pages being used by applications. The program data changed by modules (such as programs and libraries) that were loaded over the network are 'paged out' when no longer needed. Other output pages come from the file system cache (see Write Bytes Cache/sec). This attribute is the 64-bit version of Write Bytes Paging/Sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Write Bytes Paging/sec (Superseded) The rate at which the redirector is attempting to write bytes changed in the pages being used by applications. The program data changed by modules (such as programs and libraries) that were loaded over the network are 'paged out' when no longer needed. Other output pages come from the file system cache (see Write Bytes Cache/sec). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Write Operations Random/sec The rate at which, on a file-by-file basis, writes are made that are not sequential. If a write is made using a particular file handle, and then is followed by another write that is not immediately the next contiguous byte, this counter is incremented by one. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Write Packets Small/sec The rate at which writes are made by applications that are less than one-fourth of the negotiated buffer size of the server. Too many of these could indicate a waste of buffers on the server. This counter is incremented once for each write: it counts writes, not packets. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Write Packets/sec The rate at which writes are being sent to the network. Each time a single packet is sent with a request to write remote data, this counter is incremented by one. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Writes Denied/sec The rate at which the server is unable to accommodate requests for Raw Writes. When a write is much larger than the server's negotiated buffer size, the redirector requests a raw write which, if granted, would permit the transfer of the data without lots of protocol overhead on each packet. To accomplish this the server must lock out other requests, so the request is denied if the server is really busy. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Writes Large/sec The rate at which writes are made by applications that are more than twice the negotiated buffer size of the server. Too many of these could place a strain on server resources. This counter is incremented once for each write: it counts writes, not packets. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Registry attributes

Use the Registry attributes to monitor for specific values or changes in registry data.

When creating situations using the Registry attribute group you must supply values for the following attributes to restrict the monitoring for the situation:

- Path Name
- String Value
- Root Key Name

Note: The product provided NT_Registry workspace query does not produce data unless a situation is defined against this attribute group.

Numeric Value Registry Numeric Data Value. Contains numeric data for any registry entry whose type is defined as any of the numeric data types. These include: Binary, DWORD, Big Endian, QWORD. Valid values are positive integers representing any of the enumerated values for Windows Registry keys.

Path Name The Path is the concatenation of the registry sub-key and the registry value name. Valid format is a text string of up to 388 characters.

Root Key Name Registry Root key name. Valid values are positive integers representing any of the enumerated values for Windows Registry keys. Valid values include HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, HKEY_LOCAL_MACHINE, HKEY_USERS, HKEY_PERFORMANCE_DATA, HKEY_CURRENT_CONFIG, HKEY_DYN_DATA, HKEY_PERFORMANCE_TEXT, and HKEY_PERFORMANCE_NLSTEXT. When creating a situation using this attribute field, if you are using a remote machine, then only HKEY_LOCAL_MACHINE and HKEY_USER are allowed.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

String Value Registry String Data Value. Contains string data for any registry entry whose type is defined as any of the string data types. These include: String, Expandable String, Multiple String. Valid format is a text string of up to 1,128 characters.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Type Registry value type. Valid values are positive integers representing any of the enumerated values for Windows Registry keys. Valid values include Undefined, String, Expandable_String, Binary, DWORD, DWORD_Big_Endian, Link, Multiple_String, Resource_List, Full_Resource_Descriptor, Resource_Requirements, and QWORD.

Server attributes

Use the Server attributes to monitor connections and throughput between the local computer (Server/Redirector) and the network.

Blocking Requests Rejected The number of times the server has rejected blocking SMBs due to insufficient count of free work items. Indicates whether the MaxWorkItem or MinFreeWorkItems server parameters might need to be adjusted. Valid values are positive integers in the range 0 to 2147483647 and can include the

use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The number of bytes the server has received from the network. Indicates how busy the server is. This attribute is the 64-bit version of Bytes Received/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Received/sec (Superseded) The number of bytes the server has received from the network. Indicates how busy the server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Total/sec The number of bytes the server has sent to and received from the network. This value provides an overall indication of how busy the server is. This attribute is the 64-bit version of Bytes Total/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Total/sec (Superseded) The number of bytes the server has sent to and received from the network. This value provides an overall indication of how busy the server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Transmitted/sec The number of bytes the server has sent on the network. Indicates how busy the server is. This attribute is the 64-bit version of Bytes_Transmitted/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Transmitted/sec (Superseded) The number of bytes the server has sent on the network. Indicates how busy the server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Context Blocks Queued/sec The rate at which work context blocks had to be placed on the FSP queue of the server to await server action. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Errors Access Permissions The number of times opens on behalf of clients have failed with STATUS_ACCESS_DENIED. Can indicate whether somebody is randomly attempting to access files in hopes of getting at something that was not properly protected. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Errors Granted Access The number of times accesses to files opened successfully were denied. Can indicate attempts to access files without proper access authorization. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Errors Logon The number of failed logon attempts to the server. Can indicate whether password guessing programs are being used to crack the security on the server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Error Session Percent Percentage of total sessions that ended due to errors.

Errors System The number of times an internal Server Error was detected. Unexpected errors usually indicate a problem with the Server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

File Directory Searches The number of searches for files currently active in the server. Indicates current server activity. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Open The number of files currently opened in the server. Indicates current server activity. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Opened Total The number of successful open attempts performed by the server on behalf of clients. Useful in determining the amount of file I/O, determining overhead for path-based operations, and for determining the effectiveness of open locks. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

High % Bytes/Sec The percentage of network card bandwidth used by the server service. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum.

Logon Total Includes all interactive logons, network logons, service logons, successful logons, and failed logons since the system is last rebooted. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Logon/sec The rate of all server logons. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged Bytes The number of bytes of non-pageable computer memory the server is using. This value is useful for determining the values of the MaxNonpagedMemoryUsage value entry in the Windows NT Registry. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged Failures The number of times allocations from nonpaged pool have failed. Indicates that the computer's physical memory is too small. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Nonpaged Peak The maximum number of bytes of nonpaged pool the server has had in use at any one point. Indicates how much physical memory the computer should have. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Pool Paged Bytes The number of bytes of pageable computer memory the server is currently using. Can help in determining good values for the MaxPagedMemoryUsage parameter. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Failures The number of times allocations from paged pool have failed. Indicates that the computer's physical memory or paging file are too small. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Pool Paged Peak The maximum number of bytes of paged pool the server has had allocated. Indicates the proper sizes of the Page File(s) and physical memory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Server Sessions The number of sessions currently active in the server. Indicates current server activity. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sessions Errored Out The number of sessions that have been closed due to unexpected error conditions or sessions that have reached the autodisconnect timeout and have been disconnected normally. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sessions Forced Off The number of sessions that have been forced to logoff. Can indicate how many sessions were forced to logoff due to logon time constraints. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sessions Logged Off The number of sessions that have terminated normally. Useful in interpreting the Sessions Times Out and Sessions Errored Out statistics, allows percentage calculations. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Sessions Timed Out The number of sessions that have been closed due to their idle time exceeding the AutoDisconnect parameter for the server. Shows whether the AutoDisconnect setting is helping to conserve resources. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Ended Sessions Total number of sessions that have ended. Calculated as the sum of Sessions Errored Out, Sessions Forced Off, Sessions Logged Off, and Sessions Timed Out. This attribute is the 64-bit version of Total Ended Sessions. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Total Ended Sessions (Superseded) Total number of sessions that have ended. Calculated as the sum of Sessions Errored Out, Sessions Forced Off, Sessions

Logged Off, and Sessions Timed Out. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Work Item Shortages The number of times STATUS_DATA_NOT_ACCEPTED was returned at receive indication time. This occurs when no work item is available or can be allocated to service the incoming request. Indicates whether the InitWorkItems or MaxWorkItems parameters might need to be adjusted. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Work Queue attributes

Use the Server Work Queue attributes to monitor information about server work queue throughput, work items in the queue, and threads servicing the queue.

Active Threads The number of threads currently working on a request from the server client for this CPU. The system keeps this number as low as possible to minimize unnecessary context switching. This is an instantaneous count for the CPU, not an average over time. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Available Threads The number of server threads on this CPU not currently working on requests from a client. The server dynamically adjusts the number of threads to maximize server performance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Available Work Items The instantaneous number of available work items for this CPU. A sustained near-zero value indicates the need to increase the MinFreeWorkItems registry value for the Server service. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Borrowed Work Items The number of borrowed work items. Every request from a client is represented in the server as a 'work item,' and the server maintains a pool of available work items per CPU to speed processing. When a CPU runs out of work items, it borrows a free work item from another CPU. An increasing value of this running counter might indicate the need to increase the 'MaxWorkItems' or 'MinFreeWorkItems' registry values for the Server service. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The rate at which the Server is receiving bytes from the network clients on this CPU. This value is a measure of how busy the Server is. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate at which the Server is sending bytes to the network clients on this CPU. This value is a measure of how busy the Server is. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Transferred/sec The rate at which the Server is sending and receiving bytes with the network clients on this CPU. This value is a measure of how busy the Server is. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Context Blocks Queued/sec The rate at which work context blocks had to be placed on the FSP queue of the server to await server action. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Clients The instantaneous count of the clients being serviced by this CPU. The server actively balances the client load across all of the CPU's in the system. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Queue Length The current length of the server work queue for this CPU. A sustained queue length greater than four might indicate processor congestion. This is an instantaneous count, not an average over time. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Bytes/sec The rate the server is reading data from files for the clients on this CPU. This value is a measure of how busy the Server is. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Read Operations/sec The rate the server is performing file read operations for the clients on this CPU. This value is a measure of how busy the Server is. This value is always 0 in the Blocking Queue instance. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Bytes/sec The rate the Server is reading and writing data to and from the files for the clients on this CPU. This value is a measure of how busy the Server is. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Total Operations/sec The rate the Server is performing file read and file write operations for the clients on this CPU. This value is a measure of how busy the Server is. This value is always 0 in the Blocking Queue instance. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Work Item Shortages The number of times a request waited for an available workitem from the pool. Every request from a client is represented in the server as a 'work item,' and the server maintains a pool of available work items per CPU to speed processing. A sustained value greater than zero indicates the need to increase the 'MaxWorkItems' registry value for the Server service. This value is always 0 in the Blocking Queue instance.

Work Queue Name Instance Name. Valid format is a text string of up to 64 characters.

Write Bytes/sec The rate the server is writing data to files for the clients on this CPU. This value is a measure of how busy the Server is. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Write Operations/sec The rate the server is performing file write operations for the clients on this CPU. This value is a measure of how busy the Server is. This value is always 0 in the Blocking Queue instance. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Server Work Queue attributes (32-bit - Superseded)

Use the Server Work Queue attributes to monitor information about server work queue throughput, work items in the queue, and threads servicing the queue. This attribute group is superseded. There is a new attribute group with the same name that replaces it.

Active Threads The number of threads currently working on a request from the server client for this CPU. The system keeps this number as low as possible to minimize unnecessary context switching. This is an instantaneous count for the CPU, not an average over time. Valid values are positive integers in the range 0 to

2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Available Threads The number of server threads on this CPU not currently working on requests from a client. The server dynamically adjusts the number of threads to maximize server performance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Available Work Items The instantaneous number of available work items for this CPU. A sustained near-zero value indicates the need to increase the MinFreeWorkItems registry value for the Server service. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Borrowed Work Items The number of borrowed work items. Every request from a client is represented in the server as a 'work item,' and the server maintains a pool of available work items per CPU to speed processing. When a CPU runs out of work items, it borrows a free work item from another CPU. An increasing value of this running counter might indicate the need to increase the 'MaxWorkItems' or 'MinFreeWorkItems' registry values for the Server service. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The rate at which the Server is receiving bytes from the network clients on this CPU. This value is a measure of how busy the Server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate at which the Server is sending bytes to the network clients on this CPU. This value is a measure of how busy the Server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Transferred/sec The rate at which the Server is sending and receiving bytes with the network clients on this CPU. This value is a measure of how busy the Server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Context Blocks Queued/sec The rate at which work context blocks had to be placed on the FSP queue of the server to await server action. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.)

Current Clients The instantaneous count of the clients being serviced by this CPU. The server actively balances the client load across all of the CPU's in the system. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Queue Length The current length of the server work queue for this CPU. A sustained queue length greater than four might indicate processor congestion. This is an instantaneous count, not an average over time. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Bytes/sec The rate the server is reading data from files for the clients on this CPU. This value is a measure of how busy the Server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Read Operations/sec The rate the server is performing file read operations for the clients on this CPU. This value is a measure of how busy the Server is. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Name The managed system name. (Superseded.) The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. (Superseded.) Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Bytes/sec The rate the Server is reading and writing data to and from the files for the clients on this CPU. This value is a measure of how busy the Server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Operations/sec The rate the Server is performing file read and file write operations for the clients on this CPU. This value is a measure of how busy the Server is. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Work Item Shortages The number of times a request waited for an available work item from the pool. Every request from a client is represented in the server as a 'work item,' and the server maintains a pool of available work items per CPU to speed processing. A sustained value greater than zero indicates the need to increase the 'MaxWorkItems'registry value for the Server service. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Work Queue Name Instance Name. Valid format is a text string of up to 64 characters. (Superseded.)

Write Bytes/sec The rate the server is writing data to files for the clients on this CPU. This value is a measure of how busy the Server is. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Write Operations/sec The rate the server is performing file write operations for the clients on this CPU. This value is a measure of how busy the Server is. This value is always 0 in the Blocking Queue instance. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. (Superseded.) Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Service Dependencies attributes

Use Service Dependencies attributes to obtain configuration information about all of the services or load order groups that must start before a given service installed on the Windows Server. Services are background processes run by the operating system, regardless of the user logged in to the system. Service Dependencies is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Dependency The name of a service or load order group that must start before the given service can start. If there are no dependencies for the given service, this field is blank. Valid format is a text string of up to 64 characters. For example, +TID indicates the name of a load order group that must start first.

Display Name The name of the service as it is displayed in the Service Control Manager applet. Valid format is a text string of up to 64 characters. For example, Gateway Service indicates the name of the service.

Display Name (Unicode) The name of the service as it is displayed in the NT Service Control Manager applet in UTF8. Valid format is a text string of up to 400 bytes.

Server Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Service Name The internal name of the service in the Service Control Manager database. Valid format is a text string of up to 64 characters. For example, NWCWorkstation is an example of a service name.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Services attributes

Use Services attributes to obtain status and configuration information about all of the services installed on the Windows Server. Services are background processes run by the operating system, regardless of the user logged in to the system. Services is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Account ID The account name under which the service process is logged on when it runs. It takes the form of DomainName\UserName such as LocalSystem. Valid format is a text string of up to 32 characters.

Account ID (Unicode) The account name under which the service process is logged on when it runs in UTF8. It takes the form of DomainName\UserName such as .\LocalSystem. Valid format is a text string of up to 52 bytes.

Binary Path The fully qualified path to the service binary executable. Valid format is a text string of up to 64 characters. For example, D:\WINNT\System32\ Services.exe indicates the path to the service binary executable.

Binary Path (Unicode) The fully qualified path to the service binary executable in UTF8. Valid format is a text string of up to 392 bytes.

Current State The current state of the service. This state can be Stopped, Start Pending, Stop Pending, Running, Continue Pending, Paused Pending, Paused, or Unknown. Valid format is a text string of up to 20 characters. For example, Running indicates that the service is currently running.

Display Name The name of the service as it is displayed in the Service Control Manager applet. Valid format is a text string of up to 64 characters. For example, Gateway Service for Network is an example of a display name.

Display Name (Unicode) The name of the service as it is displayed in the NT Service Control Manager applet in UTF8. Valid format is a text string of up to 400 bytes.

Load Order Group The name of the load ordering group of which this service is a member. Services can be placed in groups so other services can have dependencies on a group of services. If the service is not in a load ordering group, then this field is blank. Valid format is a text string of up to 64 characters. For example, Network Provider is an example of a load order group.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Service Name (Unicode) The internal name of the service in the Service Control Manager database. Valid format is a text string of up to 256 characters. For example, NWCWorkstation is an example of a service name.

Service Name The internal name of the service in the Service Control Manager database. The maximum size of the string is 64 bytes.

Start Type Specifies how to start the service. Valid format is a text string of up to 16 characters. The following values are valid:

- Boot
- System
- Automatic
- Manual
- Disabled
- Unknown

- Delayed

Note: It can be Delayed on Windows 2008 or later systems.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

SMTP Server attributes

Use SMTP (Simple Mail Transfer Protocol) Server attributes to create situations to monitor a wide range of activities associated with the hosting of an electronic mail server. SMTP Server is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Recipients Local The percentage of recipients that is delivered locally. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Recipients Remote The percentage of recipients that is delivered remotely. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Avg Recipients/msg Received The average number of recipients per inbound message received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Avg Recipients/msg Sent The average number of recipients per outbound messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Avg Retries/msg Delivered The average number of retries per local delivery. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Avg Retries/msg Sent The average number of retries per outbound message sent. Valid values are positive integers in the range 0 to 2147483647 and can include the

use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The rate that bytes are received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate that bytes are sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

kBytes Received Total The total number of KBs received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

kBytes Sent Total The total number of KBs sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

kBytes Total The total number of KBs sent and received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Total/sec The rate that bytes are sent and received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connection Errors/sec The number of connection errors per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Directory Drops Total The total number of messages placed in a drop directory. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Directory Drops/sec The number of messages placed in a drop directory per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Directory Pickup Queue Length The number of messages in the directory pickup queue.

Note that this attribute is not available on systems running Windows 2000 with IIS 5.0. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

DNS Queries Total The total number of DNS lookups. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

DNS Queries/sec The rate of DNS lookups. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ETRN Messages Total The total number of ETRN messages received by the server. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ETRN Messages/sec The number of ETRN messages per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Inbound Connections Current The total number of connections currently inbound. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Inbound Connections Total The total number of inbound connections received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Local Queue Length The number of messages in the local queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Local Retry Queue Length The number of messages in the local retry queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Message Bytes Received/sec The rate that bytes are received in messages. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Message Bytes Sent/sec The rate that bytes are sent in messages. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Message kBytes Received Total The total number of KBs received in messages. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Message kBytes Sent Total The total number of KBs sent in messages. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Message kBytes Total The total number of KBs sent and received in messages. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Message Bytes Total/sec The rate that bytes are sent and received in messages. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Message Delivery Retries The total number of local deliveries that were retried. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Message Send Retries The total number of outbound message sends that were retried. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Delivered Total The total number of messages delivered to local mailboxes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Delivered/sec The rate that messages are delivered to local mailboxes. Valid values are positive integers in the range 0 to 2147483647 and can include the

use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Received/sec The rate that inbound messages are being received. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Received Total The total number of inbound messages accepted. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Refused for Address Objects The total number of messages refused due to no address objects. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Refused for Mail Objects The total number of messages refused due to no mail objects. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Refused for Size The total number of messages rejected because they were too big. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Retrieved/sec The rate that messages are being retrieved from the mail pick-up directory. Note: -1 indicates Undefined, 2147483647 indicates Value_Exceeds_Maximum, and -2147483648 indicates Value_Exceeds_Minimum.

Messages Retrieved Total The total number of messages retrieved from the mail pick-up directory. Note: -1 indicates Undefined, 2147483647 indicates Value_Exceeds_Maximum, and -2147483648 indicates Value_Exceeds_Minimum.

Messages Sent/sec The rate that outbound messages are being sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Messages Sent Total The total number of outbound messages sent. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

NDRs Generated The number of non-delivery reports that have been generated. Valid values are positive integers in the range 0 to 2147483647 and can include the

use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Number of MailFiles Open Number of handles to open mail files. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Number of QueueFiles Open Number of handles to open queue files. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Outbound Connections Current The number of connections currently outbound. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Outbound Connections Refused The number of outbound connection attempts refused by remote sites. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Outbound Connections Total The total number of outbound connections attempted. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Remote Queue Length The number of messages in the remote queue. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Remote Retry Queue Length The number of messages in the retry queue for remote delivery. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Routing Table Lookups Total The total number of routing table lookups. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Routing Table Lookups/sec The number of routing table lookups per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of

the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

SMTP Server Instance name of SMTP virtual server. Valid format is a text string of up to 64 characters.

System Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Connection Errors The total number of connection errors. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System attributes

Use System attributes to monitor total count information for all processors on a system. This information represents overall system activity. System is a single-instance attribute group.

% Total Privileged Time The total percentage of elapsed time a system has been busy executing instructions in privileged mode.

Note that this attribute is not available on systems running Windows 2000 or higher. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown.

% Total Processor Time The % Total Processor Time is the average percentage of time that all the processors on the system are busy executing non-idle threads. On a multiprocessor system, if all processors are always busy this is 100%, if all

processors are 50% busy this is 50% and if one-fourth of the processors are busy this is 25%. It can be viewed as the fraction of the time spent doing useful work. Each processor is assigned an Idle thread in the Idle process which consumes those unproductive processor cycles not used by any other threads. Note: -1 indicates Unknown.

Note that this attribute is not available on systems running Windows 2000 or higher. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *MIN, *MAX, or *SUM functions.

% Total User Time The average percentage of time all processors have been busy executing instructions in user mode. Note: -1 indicates Unknown.

Note that this attribute is not available on systems running Windows 2000 or higher. Valid values are positive integers in the range 0 to 100 (expressing a percentage) and can include the use of the *MIN, *MAX, or *SUM functions.

Alignment Fixups/sec The rate of alignment faults fixed by the system. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Context Switches/sec The total number of context switches that have occurred on a system per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Exception Dispatches/sec The rate of exceptions dispatched by the system. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Control Bytes/sec The aggregate of bytes transferred for all file system operations that are neither reads nor writes. These operations usually include file system control requests or requests for information about device characteristics or status. This attribute is the 64-bit version of File Control_Bytes/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

File Control Bytes/sec (Superseded) The total number of bytes the system has transferred per second for all file control operations. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Control Operations/sec The total number of file control operations the system has executed per second. This includes operations which are neither reads nor writes, such as file system control requests. Valid values are positive integers in the

range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Data Operations/sec The total number of read and write operations the system has executed per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Read Bytes/sec The aggregate of the bytes transferred for all the file system read operations on the computer. This attribute is the 64-bit version of File Read Bytes/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

File Read Bytes/sec (Superseded) The average number of bytes the system transferred per second for all file system read operations. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Read Operations/sec The total number of file read operations the system has executed per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Write Bytes/sec The aggregate of the bytes transferred for all the file system write operations on the computer. This attribute is the 64-bit version of File Write Bytes/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

File Write Bytes/sec (Superseded) The total number of bytes the system has transferred per second for all file write operations. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

File Write Operations/sec The total number of file write operations the system has executed per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Floating Emulations/sec The rate of floating emulations performed by the system. This counter displays the difference between the values observed in the last two samples, divided by the duration of the sample interval. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Network Address The host address of a system. Valid format is a text string. Note that the value No_DNS_Entry is a valid value.

Network Address IPv6 The IPv6 host address for the computer. Note that the value No_DNS_Entry is a valid value.

Number of Logical Processors The number of the logical processors on the system. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Number of Processors The total number of processors in a system. Valid values are positive integers in the range 0 to 999 and can include the use of the *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Operating System Type The marketed operating system name of the installed OS version. Valid values include Windows_Svr_2003 for version 5.2, Windows_2000 for version 5.0, and Windows_XP for version 5.1.

Operating System Version The operating system version number of a system. Valid format is a text string.

Page File Size (MB) Size of the system paging file, in MB. Note: -1 indicates Unknown.

Page Size (Bytes) The size of a page of virtual memory on a system in bytes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Processor Queue Length (Threads) The total number of threads waiting for processor time on a system. Valid values are positive integers in the range 0 to 2147483647. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Processor Queue Length Excess The number of processor queue length requests in excess of the number of processors in the system. This indicates that the processor(s) are not able to service the work load that is requested of them. Calculated as Processor Queue Length - number of processes. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Processor Type The processor type of a system. Valid format is a text string. Valid values are positive integers in the range of 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

System Calls/sec The number of calls made to system service routines per second. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Up Time (Days) Total Time (in days) that the computer has been operational since it was last started. Valid values include Less_Than_One_Day.

System Up Time (Seconds) The total time (in seconds) that the computer has been operational since it was last started. This attribute is the 64-bit version of System Up Time (Seconds). Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

System Up Time (Seconds) (Superseded) The total amount of time the system has been operational since it was last started. Valid values are positive integers in the range 0 to 2147483647 (expressing seconds) and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Interrupts/sec The rate at which the system is receiving and servicing hardware interrupts. Note that this attribute is not available on systems running Windows 2000 or higher. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown, 2147483647 indicates Value_Exceeds_Maximum and -2147483648 indicates Value_Exceeds_Minimum.

Total Memory Size (MB) The number of MBs of installed random access memory (RAM) in the computer. Note: -1 indicates Unknown.

User Name The name of a unique user account. Valid format is a text string. For example, LBROWN.

User Name (Unicode) The name of a unique user account in UTF8. Valid format is a text string of up to 388 bytes.

TCP Statistics attributes

Use TCP Statistics attributes to monitor connection statistics and segment traffic for data using the TCP protocol. TCP Statistics is a single-instance attribute group. This attribute group reports IPv4 statistics. IPv6 statistics are reported separately on Windows 2003.

Connections Active The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connections Established The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connection Failures The number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or from the SYN-RCVD state. This number also includes the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVC state. Valid format is a text string of up to 64 characters. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connections Passive The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state. Valid format is a text string of up to 64 characters. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connections Reset The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state. Valid format is a text string of up to 64 characters. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Segments Received/sec The rate that segments are received, including those received in error. This count includes segments received on currently established connections. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Segments Retransmitted/sec The rate that segments are retransmitted, that is, segments transmitted containing one or more previously transmitted bytes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Segments/sec The rate that TCP segments are sent or received using the TCP protocol. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Segments Sent/sec The rate that segments are sent, including those on current connections. This count excludes those containing only retransmitted bytes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Thread attributes

Use Thread attributes to monitor information about a specific threads within a process, such as the amount of time the thread runs, its CPU usage, and its state. Thread is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

% Privileged Time The percentage of elapsed time that this thread has spent executing code in privileged mode. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% Processor Time The percentage of elapsed time that this thread used the processor to execute instructions. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

% User Time The percentage of elapsed time that this thread has spent executing code in user mode. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Context Switches/Sec The rate of switches from one thread to another. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Elapsed Time (Seconds) The total elapsed time (in seconds) this thread has been running. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ID Process The unique identifier of this process. ID Process numbers are reused, so they only identify a process for the lifetime of that process. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

ID Thread The unique identifier of this thread. ID Thread numbers are reused, so they only identify a thread for the lifetime of that thread. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Priority Base The current base priority of this thread. The system can raise and lower a thread's base priority relative to the process base priority. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Priority Current The current priority of this thread. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Server Name The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Start Address The starting virtual address for this thread. Valid values are hex strings.

Thread Instance Instance Name for thread (Process/ThreadID). Valid format is a text string of up to 64 characters.

Thread State The current state of the thread. It is 0 for Initialized, 1 for Ready, 2 for Running, 3 for Standby, 4 for Terminated, 5 for Wait, 6 for Transition, 7 for

Unknown. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Thread Wait Reason Thread Wait Reason is only applicable when the thread is in the Wait state (see Thread State). It is 0 or 7 when the thread is waiting for the Executive, 1 or 8 for a Free Page, 2 or 9 for a Page In, 3 or 10 for a Pool Allocation, 4 or 11 for an Execution Delay, 5 or 12 for a Suspended condition, 6 or 13 for a User Request, 14 for an Event Pair High, 15 for an Event Pair Low, 16 for an LPC Receive, 17 for an LPC Reply, 18 for Virtual Memory, 19 for a Page Out; 20 and higher are not assigned at the time of this writing. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. Date and time of the sample are displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

UDP Statistics attributes

Use UDP Statistics attributes to monitor datagram traffic for data using the UDP protocol. UDP Statistics is a single-instance attribute group.

Datagrams No Port/sec The rate of received UDP datagrams for which there was no application at the destination port. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Received Errors The number of received UDP Datagrams that could not be delivered for reasons other than the lack of an application at the destination port. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Received/sec The rate that UDP datagrams are delivered to UDP users. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams/sec The rate that UDP datagrams are sent or received by the entity. Valid values are positive integers in the range 0 to 2147483647 and can include the

use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Datagrams Sent/sec The rate that UDP datagrams are sent from the entity. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day
HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Web Service attributes

Use Web Service attributes to create situations to monitor traffic and connection activity for a web server. Web Service is a multiple-instance attribute group. You cannot mix these attributes with those of any other multiple-instance attribute group.

Anonymous Users/sec The rate users are making anonymous connections using the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Received/sec The rate that data bytes are received by the Web service. This attribute is the 64-bit version of Bytes_Received/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Received/sec (Superseded) The rate that data bytes are received by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can

include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Sent/sec The rate that data bytes are sent by the Web service. This attribute is the 64-bit version of Bytes_Sent/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Sent/sec (Superseded) The rate that data bytes are sent by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Bytes Total/sec The sum of Bytes Sent/sec and Bytes Received/sec. This is the total rate of bytes transferred by the Web service. This attribute is the 64-bit version of Bytes Total/sec. Note: the value 9223372036854775807 indicates Value_Exceeds_Maximum and the value -9223372036854775808 indicates Value_Exceeds_Minimum.

Bytes Total/sec (Superseded) The sum of Bytes Sent/sec and Bytes Received/sec. This is the total rate of bytes transferred by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

CGI Requests/sec The rate of CGI requests that are simultaneously being processed by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Connection Attempts/sec The rate that connections using the Web service are being attempted. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Anonymous Users The number of users who currently have an anonymous connection using the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Blocked Async I/O Requests Current requests temporarily blocked due to bandwidth throttling settings. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current CGI Requests Current number of CGI requests that are simultaneously being processed by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM

functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current Connections The current number of connections established with the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current ISAPI Extension Requests The current number of Extension requests that are simultaneously being processed by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Current NonAnonymous Users The number of users who currently have a non-anonymous connection using the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Delete Requests/sec The rate HTTP requests using the DELETE method are made. Delete requests are generally used for file removals. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Received/sec The rate files are received by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files Sent/sec The rate files are sent by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Files/sec The rate files are transferred, that is, sent and received by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Get Requests/sec The rate HTTP requests using the GET method are made. Get requests are generally used for basic file retrievals or image maps, though they can be used with forms. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Head Requests/sec The rate HTTP requests using the HEAD method are made. Head requests generally indicate a client is querying the state of a document they already have to see if it needs to be refreshed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

ISAPI Extension Requests/sec The rate of ISAPI Extension requests that are simultaneously being processed by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Logon Attempts/sec The rate that logons using the Web service are being attempted. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Maximum Anonymous Users The maximum number of users who established concurrent anonymous connections using the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Maximum CGI Requests Maximum number of CGI requests simultaneously processed by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Maximum Connections The maximum number of simultaneous connections established with the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Maximum ISAPI Extension Requests The maximum number of Extension requests simultaneously processed by the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Maximum NonAnonymous Users The maximum number of users who established concurrent non-anonymous connections using the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum.

Measured Async I/O Bandwidth Usage Measured bandwidth of asynchronous I/O averaged over a minute. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

NonAnonymous Users/sec The rate users are making non-anonymous connections using the Web service. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions.

Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Not Found Errors/sec The rate of errors due to requests that could not be satisfied by the server because the requested document could not be found. These are generally reported as an HTTP 404 error code to the client. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Other Request Methods/sec The rate HTTP requests are made that do not use the GET, POST, PUT, DELETE, TRACE or HEAD methods. These might include LINK or other methods supported by gateway applications. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Post Requests/sec The rate HTTP requests using the POST method are made. Post requests are generally used for forms or gateway requests. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Put Requests/sec The rate HTTP requests using the PUT method are made. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

System Code Resident Bytes System Code Resident Bytes. Note that this attribute is not available on systems running Windows 2000 with IIS 5.0). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: -1 indicates Unknown and 2147483647 indicates Value_Exceeds_Maximum. None of the supported versions of Windows Operating System return this value, so it will always be Unknown.

System Name The managed system name. The form should be *hostname:agent_code*.

Examples include spark:KNT or deux.raleigh.ibm.com:KNT.

In workspace queries, this attribute should be set equal to the value $NODE$ in order to populate the workspace with data. This attribute is generally not included in situations, unless there is a need to customize the situation for a specific managed system.

Timestamp The date and time the Tivoli Enterprise Monitoring Server samples the data. This information is displayed in the standard 16-character date/time format (CYYMMDDHHMMSSmmm), where:

C	Century (0 for 20th, 1 for 21st)
YY	Year
MM	Month
DD	Day

HH	Hour
MM	Minute
SS	Second
mmm	Millisecond

Use simple text strings as described above. For example, 1101009130500000 expresses October 9, 2010, 1:05:00 pm.

Total Allowed Async I/O Requests Total requests allowed by bandwidth throttling settings (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Anonymous Users The total number of users who established an anonymous connection with the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Blocked Async I/O Requests Total requests temporarily blocked due to bandwidth throttling settings (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total CGI Requests Custom gateway executables (exe) the administrator can install to add forms processing or other dynamic data sources. CGI requests spawn a process on the server which can be a large drain on server resources. The count is the total since service startup. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Connection Attempts The number of connections that have been attempted using the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Delete Requests Total Delete Requests is the number of HTTP requests using the DELETE method (counted since service startup). Delete requests are generally used for file removals. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Files Received The total number of files received by the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Files Sent The total number of files sent by the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Files Transferred The sum of Files Sent and Files Received. This is the total number of files transferred by the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Get Requests The number of HTTP requests using the GET method (counted since service startup). Get requests are generally used for basic file retrievals or image maps, though they can be used with forms. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Head Requests The number of HTTP requests using the HEAD method (counted since service startup). Head requests generally indicate a client is querying the state of a document they already have to see if it needs to be refreshed. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total ISAPI Extension Requests Custom gateway Dynamic Link Libraries (dll) the administrator can install to add forms processing or other dynamic data sources. Unlike CGI requests, ISAPI requests are simple calls to a DLL library routine, thus they are better suited to high performance gateway applications. The count is the total since service startup. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Logon Attempts The number of logons that have been attempted using the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Method Requests The number of HTTP GET, POST, PUT, DELETE, TRACE, HEAD and other method requests (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Method Requests/sec The rate HTTP requests using GET, POST, PUT, DELETE, TRACE or HEAD methods are made. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total NonAnonymous Users The total number of users who established a non-anonymous connection with the Web service (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Not Found Errors The number of requests that could not be satisfied by the server because the requested document could not be found. These are generally reported as an HTTP 404 error code to the client. The count is the total since service startup. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Other Request Methods The number of HTTP requests that are not GET, POST, PUT, DELETE, TRACE or HEAD methods (counted since service startup). These might include LINK or other methods supported by gateway applications. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Post Requests The number of HTTP requests using the POST method (counted since service startup). Post requests are generally used for forms or gateway requests. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Put Requests The number of HTTP requests using the PUT method (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Rejected Async I/O Requests Total requests rejected due to bandwidth throttling settings (counted since service startup). Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Total Trace Requests The number of HTTP requests using the TRACE method (counted since service startup). Trace requests allow the client to see what is being received at the end of the request chain and use the information for diagnostic purposes. Valid values are positive integers in the range 0 to 2147483647 and can include the use of the *AVG, *MIN, *MAX, or *SUM functions. Note: the value 2147483647 indicates Value_Exceeds_Maximum and the value -2147483648 indicates Value_Exceeds_Minimum.

Web Site Name of web site. Valid format is a text string of up to 64 characters.

Disk capacity planning for historical data

Disk capacity planning for a monitoring agent is a prediction of the amount of disk space to be consumed for each attribute group whose historical data is being collected. Required disk storage is an important factor to consider when you are defining data collection rules and your strategy for historical data collection.

Expected number of instances is a guideline that can be different for each attribute group, because it is the number of instances of data that the agent will return for a given attribute group, and depends on the application environment that is being monitored. For example, if your attribute group is monitoring each processor on your machine and you have a dual processor machine, the number of instances is 2.

Calculate expected disk space consumption by multiplying the number of bytes per instance by the expected number of instances, and then multiplying that product by the number of samples.Table 2 provides the following information required to calculate disk space for the Monitoring Agent for Windows OS:

- *Bytes per instance (agent)* is an estimate of the record length for each row or instance written to the agent disk for historical data collection. This estimate can be used for agent disk space planning purposes.
- *Database bytes per instance (warehouse)* is an estimate of the record length for detailed records written to the warehouse database, if the attribute group is configured to be written to the warehouse. Detailed records are those that have been uploaded from the agent for long-term historical data collection. This estimate can be used for warehouse disk space planning purposes.
- *Aggregate bytes per instance (warehouse)* is an estimate of the record length for aggregate records written to the warehouse database, if the attribute group is configured to be written to the warehouse. Aggregate records are created by the Summarization agent for attribute groups that have been configured for summarization. This estimate can be used for warehouse disk space planning purposes.

The IBM Tivoli Monitoring Installation and Setup Guide contains formulas that can be used to estimate the amount of disk space used at the agent and in the warehouse database for historical data collection of an attribute group.

Table 2. Capacity planning for historical data logged by component

Table	Attribute group	Bytes per instance (agent)	Database bytes per instance (warehouse)	Aggregate bytes per instance (warehouse)
ACTSRVPG	Active_Server_Pages	404	304	1358
DHCPSRV	DHCP_Server	300	174	757
DNSDYNUPD	DNS_Dynamic_Update	292	164	477
DNSMEMORY	DNS_Memory	268	134	405
DNSQUERY	DNS_Query	316	194	717
DNSWINS	DNS_WINS	276	144	397
DNSZONET	DNS_Zone_Transfer	316	194	501
FTPSTATS	FTP_Server_Statistics	308	184	560
FTPSVC	FTP_Service	244	249	625
GOPHRSVC	Gopher_Service	320	199	620

Table 2. Capacity planning for historical data logged by component (continued)

Table	Attribute group	Bytes per instance (agent)	Database bytes per instance (warehouse)	Aggregate bytes per instance (warehouse)
HTTPCNDX	HTTP_Content_Index	276	144	445
HTTPSRVC	HTTP_Service	356	244	842
ICMPSTAT	ICMP_Statistics	352	239	978
IISSTATS	IIS_Statistics	300	174	574
IPSTATS	IP_Statistics	316	194	741
INDEXSVC	Indexing_Service	616	621	1015
INDEXSVCF	Indexing_Service_Filter	584	581	735
JOBOBJ	Job_Object	672	685	1199
JOBOBJD	Job_Object_Details	700	726	1675
KNTPASSTAT	KCA_Agent_Active_Runtime_Status	1418	1444	1481
KNTPASMGMT	KCA_Agent_Availability_Management_Status	554	559	596
KNTPASALRT	KCA_Alerts_Table	512	516	553
KNTPASCAP	KCA_Configuration_Information	3026	3067	3104
MSMQIS	MSMQ_Information_Store	272	139	281
MSMQQUE	MSMQ_Queue	452	450	643
MSMQSVC	MSMQ_Service	280	149	489
MSMQSESS	MSMQ_Sessions	340	209	462
NNTPCMD	NNTP_Commands	356	389	1614
NNTPSRV	NNTP_Server	340	369	1321
NTBIOSINFO	NT_BIOS_Information	684	689	726
NTCACHE	NT_Cache	368	259	1505
NTCOMPINFO	NT_Computer_Information	1260	1276	1313
NTDEVDEP	NT_Device_Dependencies	696	692	729
NTDEVICE	NT_Devices	1176	1181	1218
NTEVTLOG	NT_Event_Log	3152	3170	3234
NTFLCHG	NT_FILE_CHANGE	1560	1588	1749
NTFLTREND	NT_FILE_TREND	1612	1645	2337
NTIPADDR	NT_IP_Address	642	647	684
NTJOBOBJD	NT_Job_Object_Details	720	753	1774
WTLOGCLDSK	NT_Logical_Disk	408	327	1192
WTMEMORY	NT_Memory	416	319	1790
NTMEMORY	NT_Memory_64	376	415	1966
NTLOGINFO	NT_Monitored_Logs_Report	1284	1300	1540
NTMNTPT	NT_Mount_Points	652	660	697
NTNETWRKIN	NT_Network_Interface	504	523	1293
NTNETWPORT	NT_Network_Port	800	813	850
WTOBJECTS	NT_Objects	268	134	405
NTPAGEFILE	NT_Paging_File	580	576	652

Table 2. Capacity planning for historical data logged by component (continued)

Table	Attribute group	Bytes per instance (agent)	Database bytes per instance (warehouse)	Aggregate bytes per instance (warehouse)
WTPHYSDSK	NT_Physical_Disk	312	364	1475
NTPRTJOB	NT_Print_Job	1464	1485	1522
NTPRINTER	NT_Printer	2452	2480	2681
WTPROCESS	NT_Process	1056	953	1722
NTPROCESS	NT_Process_64	988	1022	1882
NTPROCSSR	NT_Processor	220	219	646
NTPROCINFO	NT_Processor_Information	480	490	527
NTPROCRSUM	NT_Processor_Summary	368	384	1045
NTREDIRECT	NT_Redirector	504	425	2513
WTREGISTRY	NT_Registry	1644	1645	1682
WTSERVER	NT_Server	392	285	1171
WTSERVERQ	NT_Server_Work_Queues	248	254	930
NTSERVERQ	NT_Server_Work_Queues_64	276	290	1002
NTSVCDEP	NT_Service_Dependencies	708	704	741
NTSERVICE	NT_Services	1496	1507	1544
WTSYSTEM	NT_System	924	824	1788
WTTHREAD	NT_Thread	356	229	515
NETWRKIN	Network_Interface	504	516	1174
NETSEGMT	Network_Segment	208	204	514
PRINTQ	Print_Queue	604	617	1129
PROCESSIO	Process_IO	732	607	956
KNTRASPT	RAS_Port	248	254	714
KNTRASTOT	RAS_Total	316	194	669
SMTPSRV	SMTP_Server	396	439	2006
TCPSTATS	TCP_Statistics	280	149	441
UDPSTATS	UDP_Statistics	264	129	337
WEBSVC	Web_Service	420	466	2015

For more information about historical data collection, see the *IBM Tivoli Monitoring Administrator's Guide*.

Chapter 5. Situations reference

This chapter contains an overview of situations, references for detailed information about situations, and descriptions of the predefined situations included in this monitoring agent.

About situations

A situation is a logical expression involving one or more system conditions. Situations are used to monitor the condition of systems in your network. You can manage situations from the Tivoli Enterprise Portal by using the situation editor.

The IBM Tivoli Monitoring agents that you use to monitor your system environment are shipped with a set of predefined situations that you can use as-is or you can create new situations to meet your requirements. Predefined situations contain attributes that check for system conditions common to many enterprises.

Using predefined situations can improve the speed with which you can begin using Monitoring Agent for Windows OS. You can examine and, if necessary, change the conditions or values being monitored by a predefined situation to those best suited to your enterprise.

Note: The predefined situations provided with this monitoring agent are not read-only. Do not edit these situations and save over them. Software updates will write over any of the changes that you make to these situations. Instead, copy the situations that you want to change to suit your enterprise.

In some cases, the values assigned to the predefined situations are examples only and must be modified to reflect the conditions of your distributed system.

You can display predefined situations and create your own situations using the Situation editor. The left frame of the Situation editor initially lists the situations associated with the Navigator item that you selected. When you click a situation name or create a new situation, the right frame opens with the following tabs:

Formula
Condition being tested

Distribution
List of managed systems (operating systems, subsystems, or applications) to which the situation can be distributed.

Expert Advice
Comments and instructions to be read in the event workspace

Action
Command to be sent to the system

Until Duration of the situation

EIF Whether to send a Tivoli Enterprise Console event and event severity

IBM Tivoli Monitoring for Windows includes the following types of predefined situations:

Automatically installed and activated at startup
These situations are automatically installed, distributed, assigned to a managed object, and started.

Not automatically installed but activated at startup
These situations are not automatically installed, distributed, assigned to a managed object, but once they are installed, they are automatically started.

Automatically installed and not activated at startup
These situations are automatically installed when you install the Tivoli Enterprise Portal Server. However, they must be distributed, added to a managed object, and started.

Bottleneck analysis, not activated at startup
These situations are designed specifically to help you to isolate areas of your system that are contributing to bottleneck conditions. These situations are not activated at startup.

More information about situations

The *IBM Tivoli Monitoring User's Guide* contains more information about predefined and custom situations and how to use them to respond to alerts.

For a list of the predefined situations for this monitoring agent and a description of each situation, refer to the Predefined situations section below and the information in that section for each individual situation.

Predefined situations

This monitoring agent contains the following predefined situations, which are organized by the three groups that describe their installation and activation:

- Automatically installed and activated at startup
  - NT_AMS_Alert_Critical
  - NT_Invalid_Logon_Attempt
  - NT_Log_Space_Low
  - NT_Paging_File_Critical
  - NT_Paging_File_Warning
  - NT_Physical_Disk_Busy_Critical
  - NT_Physical_Disk_Busy_Warning
  - NT_Process_CPU_Critical
  - NT_Process_CPU_Critical_2
  - NT_Process_CPU_Warning
  - NT_Process_CPU_Warning_2
  - NT_Service_Error
  - NT_System_File_Critical
  - NT_System_File_Warning
- Automatically installed and not activated at startup
  - NT_Available_Bytes_Critical
  - NT_Available_Bytes_Critical_2
  - NT_Available_Bytes_Warning
  - NT_Available_Bytes_Warning_2
  - NT_Disk_Space_Low

  - NT_Logical_Disk_Space_Critical
  - NT_Logical_Disk_Space_Warning
  - NT_Missing_Msdtc_Warning
  - NT_Missing_Msdtc_Warning_2
  - NT_Missing_Process
  - NT_Missing_Process_2
  - NT_Number_Processes_Critical
  - NT_Number_Processes_Warning
  - NT_Process_Memory_Critical
  - NT_Process_Memory_Critical_2
  - NT_Process_Memory_Warning
  - NT_Process_Memory_Warning_2
  - NT_Processor_Interrupt_Critical
  - NT_Processor_Interrupts_Warning
  - NT_Services_Automatic_Start
  - NT_System_CPU_Critical
  - NT_System_CPU_Warning
- Not automatically installed, activated at startup
  - NT_BP_Evt_Source_Critical
  - NT_BP_MemAvailKB_Critical
  - NT_BP_ProcCpuPct_Warning
  - NT_BP_ProcMissing_Critical
  - NT_BP_TcpRetrans_Warning
- Bottleneck analysis, not activated at startup
  - NT_Bottleneck_Disk
  - NT_Bottleneck_Memory
  - NT_Bottleneck_Paging
  - NT_Bottleneck_Processor
  - NT_Context_Switches_Sec
  - NT_Context_Switches_Sec_Low
  - NT_Memory_Pages_Sec
  - NT_Memory_Pages_Sec_2
  - NT_Memory_Pages_Sec_Low
  - NT_Memory_Pages_Sec_Low_2
  - NT_Percent_Disk_Time
  - NT_Percent_Disk_Time_Low
  - NT_Percent_Processor_Time
  - NT_Percent_Processor_Time_Low
  - NT_Percent_Total_Proc_Time
  - NT_Percent_Total_Proc_Time_Low
  - NT_System_Proc_Q_Length
  - NT_System_Proc_Q_Length_Low
  - NT_System_Total_Interrupts
  - NT_System_Total_Interrupts_Low

The remaining sections of this chapter contain descriptions of each of these predefined situations. The situations are organized by the three groups that describe their installation and activation.

Predefined situations: activated at startup

Descriptions and formulas: automatically installed, distributed, and assigned

IBM Tivoli Monitoring: Windows OS Agent includes the Activated at startup predefined situations. These situations are automatically installed, distributed, assigned to a managed object, and started.

NT_AMS_Alert_Critical monitors to determine if one of the following conditions is true:

- A managed agent has exceeded its restart count for the day as configured in the 'maxRestarts' field of its Common Agent Package file.
- A managed agent is overutilizing the available CPU resources as configured in the 'cpuThreshold' field of its Common Agent Package file.
- A managed agent is overutilizing the available system memory resources as configured in the 'memoryThreshold' field of its Common Agent Package file.
- An attempt at auto-restarting a managed agent failed.
- An attempt at starting a stopped or manually stopped managed agent failed.
- The Agent Management Services watchdog is no longer reliable. If either watchdog stops monitoring, you will receive this message.

The formula for this situation is as follows:

```
Alert Message=='Agent exceeded restart count' OR
Alert Message=='Agent overutilizing CPU' OR
Alert Message=='Agent overutilizing memory'  OR
Alert Message=='Agent restart failed' OR
Alert Message=='Agent manual stop failed' OR
Alert Message =='Agent Management Services watchdog no longer reliable'
```

NT_Invalid_Logon_Attempt monitors for logon attempts with an invalid account or password.

NT_Event_Log.Event_ID EQ 529

NT_Log_Space_Low determines whether one of the NT Logs is close to capacity.

NT_Monitored_Logs_Report.%_Usage GE 95

NT_Paging_File_Critical monitors the percent of Page File in use.

NT_Paging_File.%_Usage GE 80 AND NT_Paging_File.Pagefile_Name_U NE _Total

NT_Paging_File_Warning monitors the percent of Page File in use.

NT_Paging_File.%_Usage GE 75 AND NT_Paging_File.%_Usage LT 80 AND NT_Paging_File.Pagefile_Name_U NE _Total

NT_Physical_Disk_Busy_Critical monitors the percent of time the disk drive is busy.

NT_Physical_Disk.%_Disk_Time GT 90 AND NT_Physical_Disk.Disk_Name NE _Total

NT_Physical_Disk_Busy_Warning monitors the percent of time the disk drive is busy.

NT_Physical_Disk.%_Disk_Time GT 80 AND NT_Physical_Disk.%_Disk_Time LE 90 AND NT_Physical_Disk.Disk_Name NE _Total

NT_Process_CPU_Critical superseded by NT_Process_CPU_Critical_2. Monitors the percent of processor time used by a specific process.

NT_Process.%_Processor_Time GE 65 AND NT_Process.Priority_Base NE 0 AND NT_Process.Process_Name NE _Total

NT_Process_CPU_Critical_2 monitors the percent of processor time used by a specific process.

NT_Process_64.%_Processor_Time GE 65 AND NT_Process_64.Priority_Base NE 0 AND NT_Process_64.Process_Name NE _Total

NT_Process_CPU_Warning superseded by NT_Process_CPU_Warning_2. Monitors the percent of processor time used by a specific process.

NT_Process.%_Processor_Time GE 50 AND NT_Process.%_Processor_Time LT 65 AND NT_Process.Priority_Base NE 0 AND NT_Process.Process_Name NE _Total

NT_Process_CPU_Warning_2 monitors the percent of processor time used by a specific process.

NT_Process_64.%_Processor_Time GE 50 AND NT_Process_64.%_Processor_Time LT 65 AND NT_Process_64.Priority_Base NE 0 AND NT_Process_64.Process_Name NE _Total

NT_Service_Error monitors the reporting of a service error.

NT_Event_Log.Source EQ 'Service Control Manager' AND NT_Event_Log.Type EQ Error

NT_System_File_Critical monitors the rate of operations to file system devices per second.

NT_System.File_Data_Operations/Sec GE 100000

NT_System_File_Warning monitors the rate of operations to file system devices per second.

NT_System.File_Data_Operations/Sec GE 10000 AND NT_System.File_Data_Operations/Sec LT 100000

Descriptions and formulas: not automatically distributed or assigned

IBM Tivoli Monitoring: Windows OS Agent includes at start up (installs) the Best Practice predefined situations. These situations are not automatically distributed or

assigned to a managed object. You must distribute the following situations to the managed system or managed system list that you want to monitor.

NT_BP_Evt_Source_Critical monitors the windows event log for specific Event IDs.

*IF ((*VALUE NT_Event_Log.Source_U *EQ 'Rdr' *AND *VALUE NT_Event_ Log.Event_ID *EQ 3013) *OR (*VALUE NT_Event_Log.Source_U *EQ 'Srv' *AN D *VALUE NT_Event_Log.Event_ID *EQ 2011) *OR (*VALUE NT_Event_Log.Sour ce_U *EQ 'disk' *AND *VALUE NT_Event_Log.Event_ID *EQ 11) *OR (*VALUE NT_Event_Log.Source_U *EQ 'Netlogon' *AND *VALUE NT_Event_Log.Event_ID * EQ 5719))

NT_BP_MemAvailKB_Critical monitors available virtual memory kilobytes.

*IF *VALUE NT_Memory_64.Available_kBytes *LT 10000

NT_BP_ProcCpuPct_Warning monitors the CPU percent utilization by all processes except Antivirus, TSM and Idle.

*IF *VALUE NT_Process_64.%_Processor_Time *GE 95 *AND *VALUE NT_Proc ess_64.Process_Name *NE '_Total' *AND *VALUE NT_Process_64.Process_Name *NE Idle *AND *VALUE NT_Process_64.Process_Name *NE Rtvscan *AND *VALUE NT_Process_64.Process_Name *NE dsmcsvc"

NT_BP_ProcMissing_Critical monitors standard processes on a windows 2000 system.

*IF *MISSING NT_Process_64.Process_Name *EQ ('lsass','services','svc host')

NT_BP_TcpRetrans_Warning monitors the rate of segments transmitted containing previously transmitted bytes. This monitor can assist in identifying a failing NIC.

*IF *VALUE TCP_Statistics.Segments_Retransmitted/sec *GT 1

Predefined situations: not activated at startup

IBM Tivoli Monitoring: Windows OS Agent includes the predefined situations that are automatically installed, but not activated at startup. They must be distributed, added to a managed object, and started.

Descriptions and formulas

NT_Available_Bytes_Critical superseded by NT_Available_Bytes_Critical_2. Monitors virtual memory on the Zeroed, Free, and Standby lists.

NT_Memory.Available_Bytes LT 524888 AND NT_Memory.Available_Bytes GT 0

NT_Available_Bytes_Critical_2 monitors virtual memory on the Zeroed, Free, and Standby lists.

NT_Memory_64.Available_Bytes LT 524888 AND NT_Memory_64.Available_Bytes GT 0

NT_Available_Bytes_Warning superseded by NT_Available_Bytes_Warning_2. Monitors virtual memory on the Zeroed, Free, and Standby lists.

NT_Memory.Available_Bytes GE 524888 AND NT_Memory.Available_Bytes LT 1048576

NT_Available_Bytes_Warning_2 monitors virtual memory on the Zeroed, Free, and Standby lists.

NT_Memory_64.Available_Bytes GE 524888 AND NT_Memory_64.Available_Bytes LT 1048576

NT_Disk_Space_Low monitors free space on a logical disk drive.

NT_Logical_Disk.Free_Megabytes LT 5 AND NT_Logical_Disk.Disk_Name NE _Total

NT_Logical_Disk_Space_Critical monitors percentage free space on a logical disk drive.

NT_Logical_Disk.%_Free LT 5 AND NT_Logical_Disk.Disk_Name NE _Total

NT_Logical_Disk_Space_Warning monitors percentage free space on a logical disk drive.

NT_Logical_Disk.%_Free LT 10 AND NT_Logical_Disk.%_Free GE 5 AND NT_Logical_Disk.Disk_Name NE _Total

NT_Missing_Msdtc_Warning superseded by NT_Missing_Msdtc_Warning_2. Determines whether Microsoft Distributed Coordinator is running.

MISSING NT_Process.Process_Name EQ (MSDTC)

NT_Missing_Msdtc_Warning_2 determines whether Microsoft Distributed Coordinator is running.

MISSING NT_Process_64.Process_Name EQ (MSDTC)

NT_Missing_Process superseded by NT_Missing_Process_2. Determines whether the NT Scheduler process is running.

MISSING NT_Process.Process_Name EQ ('schedule')

NT_Missing_Process_2 determines whether the NT Scheduler process is running.

MISSING NT_Process_64.Process_Name EQ ('schedule')

NT_Number_Processes_Critical determines the number of processes present.

NT_Objects.Processes GE 300

NT_Number_Processes_Warning determines the number of processes present.

NT_Objects.Processes GE 200 AND NT_Objects.Processes LT 300

NT_Process_Memory_Critical superseded by NT_Process_Memory_Critical_2. Determines the working set size for a specific process.

NT_Process.Process_Name NE _Total AND VALUE NT_Process.Working_Set GT 40000000

NT_Process_Memory_Critical_2 determines the working set size for a specific process.

NT_Process_64.Process_Name NE _Total AND VALUE NT_Process_64.Working_Set GT 40000000

NT_Process_Memory_Warning superseded by NT_Process_Memory_Warning_2. Determines the working set size for a specific process.

NT_Process.Process_Name NE _Total AND NT_Process.Working_Set GE 32000000 AND NT_Process.Working_Set LT 40000000

NT_Process_Memory_Warning_2 determines the working set size for a specific process.

NT_Process_64.Process_Name NE _Total AND NT_Process_64.Working_Set GE 32000000 AND NT_Process_64.Working_Set LT 40000000

NT_Processor_Interrupt_Critical monitors the number of device interrupts per second. This situation replaces the NT_Processor_Interrupts_Critical situation. The replaced situation no longer starts, but it has not been deleted in case you have customized it. If you have done so, look for your customizations and put them in this new situation. Then, delete the replaced situation.

NT_Processor.Interrupts/sec GE 3000 AND NT_Processor.Processor NE _Total

NT_Processor_Interrupts_Warning monitors the number of device interrupts per second.

NT_Processor.Interrupts/sec GE 2000 AND NT_Processor.Interrupts/sec LT 3000 AND NT_Processor.Processor NE _Total

NT_Services_Automatic_Start starts any non-running Automatic Start services.

NT_Services.Start_Type EQ Automatic AND NT_Services.Current_State EQ Stopped ACTION net start &NT_Services.Service_Name

NT_System_CPU_Critical monitors the % time that all processors are busy.

NT_System.Operating_System_Version EQ 4.0 AND NT_System. %_Total_Processor_Time GE 90 **OR** NT_System.Operating_System_Version GE 5.0 AND NT_Processor.%_Processor_Time GE 90 AND NT_Processor.Processor EQ _Total

NT_System_CPU_Warning monitors the % time that all processors are busy.

NT_System.Operating_System_Version EQ 4.0 AND NT_System. %_Total_Processor_Time GE 80 AND NT_System.%_Total_Processor_Time *LT 90 **OR** NT_System.Operating_System_Version GE 5.0 AND NT_Processor. %_Processor_Time GE 80 AND NT_Processor.%_Processor_Time LT 90 AND NT_Processor.Processor EQ _Total

Predefined situations: bottleneck analysis

IBM Tivoli Monitoring: Windows OS Agent includes the bottleneck analysis predefined situations. These situations are designed specifically to help you to isolate areas of your system that are contributing to bottleneck conditions.

Descriptions and formulas

NT_Bottleneck_Disk monitors for potential system slowdowns due to disk activity

NT_Percent_Disk_Time EQ TRUE AND NT_Percent_Processor_Time_Low EQ TRUE AND NT_Percent_Total_Proc_Time_Low EQ TRUE AND NT_Memory_Pages_Sec_Low EQ TRUE

NT_Bottleneck_Memory monitors for potential system slowdowns due to insufficient available memory.

NT_Memory_Pages_Sec EQ TRUE AND NT_Percent_Processor_Time EQ TRUE

NT_Bottleneck_Paging monitors for potential system slowdowns due to paging activity.

NT_Percent_Disk_Time EQ TRUE AND NT_Memory_Pages_Sec EQ TRUE AND NT_Percent_Processor_Time_Low EQ TRUE

NT_Bottleneck_Processor monitors for potential system slowdowns due to high processor utilization.

NT_Percent_Processor_Time EQ TRUE AND NT_Memory_Pages_Sec_Low EQ TRUE AND NT_Percent_Disk_Time_Low EQ TRUE

NT_Context_Switches_Sec monitors for indications of multitasking level.

NT_System.Context_Switches/Sec GT 100

NT_Context_Switches_Sec_Low monitors context switches/sec low settings (for bottleneck analysis.)

NT_System.Context_Switches/Sec LE 5

NT_Memory_Pages_Sec superseded by NT_Memory_Pages_Sec_2. Monitors for indications of high memory demand.

NT_Memory.Pages/sec GT 100

NT_Memory_Pages_Sec_2 monitors for indications of high memory demand.

NT_Memory_64.Pages/sec GT 100

NT_Memory_Pages_Sec_Low superseded by NT_Memory_Pages_Sec_Low_2. Monitors Memory Pages/sec low setting (for bottleneck analysis).

NT_Memory.Pages/sec LE 1

NT_Memory_Pages_Sec_Low_2 monitors Memory Pages/sec low setting (for bottleneck analysis).

NT_Memory_64.Pages/sec LE 1

NT_Percent_Disk_Time monitors for indications of high disk activity.

NT_Physical_Disk.%_Disk_Time GE 65 AND NT_Physical_Disk.Disk_Name NE _Total

NT_Percent_Disk_Time_Low monitors % disk time low setting (for bottleneck analysis.)

NT_Physical_Disk.%_Disk_Time LE 15 AND NT_Physical_Disk.Disk_Name NE _Total

NT_Percent_Processor_Time monitors for indications of high processor activity.

NT_Processor.%_Processor_Time GE 70 AND NT_Processor.Processor NE _Total

NT_Percent_Processor_Time_Low monitors for % processor time low setting (for bottleneck analysis.)

NT_Processor.%_Processor_Time LE 10 AND NT_Processor.Processor NE _Total

NT_Percent_Total_Proc_Time monitors for indications of high activity on all processors.

NT_System.Operating_System_Version EQ 4.0 AND NT_System. %_Total_Processor_Time GT 70 **OR** NT_System.Operating_System_Version GE 5.0 AND NT_Processor.%_Processor_Time GT 70 AND NT_Processor.Processor EQ _Total

NT_Percent_Total_Proc_Time_Low monitors for % total processor time low setting (for bottleneck analysis.)

NT_System.Operating_System_Version GE 5.0 AND NT_Processor. %_Processor_Time LE 10 AND NT_Processor.Processor EQ _Total**OR** NT_System.Operating_System_Version EQ 4.0 AND NT_System. %_Total_Processor_Time LE 10 AND NT_System.%_Total_Processor_Time GT 0

NT_System_Proc_Q_Length monitors for indications of processor congestion.

NT_System.Processor_Queue_Length GT 25

NT_System_Proc_Q_Length_Low monitors system proc queue length low settings (for bottleneck analysis).

NT_System.Processor_Queue_Length LE 1

NT_System_Total_Interrupts monitors I/O device activity.

NT_System.Operating_System_Version EQ 4.0 AND NT_System.Total_Interrupts/ Sec GT 100 **OR**NT_System.Operating_System_Version GE 5.0 AND NT_Processor.Interrupts/sec GT 100 AND NT_Processor.Processor EQ _Total

NT_System_Total_Interrupts_Low monitors system total interrupts low setting (for bottleneck analysis.)

NT_System.Operating_System_Version EQ 4.0 AND NT_System.Total_Interrupts/
Sec LE 5 **OR** NT_System.Operating_System_Version GE 5.0 AND
NT_Processor.Interrupts/sec LE 5 AND NT_Processor.Processor EQ _Total

Chapter 6. Take Action commands reference

This chapter contains an overview of Take Action commands, references for detailed information about Take Action commands, and descriptions of the Take Action commands included in this monitoring agent.

About Take Action commands

Take Action commands can be run from the desktop or included in a situation or a policy.

When included in a situation, the command executes when the situation becomes true. A Take Action command in a situation is also referred to as a reflex automation. When you enable a Take Action command in a situation, you automate a response to system conditions. For example, you can use a Take Action command to send a command to restart a process on the managed system or to send a text message to a cell phone.

More information about Take Action commands

For more information about working with Take Action commands, see the *IBM Tivoli Monitoring User's Guide*.

For a list of the Take Action commands for this monitoring agent and a description of each command, refer to the Predefined Take Action commands section below and the information in that section for each individual command.

Predefined Take Action commands

This monitoring agent contains the following Take Action commands:

- AMS Recycle Agent Instance
- AMS Reset Agent Daily Restart Count
- AMS Start Agent
- AMS Start Agent Instance
- AMS Stop Agent
- AMS Start Management
- AMS Stop Management
- Start Services
- Stop Services

The remaining sections of this chapter contain descriptions of each of these Take Action commands, which are listed alphabetically.

The following information is provided about each Take Action command:

Description
Which actions the command performs on the system to which is it sent

Arguments
List of arguments, if any, for the Take Action with a short description and default value for each one

Destination systems
Where the command is to be executed: on the Managed System (monitoring agent) where the agent resides or on the Managing System (Tivoli Enterprise Monitoring Server) to which it is connected

Usage Notes
Additional notes relevant to using the task

AMS Recycle Agent Instance

Description
Use this action to stop and start any agent with a single request. This recycle does not increase the restart count of an agent.

GUI data entry fields

Agent Name
The name of the agent as it is displayed in the Agents' Runtime Status View's Agent Name column.

Process Name
The name of the agent's process as it is displayed in the Agents' Runtime Status View's Process Name column.

Instance Name
If it exists, the name of an agent instance as it is displayed in the Agents' Runtime Status View's Instance Name column.

Process ID
The process ID of the agent process as it is displayed in the Agents' Runtime Status View's Process ID column.

Restrictions
Managed system

Usage notes
Not available to previous versions of the OS agents. To use this action against the OS agent, the Agent Management Services watchdog must be running.

AMS Reset Agent Daily Restart Count

Description
Use this action to reset the daily restart count of an agent to 0.

GUI data entry fields

Agent Name
The name of the agent as it is displayed in the Agents' Runtime Status View's Agent Name column.

Process Name
The name of the agent's process as it is displayed in the Agents' Runtime Status View's Process Name column.

Instance Name
If it exists, the name of an agent instance as it is displayed in the Agents' Runtime Status View's Instance Name column.

Restrictions
Managed system

Usage notes

Not available to agents that are not at the latest level. To use this action against the OS agent, the Agent Management Services watchdog must be running.

AMS Start Agent action

Description

Use this action to start an agent that is under the management of Agent Management Services. The action includes an optional input field for resetting the Daily Restart Count back to 0. This action is helpful when an agent has exceeded its maxRestartCount for the day.

GUI data entry fields

Agent Name
The name of the agent as it is displayed in the Agents' Runtime Status View's Agent Name column.

Daily Restart Count
Value indicating whether to reset the daily restart count. The value 1 indicates True, and the value 0 (default) indicates False.

Process Name
The name of the process representing the agent instance as it is displayed in the Agents' Runtime Status View's Process Name column.

Restrictions

Managed system

Usage notes

You cannot target the Monitoring Agent for Windows OS with this action. Only the other agents being managed by Agent Management Services running on the Monitoring Agent for Windows OS can be targeted with this action.

AMS Start Agent Instance action

Description

Use this action to start a monitoring agent instance of type ITM Windows or ITM UNIX that is under the management of Agent Management Services. The action includes an optional input field for resetting the Daily Restart Count back to 0. This action is helpful when an agent instance has exceeded its maxRestartCount for the day.

GUI data entry fields

Agent Name
The name of the agent as it is displayed in the Agents' Runtime Status View's Agent Name column.

Daily Restart Count
Value indicating whether to reset the daily restart count. The value 1 indicates True, and the value 0 (default) indicates False.

Process Name
The name of the process representing the agent instance as it is displayed in the Agents' Runtime Status View's Process Name column.

Instance Name
The name of the monitoring agent instance as it is displayed in the Agents' Runtime Status View's Instance Name column.

Restrictions
Managed system

Usage notes
You cannot target the Monitoring Agent for Windows OS with this action. Only the other agents being managed by Agent Management Services running on the Monitoring Agent for Windows OS can be targeted with this action.

AMS Stop Agent action

Description
Use this action to stop an agent that is under the management of Agent Management Services. The action will put a running instance of an agent in to the 'Manually Stopped' state, meaning that Agent Management Services will not perform any auto-restarts. To prompt Agent Management Services to commence auto-restarting, use the AMS Start Agent command or AMS Start Agent Instance command to manually put the agent back in to a Running state.

GUI data entry fields

Process ID
By default, this argument is populated with the Process ID of the particular agent instance selected from the Tivoli Enterprise Portal. To stop all instances of an agent, such as by using the tacmd executeaction AMS Stop Agent command, leave this argument blank.

Restrictions
Managed system

Usage notes
You cannot target the Monitoring Agent for Windows OS with this action. Only the other agents being managed by Agent Management Services running on the Monitoring Agent for Windows OS can be targeted with this action.

AMS Start Management action

Description
Use this action to put an agent under the management of Agent Management Services. This management provides the auto-restart capability.

Restrictions
Managed system

Usage notes
You now can target the Monitoring Agent for Windows OS with this command. Starting management of the OS Agent restarts the physical watchdog and rearms Agent Management Services. Watch of managed agents resumes. There is no change to non-OS agent management operations.

AMS Stop Management action

Description
Use this action to remove an agent from management by Agent Management Services. The action will cause Agent Management Services watchdog to stop performing health checks and auto restarts.

Restrictions
Managed system

Usage notes
You now can target the Monitoring Agent for Windows OS with this command. However, stopping management stops the physical watchdog and disarms Agent Management Services, which also stops watching and restarting of any managed agents. While the OS Agent is unmanaged, the Start Management action will not be allowed against any other non-OS agent. The NT_AMS_Alert_Critical situation is activated if this take action is run on the OS agent.

Start Services action

Description
Starts a non-running service on a managed system

GUI data entry fields
Service Name
Name of the service that is being started. When the Start Services Take Action is applied to a situation that monitors data from the NT_Services attribute group, the value of the NT_Services.Service_Name attribute is applied to the Take Action.

Restrictions
Managed system

Usage notes
Not applicable

Stop Services action

Description
Stops a running service on a managed system

GUI data entry fields
Service Name
Name of the service that is being stopped. When the Stop Services Take Action is applied to a situation that monitors data from the NT_Services attribute group, the value of the NT_Services.Service_Name attribute is applied to the Take Action.

Restrictions
Managed system

Usage notes
Not applicable

Need a list of return codes???

Chapter 7. Policies reference

This chapter contains an overview of policies, references for detailed information about policies, and descriptions of the predefined policies included in this monitoring agent.

About policies

Policies are an advanced automation technique for implementing more complex workflow strategies than you can create through simple automation.

A *policy* is a set of automated system processes that can perform actions, schedule work for users, or automate manual tasks. You use the Workflow Editor to design policies. You control the order in which the policy executes a series of automated steps, which are also called activities. Policies are connected to create a workflow. After an activity is completed, Tivoli Enterprise Portal receives return code feedback and advanced automation logic responds with subsequent activities prescribed by the feedback.

Note: The predefined policies provided with this monitoring agent are not read-only. Do not edit these policies and save over them. Software updates will write over any of the changes that you make to these policies. Instead, clone the policies that you want to change to suit your enterprise.

More information about policies

For more information about working with policies, see the *IBM Tivoli Monitoring User's Guide*.

For information about using the Workflow Editor, see the *IBM Tivoli Monitoring Administrator's Guide* or the Tivoli Enterprise Portal online help.

For a list of the policies for this monitoring agent and a description of each policy, refer to the Predefined policies section below and the information in that section for each individual policy.

Predefined policies

The remaining sections of this chapter contain descriptions of these policies, which are listed alphabetically.

NT Disk Busy

Detects excessive disk activity. This policy schedules specific actions to occur during off-peak hours if a physical disk is too busy. The policy performs the following steps:

1. Wait until situation, NT_Percent_Disk_Time, is true.
2. When true, evaluate situation, NT_MissingProcess. This checks to see if the Scheduler service is running.
3. If NT_MissingProcess evaluates to false, skip to step 5.
4. Issue the following Take Action command, "net start scheduler", to start the Scheduler process.

5. Issue the following Take Action command, "at 1:00 `c:\move.bat`", to perform some specific action at 1:00 AM.

   Note: The `c:\move.bat` is a placeholder script for any set of commands that you want to run in response to this condition. You must supply the move.bat script.

NT Disk Full

Detects disk free space less than 5% or 5 MB. This policy detects when available space on a logical disk becomes critical and requests manual intervention by prompting the user to chose a corrective action from a list of options. The policy performs the following steps:

1. Wait until situation, NT_Logical_Disk_Space_Critical, is true.
2. When true, evaluate situation, NT_Disk_Space_Low. This checks whether the logical drive has less than 5MB of space available.
3. If NT_Disk_Space_Low evaluates to true, display a message to every workgroup indicating that the drive has less than 5MB of space available. Prompt administrator to run a corrective action from a list of options.

   Note: The two options supplied in this policy are placeholders for customer provided corrective actions.
4. If NT_Disk_Space_Low evaluates to false, display a message to every workgroup indicating that drive space is critical. Prompt administrator to run a corrective action from a list of options.

   Note: The two options supplied in this policy are placeholders for customer provided corrective actions.
5. Perform the selected corrective action.

NT Log Management

Detects Windows logs at 95% or greater utilization. This policy detects when the amount of space used by Windows Event Logs becomes too high and requests manual intervention by prompting the user to chose a corrective action from a list of options. The policy performs the following steps:

1. Wait until situation, NT_Log_Space_Low, is true.
2. When true, display a message to every workgroup indicating that the log usage is at 95%. Prompt the administrator to run a corrective action from a list of options.

   Note: The two options supplied in this policy are placeholders for customer provided corrective actions.
   - Run a Take Action command to send a message to the network administrator.
   - Run a program/command to clear the log and then send a message to the network administrator informing them of the action.

Process CPU

Detects processes running with high CPU utilization. This policy detects when the amount of CPU used by a specific process becomes too high and requests manual intervention by prompting the user to chose a corrective action from a list of options. The policy performs the following steps:

1. Wait until situation, NT_Process_CPU_Critical, is true.

2. Display a message to every workgroup indicating that a process is using an excessive amount of CPU. Prompt the administrator to run a corrective action from a list of options.

   Note: The three options supplied in this policy are placeholders for customer provided corrective actions.

   - Run a Take Action command to send a message to the network administrator.
   - Run a Take Action command to send an email to the network administrator.
   - Run a Take Action command to stop the process.

Process Memory

Detects Windows processes with a high working set size. This policy detects when the amount of memory used by a specific process becomes too high and requests manual intervention by prompting the user to chose a corrective action from a list of options. The policy performs the following steps:

1. Wait until situation, NT_Process_Memory_Critical, is true.
2. When true evaluate situation, NT_Memory_Pages_Sec. If not true then this task is done.
3. If NT_Memory_Pages_Sec is true run a Take Action command to send a message to the network administrator informing them that the process' memory usage is excessive.
4. Display a message to every workgroup indicating that the situation had triggered action by this policy. Prompt the administrator to run a corrective action from a list of options.

   Note: The two options supplied in this policy are placeholders for customer provided corrective actions.

   - Run a Take Action command to send a message to the network administrator.
   - Run a Take Action command to stop the process.

Chapter 8. Tivoli Common Reporting for the monitoring agent

This chapter contains a description of the data model for the Monitoring Agents for Windows OS, Linux OS, and UNIX OS reports and descriptions of these reports.

See the following additional information about using reports with this monitoring agent:

- The "Tivoli Common Reporting" chapter in the *IBM Tivoli Monitoring Administrator's Guide, V6.2.3* or later contains information about prerequisites and importing and running the reports.
- To enable Tivoli Common Reporting for monitoring agents, use the Report Installer. When requested by the Report Installer, choose the "IBM Tivoli Monitoring OS Agents Reports" package.

Complete documentation for the Tivoli Common Reporting tool is located at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/topic/com.ibm.tivoli.tcr_cog.doc/tcr_welcome.html

You must have the following prerequisite actions completed to use this function:

- IBM Tivoli Monitoring v6.2.3 must be installed with the OS agents up and running.
- The Summarization and Pruning agent must be started with or without shifts enabled.
- Historical collection must be turned on and collection started.
- Summarized tables and views must be created and populated in the Tivoli Data Warehouse.

The data model for the Monitoring Agents for Windows OS, Linux OS, and UNIX OS reports will have the following features:

- The model covers data from OS Agents only.
- The model contains a subset of the attribute groups collected by OS Agents in aggregated form for time dimension: AVG, MIN, MAX, SUM, LAT, TOT, HI, LOW. See Table 3 on page 323 for the list of included tables.
- The model includes a Managed System dimension with the Agent Type attribute (on Windows, Linux, and UNIX systems). It is placed in the IBM Tivoli Monitoring Shared Dimensions namespace.
- The model includes all the aggregations handled by Summarization and Pruning from daily to yearly including the raw data.
- The model contains forecasting based on the linear trend for the following metrics for each time dimension:

  For Linux:

  – KLZ_CPU_FCAST_XX.AVG_Idle_CPU
  – KLZ_Disk_FCAST_XX.AVG_Disk_Used_Percent
  – KLZ_VM_Stats_FCAST_XX.AVG_Used_Virtual_Storage_Pct
  – KLZ_Network_FCAST_XX.AVG_Bytes_Transmitted_per_sec
  – KLZ_Network_FCAST_XX.AVG_Bytes_Received_per_sec

  For UNIX:

  - System_FCAST_XX.AVG_Idle_CPU
  - Disk_FCAST_XX.AVG_Space_Used_Percent
  - Unix_Memory_FCAST_XX.AVG_Virtual_Storage_Pct_Used
  - Network_FCAST_XX.AVG_Transmitted_MB_Total
  - Network_FCAST_XX.AVG_Received_MB_Total

  For Windows:
  - NT_System_FCAST_XX.AVG_%_Total_Processor_Time
  - NT_Logical_Disk_FCAST_XX.AVG_%_Used
  - NT_Memory_64_FCAST_XX.AVG_Available_Usage_Percentage
  - NT_Server_FCAST_XX.AVG_Bytes_Transmitted/sec
  - NT_Server_FCAST_XX.AVG_Bytes_Received/sec
- The metrics are organized in the following way:
  - Key Metrics
    - Performance
    - Availability
  - Extended metrics
- The metric's data items names reflect the catalog attributes names with the following suffixes:
  - SUM_ into (Sum)
  - LAT_ into (Latest)
  - MIN_ into (Minimum)
  - MAX_ into (Maximum)
  - TOT_ into (Total)
  - AVG_ into (Average)
  - HI_ into (Higher)
  - LOW_ into (Lower)
- Support for raw data is provided.
- The Summarization and Pruning configuration is shown in a specific query subject (Summarization and Pruning Configuration). The result is one row that represents the most recent entry in the KSY_SUMMARIZATION_CONFIG_DV view. The query subject contains the following query items:
  - Shift Enabled. The value is 1 if the shifts hours were specified, otherwise, the value is 0.
  - Vacations Enabled. The value is 1 if the vacations days were specified, otherwise, the value is 0.
  - Peak Hours per Day. The value contains the number of peak hours specified in the shifts hours settings.
- An availability daily data query subject for each agent type is provided. Metrics are computed using the following specific availability attributes: KLZ_System_Statistics.TOT_System_Uptime, System_DV.TOT_Up_Time, NT_System.TOT_System_Up_Time_64. The calculated query items have the following meaning:
  - % Up Time. The percentage the system is available in the day.
  - % Down Time. The percentage the system is not available in the day.
  - Up Days. The portion of the day the system is available.
  - Down Days. The portion of the day the system is not available.
  - MTBSI. Mean Time Before System Interruption (in hours).

– MTTR. Mean Time To Recovery (in hours).

The following paragraphs describe the reports. In particular, they contain the required views for each one. If these views are not present, the report might not work. To ensure that the required views are present, run the following query against the Tivoli Data Warehouse:

```
DB2: select distinct "VIEWNAME" from SYSCAT.VIEWS where
"VIEWNAME" like '%V'
Oracle: select distinct "VIEW_NAME" from USER_VIEWS where
"VIEW_NAME" like '%V'
MS SQL Server: select distinct "NAME" from SYS.VIEWS where
"NAME" like '%V'
```

The following databases are supported: DB2, Oracle, and SQL Server.

The following reports are available:

- Utilization Details for Single Resource

  This report shows CPU, memory, disk, network utilization and top 10 CPU utilizing processes for a system during the selected time period in a line chart. Statistical process information is shown in all line charts (including average, upper and lower control limits). A linear trending feature is also provided and it is based on the selected forecast period.
- Utilization Details for Multiple Resources

  This report shows CPU, memory, disk and network utilization for multiple systems during the selected time period in an overlaid line chart. A linear trending feature is also provided, and it is based on the selected forecast period.
- Utilization Comparison for Single Resource

  This report shows the comparison between CPU, disk and memory utilization for a particular server, over a period of time, in an overlaid line chart.
- Utilization Comparison for Multiple Resource

  This report shows the comparison between CPU, disk and memory utilization for the selected servers over a period of time.
- Utilization Heat Chart for Single Resource

  This report helps identify patterns of utilization of a particular system over a period of time. The first column shows dates during the selected time period and the other columns represent hours during the day. The chart can be used for showing a heat chart for CPU, Memory and Disk or all three in the same report. The dates have hyperlinks that you can use to drill down to Utilization Details for Single Resource. A linear trending feature is also provided, which is based on the selected forecast period.
- Memory Utilization for Single Resource

  This report shows memory usage details for a specific system. It uses a line chart to show the percentage of virtual, physical and swap memory usage. It also provides finer memory metrics in a table.
- Memory Utilization for Multiple Resources Comparison

  This report shows memory usage details for multiple systems over a period of time. It uses three overlaid line charts for virtual, physical and swap memory.
- Top Resources Utilization

  This report shows top resources by CPU, Disk and Memory utilization. The stacked bars show average CPU used and free (in percent) for each system over the selected report period. If the number of systems is less than 20, then a bar is shown in each row. For example, there are 20 rows in the table with charts for each system. If the number of systems is more than 20, then there is a bar chart

on top with the top 20 systems, and the rest of the data is in the table. This is done to eliminate overcrowding of the bars in the chart.

- Top Situations by Status

  This report shows the top 10 situations sorted by the selected status in a bar chart, along with finer details on all the top situations, listed in a table.
- Enterprise Daily Utilization Heat Chart

  This report shows CPU, disk and memory patterns for all servers, for a select operating system type, and on a particular date. The first column lists the server names. The rest of the columns show utilization data during the day hours and the last column shows the average for the server on the selected date. You can choose to see either CPU, disk, memory or all metrics.
- Enterprise Resources List

  This report lists all the Windows, Linux and UNIX resources in the environment. By clicking on a resource name, you can drill through to see the utilization details for that resource over the last 30 days.
- Enterprise Summary

  This report shows the overall availability and utilization of all Windows, Linux and UNIX monitoring agents.
- Top Resources by Availability

  This report displays availability of the top N systems based on System Uptime over a period of time.
- Top Resources Utilization Summary Heat Chart

  This report shows top resources by CPU, Disk or Memory utilization in a summary heat chart.
- Resource Availability Comparison

  This report shows availability comparison between two or more servers.
- Top Resources by Availability (MTTR/MTBSI)

  This report displays availability trending of the top N systems based on the Mean Time Before System Interruption (MTBSI) and Mean Time To Recovery (MTTR).
- Availability Heat Chart for Single Resource

  This report helps identify patterns of resource availability over a period of time.
- CPU Utilization Comparison for Multiple Resources

  This report shows CPU usage details for multiple systems.
- CPU Utilization for Single Resource

  This report shows CPU usage details for a specific system.
- Disk Utilization for Single Resource

  This report shows the percentage of space usage for the logical disks of a particular server, over a period of time, in an overlaid line chart, along with a table that shows finer details on logical disks usage.
- Disk Utilization Comparison for Multiple Resources

  This report shows disk usage details for multiple systems, over a period of time, in two overlaid line charts.
- Situations History

  This report shows the distribution of situation events status in a pie chart, along with more detailed information on the history of situation events listed in a table.

These reports use the following attribute groups:

- **Windows agent:**
  - Logical_Disk
  - Memory
  - Process
  - Server
  - System
- **Linux agent:**
  - CPU
  - Disk
  - Network
  - Process
  - VM_Stats
- **UNIX agent:**
  - Disk
  - Network
  - Process
  - System
  - Memory
- KSY SUMMARIZATION CONFIG

The next sections in this chapter contain descriptions of the reports. For each report, the following information is included:

- Name
- Description
- Purpose
- Parameters
- Tables or views used
- Output
- Usage

One of the parameters, summarization type, has the following maximum forecast periods:

- Hourly: 60 hours in the future
- Daily: 60 days in the future
- Weekly: 1 year in the future
- Monthly: 5 years in the future
- Quarterly: no limit
- Yearly: no limit

Utilization Details for Single Resource report

Name	Utilization Details for Single Resource

Description	This report shows resources utilization for a selected server: CPU utilization, disk utilization, memory utilization, network utilization. Each metric is shown on a separate chart where data for the server is overlaid. For disk utilization, only this average value for all logical disks is shown. For network utilization, total value for all network interfaces is shown. The time frame for report data can be determined in the standard way by using the *Duration* and *Include shift periods* parameters. The server can be selected from a list of available servers by using the *OS Type* and *Servers* parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on linear trend computed over historical data. The report also shows the top 10 CPU utilizing processes for the selected server.
Purpose	Helps identify system performance problems related to over-utilization of key system resources. Helps identify which systems are performing poorly due to low physical memory, causing excessive paging, performing poorly due to CPU intensive tasks, or performing poorly due to other factors such as poor load balancing of applications across available systems.

Parameters	**OS Type** Determines the type of agent to work on, and is selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from or to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and is selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type are displayed in a drop-down list sorted alphabetically. You can see up to 30 system names. For more than 30 names, type the name to see the filtered list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast **Show Data** Specifies if the chart data source should be displayed in a table or not.

Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **CPU Utilization:** **Windows agent:** NT_System_HV, NT_System_DV, NT_System_WV, NT_System_MV, NT_System_QV, NT_System_YV **Linux agent:** KLZ_CPU_HV, KLZ_CPU_DV, KLZ_CPU_WV, KLZ_CPU_MV, KLZ_CPU_QV, KLZ_CPU_YV **UNIX agent:** System_HV, System_DV, System_WV, System_MV, System_QV, System_YV **Disk Utilization:** **Windows agent:** NT_Logical_Disk_HV, NT_Logical_Disk_DV, NT_Logical_Disk_WV, NT_Logical_Disk_MV, NT_Logical_Disk_QV, NT_Logical_Disk_YV **Linux agent:** KLZ_Disk_HV, KLZ_Disk_DV, KLZ_Disk_WV, KLZ_Disk_MV, KLZ_Disk_QV, KLZ_Disk_YVV **UNIX agent:** Disk_HV, Disk_DV, Disk_WV, Disk_MV, Disk_QV, Disk_YV **Memory Utilization:** **Windows agent:** NT_Memory_64_HV, NT_Memory_64_DV, NT_Memory_64_WV, NT_Memory_64_MV, NT_Memory_64_QV, NT_Memory_64_YV **Linux agent:** KLZ_VM_Stats_HV, KLZ_VM_Stats_DV, KLZ_VM_Stats_WV, KLZ_VM_Stats_MV, KLZ_VM_Stats_QV, KLZ_VM_Stats_YV **UNIX agent:** Unix_Memory_HV, Unix_Memory_DV, Unix_Memory_WV, Unix_Memory_MV, Unix_Memory_QV, Unix_Memory_YV **Network Utilization:** **Windows agent:** NT_Server_HV, NT_Server_DV, NT_Server_WV, NT_Server_MV, NT_Server_QV, NT_Server_YV **Linux agent:** KLZ_Network_HV, KLZ_Network_DV, KLZ_Network_WV, KLZ_Network_MV, KLZ_Network_QV, KLZ_Network_YV **UNIX agent:** Network_HV, NetworkDV, Network_WV, Network_MV,Network_QV, Network_YV **Processes:** **Windows agent:** NT_Process_64_HV, NT_Process_64_DV, NT_Process_64_WV, NT_Process_64_MV, NT_Process_64_QV, NT_Process_64_YV **Linux agent:** KLZ_Process_HV, KLZ_Process_DV, KLZ_Process_WV, KLZ_Process_MV, KLZ_Process_QV, KLZ_Process_YV **UNIX agent:** Process_HV, Process_DV, Process_WV, Process_MV, Process_QV, Process_YV
Output	Four line charts to show CPU, disk, memory and network usage for the selected system. Each chart has 3 lines representing average, maximum and minimum % processor time used by a server over a period along with SPC data like average, upper control limit and lower control limit. A table representing the top 10 CPU utilizing processes for the selected server .

Usage	The IT administrator or manager responsible for meeting service levels based on server performance needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs) and at what times are they at most risk of violation. The same report can be used for hourly, daily, weekly, monthly, quarterly, and yearly. The ability to compare all four metrics in one chart is useful.
Drill through	On memory section title to Memory Utilization for Single Resource.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				
Linux	Linux CPU	KLZ_CPU	X	X	X	X	X	X
	Linux Disk	KLZ_Disk	X	X	X	X	X	X
	Linux VM Stats	KLZ_VM_Stats	X	X	X	X	X	X
	Linux Network	KLZ_Network	X	X	X	X	X	X
	Linux Process	KLZ_Process	X	X	X	X	X	X
UNIX	System	System	X	X	X	X	X	X
	Disk	Disk	X	X	X	X	X	X
	UNIX Memory	UNIX_Memory	X	X	X	X	X	X
	Network	Network	X	X	X	X	X	X
	Process	Process	X	X	X	X	X	X
Windows	System	NT_System	X	X	X	X	X	X
	Logical Disk	NT_Logical_Disk	X	X	X	X	X	X
	Memory	NT_Memory_64	X	X	X	X	X	X
	Server	NT_Server	X	X	X	X	X	X
	Process	NT_Process_64	X	X	X	X	X	X

Utilization Details for Multiple Resources report

Name	Utilization Details for Multiple Resources
Description	This report shows resources utilization for selected servers: CPU utilization, disk utilization, memory utilization, network utilization. Each metric is shown on a separate line chart where data for all servers is overlaid. For disk utilization, only average value for all logical disks is shown. For network utilization, total value for all network interfaces is shown. The time frame for report data can be determined in standard way by using the *Duration* and *Include shift periods* parameters. The servers can be selected from a list of available servers using the *OS Type* and *Servers* parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on linear trend computed over historical data.

Purpose	Helps identify and compare system performance problems related to over-utilization of key system resources. Helps identify which systems are performing poorly due to low physical memory, causing excessive paging, performing poorly due to CPU intensive tasks, or performing poorly due to other factors such as poor load balancing of applications across available systems.
Parameters	**OS Type** Determines the type of agent to work on and can be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and should be selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type are displayed in a drop-down list sorted alphabetically. You are able to see up to 30 system names. For more than 30 names, type the name to filter the list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days

Parameters (Cont.)	**Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **CPU Utilization:** **Windows agent:** NT_System_HV, NT_System_DV, NT_System_WV, NT_System_MV, NT_System_QV, NT_System_YV **Linux agent:** KLZ_CPU_HV, KLZ_CPU_DV, KLZ_CPU_WV, KLZ_CPU_MV, KLZ_CPU_QV, KLZ_CPU_YV **UNIX agent:** System_HV, System_DV, System_WV, System_MV, System_QV, System_YV **Disk Utilization:** **Windows agent:** NT_Logical_Disk_HV, NT_Logical_Disk_DV, NT_Logical_Disk_WV, NT_Logical_Disk_MV, NT_Logical_Disk_QV, NT_Logical_Disk_YV **Linux agent:** KLZ_Disk_HV, KLZ_Disk_DV, KLZ_Disk_WV, KLZ_Disk_MV, KLZ_Disk_QV, KLZ_Disk_YV **UNIX agent:** Disk_HV, Disk_DV, Disk_WV, Disk_MV, Disk_QV, Disk_YV **Memory Utilization:** **Windows agent:** NT_Memory_64_HV, NT_Memory_64_DV, NT_Memory_64_WV, NT_Memory_64_MV, NT_Memory_64_QV, NT_Memory_64_YV **Linux agent:** KLZ_VM_Stats_HV, KLZ_VM_Stats_DV, KLZ_VM_Stats_WV, KLZ_VM_Stats_MV, KLZ_VM_Stats_QV, KLZ_VM_Stats_YV **UNIX agent:** Unix_Memory_HV, Unix_Memory_DV, Unix_Memory_WV, Unix_Memory_MV, Unix_Memory_QV, Unix_Memory_YV **Network Utilization:** **Windows agent:** NT_Server_HV, NT_Server_DV, NT_Server_WV, NT_Server_MV, NT_Server_QV, NT_Server_YV **Linux agent:** KLZ_Network_HV, KLZ_Network_DV, KLZ_Network_WV, KLZ_Network_MV, KLZ_Network_QV, KLZ_Network_YV **UNIX agent:** Network_HV, NetworkDV, Network_WV, Network_MV,Network_QV, Network_YV
Output	Three overlaid line charts for selected systems, with each line representing the different systems. The legend is interactive.

Usage	The IT administrator or manager responsible for meeting service levels based on server performance needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). Reports indicate which systems are overutilized or underutilized relative to a collection of systems. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	On legends to Utilization Details for Single Resource. On the memory section title to Memory Utilization for Multiple Resources Comparison. On the CPU section title to CPU Utilization Comparison for Multiple Resources. On the disk section title to Disk Utilization Comparison for Multiple Resources.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				
Linux	Linux CPU	KLZ_CPU	X	X	X	X	X	X
	Linux Disk	KLZ_Disk	X	X	X	X	X	X
	Linux VM Stats	KLZ_VM_Stats	X	X	X	X	X	X
	Linux Network	KLZ_Network	X	X	X	X	X	X
UNIX	System	System	X	X	X	X	X	X
	Disk	Disk	X	X	X	X	X	X
	UNIX Memory	UNIX_Memory	X	X	X	X	X	X
	Network	Network	X	X	X	X	X	X
Windows	System	NT_System	X	X	X	X	X	X
	Logical Disk	NT_Logical_Disk	X	X	X	X	X	X
	Memory	NT_Memory_64	X	X	X	X	X	X
	Server	NT_Server	X	X	X	X	X	X

Utilization Comparison for Single Resource report

Name	Utilization Comparison for Single Resource
Description	This report shows the comparison between CPU, disk, and memory utilization for a particular server, over a period of time, in an overlaid line chart. By clicking on the chart title, you can drill-through to see the Utilization Details for Single Resource report for the same server. The time frame for report data can be determined in the standard way by using the *Duration* and *Include shift periods* parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on linear trend computed over historical data.
Purpose	This report helps to compare the CPU, disk, and memory utilization of a single server.

Parameters	**OS Type** Determines the type of agent to work on, and is selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from or to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and is selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type are displayed in a drop-down list sorted alphabetically. You can see up to 30 system names. For more than 30 names, type the name to see the filtered list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast

Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_HV, NT_System_DV, NT_System_WV, NT_System_MV, NT_System_QV, NT_System_YV, NT_Logical_Disk_HV, NT_Logical_Disk_DV, NT_Logical_Disk_WV, NT_Logical_Disk_MV, NT_Logical_Disk_QV, NT_Logical_Disk_YV, NT_Memory_64_HV, NT_Memory_64_DV, NT_Memory_64_WV, NT_Memory_64_MV, NT_Memory_64_QV, NT_Memory_64_YV **Linux agent:** KLZ_CPU_HV, KLZ_CPU_DV, KLZ_CPU_WV, KLZ_CPU_MV, KLZ_CPU_QV, KLZ_CPU_YV, KLZ_Disk_HV, KLZ_Disk_DV, KLZ_Disk_WV, KLZ_Disk_MV, KLZ_Disk_QV, KLZ_Disk_YV, KLZ_VM_Stats_HV, KLZ_VM_Stats_DV, KLZ_VM_Stats_WV, KLZ_VM_Stats_MV, KLZ_VM_Stats_QV, KLZ_VM_Stats_YV **UNIX agent:** System_HV, System_DV, System_WV, System_MV, System_QV, System_YV, Disk_HV, Disk_DV, Disk_WV, Disk_MV, Disk_QV, Disk_YV, Unix_Memory_HV, Unix_Memory_DV, Unix_Memory_WV, Unix_Memory_MV, Unix_Memory_QV, Unix_Memory_YV
Output	An overlaid line chart showing the comparison between CPU, disk, and memory utilization for a particular server, over a period of time.
Usage	The IT administrator or manager responsible for meeting the server service levels needs to receive a daily report showing which servers are at risk of violating Service Level Agreements (SLAs). The report shows the overall resource utilization of a single server. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	By clicking on the chart title, you can drill-through to see the Utilization Details for Single Resource report for the same server.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux CPU	KLZ_CPU	X	X	X	X	X	X
	Linux Disk	KLZ_Disk	X	X	X	X	X	X
	Linux VM Stats	KLZ_VM_Stats	X	X	X	X	X	X
UNIX	System	System	X	X	X	X	X	X
	Disk	Disk	X	X	X	X	X	X
	UNIX Memory	UNIX_Memory	X	X	X	X	X	X
Windows	System	NT_System	X	X	X	X	X	X
	Logical Disk	NT_Logical_Disk	X	X	X	X	X	X
	Memory	NT_Memory_64	X	X	X	X	X	X

Utilization Comparison for Multiple Resources report

Name	Utilization Comparison for Multiple Resources

Description	This report shows the comparison between CPU, disk, and memory utilization for the selected servers over a period of time. By clicking on the chart title, you can drill-through to see the corresponding Utilization Details for Multiple Resources report. By clicking on the server name, you can drill-through to see the Utilization Details for Single Resource report for the selected server. By clicking on the chart data points, you can drill-through to the corresponding CPU, Disk, or Memory Utilization for Single Resource report. The time frame for report data can be determined in the standard way by using the *Duration* and *Include shift periods* parameters. The servers can be selected from a list of available servers using the OS Type and Servers parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on linear trend computed over historical data.
Purpose	This report helps to compare the CPU, disk, and memory utilization for multiple servers.

Parameters	**OS Type** Determines the type of agent to work on, and is selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from or to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and is selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type are displayed in a drop-down list sorted alphabetically. You can see up to 30 system names. For more than 30 names, type the name to see the filtered list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast

Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_HV, NT_System_DV, NT_System_WV, NT_System_MV, NT_System_QV, NT_System_YV, NT_Logical_Disk_HV, NT_Logical_Disk_DV, NT_Logical_Disk_WV, NT_Logical_Disk_MV, NT_Logical_Disk_QV, NT_Logical_Disk_YV, NT_Memory_64_HV, NT_Memory_64_DV, NT_Memory_64_WV, NT_Memory_64_MV, NT_Memory_64_QV, NT_Memory_64_YV **Linux agent:** KLZ_CPU_HV, KLZ_CPU_DV, KLZ_CPU_WV, KLZ_CPU_MV, KLZ_CPU_QV, KLZ_CPU_YV, KLZ_Disk_HV, KLZ_Disk_DV, KLZ_Disk_WV, KLZ_Disk_MV, KLZ_Disk_QV, KLZ_Disk_YV, KLZ_VM_Stats_HV, KLZ_VM_Stats_DV, KLZ_VM_Stats_WV, KLZ_VM_Stats_MV, KLZ_VM_Stats_QV, KLZ_VM_Stats_YV **UNIX agent:** System_HV, System_DV, System_WV, System_MV, System_QV, System_YV, Disk_HV, Disk_DV, Disk_WV, Disk_MV, Disk_QV, Disk_YV, Unix_Memory_HV, Unix_Memory_DV, Unix_Memory_WV, Unix_Memory_MV, Unix_Memory_QV, Unix_Memory_YV
Output	Three line charts showing the CPU, disk, and memory utilization are displayed for each server selected. A table, which can be collapsed, corresponds to each chart.
Usage	The IT administrator or manager responsible for meeting the server service levels needs to receive a daily report showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates which systems are over-utilized or under-utilized relative to a collection of systems. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	By clicking on the chart title, you can drill-through to see the corresponding Utilization Details for Multiple Resources report. By clicking on the server name, you can drill-through to see the Utilization Details for Single Resource report for the selected server. By clicking on the chart data points, you can drill-through to the corresponding CPU, Disk or Memory Utilization for Single Resource report.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux CPU	KLZ_CPU	X	X	X	X	X	X
	Linux Disk	KLZ_Disk	X	X	X	X	X	X
	Linux VM Stats	KLZ_VM_Stats	X	X	X	X	X	X
UNIX	System	System	X	X	X	X	X	X
	Disk	Disk	X	X	X	X	X	X
	UNIX Memory	UNIX_Memory	X	X	X	X	X	X
Windows	System	NT_System	X	X	X	X	X	X
	Logical Disk	NT_Logical_Disk	X	X	X	X	X	X
	Memory	NT_Memory_64	X	X	X	X	X	X

Utilization Heat Chart for Single Resource report

Name	Utilization Heat Chart for Single Resource

Description	This report helps identify patterns of utilization of a particular system over a period of time. The first column shows dates during the selected time period and the other columns represent hours during the day. The chart can be used for showing a heat chart for CPU, memory, disk or all three in the same report. The dates have hyperlinks that allow you to drill through to the Utilization Details for Single Resource report.
Purpose	Helps identify system performance of a system or server over a period of time. Shows daily patterns for utilization.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and should be selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type is displayed in a drop-down list sorted alphabetically. You can see up to 30 system names. For more than 30 names, type the name to filter the list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days

Parameters (continued)	**Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast **Upper Limit for Good Status** Specifies the upper limit for good status. **Upper Limit for Fair Status** Specifies the upper limit for fair status. **Upper Limit for Warning Status** Specifies the upper limit for warning status. **Upper Limit for Bad Status and Lower Limit for Critical Status** Specifies the upper limit for bad status and the lower limit for critical status.
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **CPU Utilization:** **Windows agent:** NT_System_HV **Linux agent:** KLZ_CPU_HV **UNIX agent:** System_HV **Disk Utilization:** **Windows agent:** NT_Logical_Disk_HV **Linux agent:** KLZ_Disk_HV **UNIX agent:** Disk_HV **Memory Utilization:** **Windows agent:** NT_Memory_64_HV **Linux agent:** KLZ_VM_Stats_HV **UNIX agent:** Unix_Memory_HV
Output	A heat chart. The first column shows dates during the selected time period and the other columns represent 24 hours during the day starting with 0. The last column shows average value for that day. The report can be generated for CPU, disk or memory utilization. The timestamp is a hyperlink that you can use to drill through to a details report for CPU, disk, memory, network usage, top 10 processes for that particular system on the selected day. The thresholds for the colors can be specified in the parameters.
Usage	The IT administrator or manager responsible for meeting service levels based on server performance needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). Reports indicate which systems are overutilized or underutilized relative to a collection of systems. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	On row level to Utilization Details for Single Resource.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				
Linux	Linux CPU	KLZ_CPU	X					
	Linux Disk	KLZ_Disk	X					
	Linux VM Stats	KLZ_VM_Stats	X					
UNIX	System	System	X					
	Disk	Disk	X					
	UNIX Memory	UNIX_Memory	X					
Windows	System	NT_System	X					
	Logical Disk	NT_Logical_Disk	X					
	Memory	NT_Memory_64	X					

Memory Utilization for Single Resource report

Name	Memory Utilization for Single Resource
Description	This report shows memory usage details for a specific system. It uses a line chart to show the percentage of virtual, physical and swap memory usage. It also provides finer memory metrics in a table. The time frame for report data can be determined in the standard way by using the Duration and Include shift periods parameters. The server can be selected from a list of available servers by using the *OS Type* and *Servers* parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on linear trends computed over historical data.
Purpose	Helps identify which systems are performing poorly due to low physical memory causing excessive paging.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and should be selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type is displayed in a drop-down list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days

Parameters (continued)	**Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_Memory_64_HV, NT_Memory_64_DV, NT_Memory_64_WV, NT_Memory_64_MV,NT_Memory_64_QV, NT_Memory_64_YV, NT_Paging_File_HV, NT_Paging_File_DV, NT_Paging_File_WV, NT_Paging_File_MV,NT_Paging_File_QV, NT_Paging_File_YV **Linux agent:** KLZ_VM_Stats_HV, KLZ_VM_Stats_DV, KLZ_VM_Stats_WV, KLZ_VM_Stats_MV,KLZ_VM_Stats_QV, KLZ_VM_Stats_YV **UNIX agent:** Unix_Memory_HV, Unix_Memory_DV, Unix_Memory_WV, Unix_Memory_MV,Unix_Memory_QV, Unix_Memory_YV
Output	A line chart showing the average usage of virtual, physical and swap memory. A table showing finer memory details.
Usage	The IT administrator or manager responsible for meeting service levels based on server performance needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates what is the memory health of a single system systems and if it is over-utilized or under-utilized. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	None.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux VM Stats	KLZ_Network	X	X	X	X	X	X
	UNIX Memory	UNIX_Memory	X	X	X	X	X	X
Windows	Memory	NT_Memory_64	X	X	X	X	X	X
	Paging File	NT_Paging_File	X	X	X	X	X	X

Memory Utilization for Multiple Resources Comparison report

Name	Memory Utilization for Multiple Resources Comparison

Description	This report shows memory usage details for multiple systems over a period of time. It uses three overlaid line charts for virtual, physical and swap memory. The time frame for report data can be determined in standard way by using the Duration and Include shift periods parameters. The servers can be selected from a list of available servers by using the *OS Type* and *Servers* parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on linear trend computed over historical data.
Purpose	Helps identify and compare different systems behavior to identify potential memory issues due to unbalanced workload or wrong configurations. Helps identify which systems are performing poorly due to low physical memory, causing excessive paging.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and should be selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type is displayed in a drop-down list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days

Parameters (continued)	**Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_Memory_64_HV, NT_Memory_64_DV, NT_Memory_64_WV, NT_Memory_64_MV,NT_Memory_64_QV, NT_Memory_64_YV, NT_Paging_File_HV, NT_Paging_File_DV, NT_Paging_File_WV, NT_Paging_File_MV,NT_Paging_File_QV, NT_Paging_File_YV **Linux agent:** KLZ_VM_Stats_HV, KLZ_VM_Stats_DV, KLZ_VM_Stats_WV, KLZ_VM_Stats_MV,KLZ_VM_Stats_QV, KLZ_VM_Stats_YV **UNIX agent:** Unix_Memory_HV, Unix_Memory_DV, Unix_Memory_WV, Unix_Memory_MV,Unix_Memory_QV, Unix_Memory_YV
Output	Three overlaid line charts for selected systems, with each line representing the different systems. Each chart represents the behavior of a memory aspect.
Usage	The IT administrator or manager responsible for meeting service levels based on server performance needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates which systems are over-utilized or under-utilized relative to a collection of systems. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	On legends to Memory Utilization for Single Resource.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux VM Stats	KLZ_Network	X	X	X	X	X	X
	UNIX Memory	UNIX_Memory	X	X	X	X	X	X
Windows	Memory	NT_Memory_64	X	X	X	X	X	X
	Paging File	NT_Paging_File	X	X	X	X	X	X

Top Resources Utilization report

Name	Top Resources Utilization

Description	This report shows top resources by CPU, disk and memory utilization. The stacked bars show average resource used and free (in percent) for each system over the selected report period. If the number of systems is less than 20, then a bar is shown in each row. For example, there are 20 rows in the table with charts for each system. If the number of systems is more than 20, then a bar chart is on top with the top 20 systems and the rest of the data is in the table. This is done to eliminate over-crowding of the bars in the chart.
Purpose	*CPU utilization:* Helps identify which systems are most overloaded and which have the least load based on the percentage of CPU utilization. Identifies which systems are over-utilized and which are under-utilized. *Disk utilization:* Helps identify which systems are experiencing heavy disk activity. Additionally, shows systems running low on disk space. This allows for planning the addition of hard drives or balancing of applications or data across available hard disk resources. *Memory utilization:* Helps identify growth in memory utilization which can lead to application and server outages. This allows for planning the increasing of paging space or the addition of physical memory.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and should be selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Number of systems** The maximum number of systems to display. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Resource** A drop-down list that you can use to choose which type of resource to display: • All • CPU • Disk • Memory

Tables or views used	**CPU utilization** • **General:** KSY_SUMMARIZATION_CONFIG_DV • **Windows agent:** NT_System_HV, NT_System_DV, NT_System_WV, NT_System_MV, NT_System_QV, NT_System_YV • **Linux agent:** KLZ_CPU_HV, KLZ_CPU_DV, KLZ_CPU_WV, KLZ_CPU_MV, KLZ_CPU_QV, KLZ_CPU_YV • **UNIX agent:** System_HV, System_DV, System_WV, System_MV, System_QV, System_YV **Disk utilization** • **Windows agent:** NT_Logical_Disk_HV, NT_Logical_Disk_DV, NT_Logical_Disk_WV, NT_Logical_Disk_MV, NT_Logical_Disk_QV, NT_Logical_Disk_YV • **Linux agent:** KLZ_Disk_HV, KLZ_Disk_DV, KLZ_Disk_WV, KLZ_Disk_MV, KLZ_Disk_QV, KLZ_Disk_YV • **UNIX agent:** Disk_HV, Disk_DV, Disk_WV, Disk_MV, Disk_QV, Disk_YV **Memory utilization** • **Windows agent:** NT_Memory_64_HV, NT_Memory_64_DV, NT_Memory_64_WV, NT_Memory_64_MV, NT_Memory_64_QV, NT_Memory_64_YV • **Linux agent:** KLZ_VM_Stats_HV, KLZ_VM_Stats_DV, KLZ_VM_Stats_WV, KLZ_VM_Stats_MV, KLZ_VM_Stats_QV, KLZ_VM_Stats_YV • **UNIX agent:** Unix_Memory_HV, Unix_Memory_DV, Unix_Memory_WV, Unix_Memory_MV, Unix_Memory_QV, Unix_Memory_YV
Output	A table is displayed with each row displaying a stacked bar representing one of the following for each system over the selected report period. • average CPU used and free (in percent) • average disk space used and free (in GB and in percent) • average memory used and free (in percent) If the number of systems is less than 20, then a bar is shown in each row. For example, there are 20 rows in the table with charts for each system. If the number of systems is more than 20, then a bar chart is on top with the top 20 systems and the rest of the data is in the table. This is done to eliminate over-crowding of the bars in the chart. The charts are interactive. By clicking on the server, the hyperlink to the Utilization Details for Single Resource is provided.
Usage	The IT administrator or manager responsible for meeting service levels based on server performance needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). Reports indicate which systems are overutilized or underutilized relative to a collection of systems. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	On systems axis to Utilization Details for Single Resource.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				

OS Type	Attribute Group	Table	Summarization					
Linux	Linux CPU	KLZ_CPU	X	X	X	X	X	X
	Linux Disk	KLZ_Disk	X	X	X	X	X	X
	Linux VM Stats	KLZ_VM_Stats	X	X	X	X	X	X
UNIX	System	System	X	X	X	X	X	X
	Disk	Disk	X	X	X	X	X	X
	UNIX Memory	UNIX_Memory	X	X	X	X	X	X
Windows	System	NT_System	X	X	X	X	X	X
	Logical Disk	NT_Logical_Disk	X	X	X	X	X	X
	Memory	NT_Memory_64	X	X	X	X	X	X

Top Situations by Status report

Name	Top Situations by Status
Description	This report shows the top 10 situations sorted by the selected status in a bar chart, along with finer details on all the top situations, listed in a table. The time frame for the report data can be determined, in the standard way, by using the *Duration* parameter.
Purpose	Helps to analyze the top situations generating the selected event.
Parameters	**Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Status** You can choose which situation status to use in order to identify the top situations. The options are displayed in a drop-down menu where a single value can be selected between the following ones: • Acknowledged • Closed • Open • Reset • Stopped • Unknown **Aggregate Situations** You can choose if the situations should be aggregated by the Managed System and Atomize attributes or not. The default value for this parameter is Yes.
Tables or views used	**General:** CCC Logs: STATUS_HISTORY (Raw Data)

Output	A bar chart showing the top 10 situations sorted by the selected status. A table showing finer details on all the top situations sorted by the selected status.
Usage	The IT administrator or manager responsible for meeting the server service levels needs to receive periodic reports which identify the top situations generating a specific event.
Drill through	By clicking on the situation name in the table, you can drill-through to see the corresponding Situations History report.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
CCC Logs	CCC Logs	STATUS_HISTORY						

Enterprise Resources List report

Name	Enterprise Resources List
Description	This report lists all the Windows, Linux and UNIX resources in the environment. On clicking on a resource name you can drill through to see the utilization details for that resource over a period of time.
Purpose	You can use this report to see the list of OS Agents in the enterprise during a particular time.
Parameters	None
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System **Linux agent:** KLZ_CPU **UNIX agent:** System
Output	The output consists of three tables showing the resource names for Windows, Linux and UNIX. Each resource name is a hyperlink, and you can use this link to drill down to the Utilization Heat Chart for Single Resource report.
Usage	The manager responsible for meeting service levels needs to receive a weekly report of the existing systems in his environment.
Drill through	On each row in the list to Utilization Heat Chart for Single Resource.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				

Enterprise Daily Utilization Heat Chart report

Name	Enterprise Daily Utilization Heat Chart
Description	This report shows CPU, disk, and memory patterns for all servers, for a select operating system type, and on a particular date. The first column lists the server names. The rest of the columns show utilization data during the day hours and the last column shows the average for the server on the selected date. You can choose to see either CPU, disk, memory, or all three metrics. The date can be selected from a date prompt. The type of operating system (Linux, UNIX, Windows) can be selected from a drop down menu.
Purpose	This report helps to compare the CPU, disk and memory utilization of the machines with the same operating system in the Enterprise.
Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date** A date prompt where you can choose the date of the report. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Attribute** A drop-down list that you can use to choice what type of resource you would like to display: • All (Default) • CPU • Disk • Memory **Upper Limit for Good Status** Specifies the upper limit for good status. **Upper Limit for Fair Status** Specifies the upper limit for fair status. **Upper Limit for Warning Status** Specifies the upper limit for warning status. **Upper Limit for Bad Status and Lower Limit for Critical Status** Specifies the upper limit for bad status and the lower limit for critical status.
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_HV, NT_Logical_Disk_HV, NT_Memory_64_HV **Linux agent:** KLZ_CPU_HV, KLZ_Disk_HV, KLZ_VM_Stats_HV **UNIX agent:** System_HV, Disk_HV, Unix_Memory_HV

Output	A heat chart per attribute (CPU, Disk, Memory) is shown for all the servers with the selected operating system. The first column lists the server names. The rest of the columns show utilization data during the day hours and the last column shows the average for the server on the selected date. You can choose to see either CPU, disk, memory or all metrics.
Usage	The IT administrator or manager responsible for meeting the server service levels needs to receive a daily report showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates which systems are over-utilized or under-utilized relative to a collection of systems.
Drill through	None.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux CPU	KLZ_CPU	X					
	Linux Disk	KLZ_Disk	X					
	Linux VM Stats	KLZ_VM_Stats	X					
UNIX	System	System	X					
	Disk	Disk	X					
	UNIX Memory	UNIX_Memory	X					
Windows	System	NT_System	X					
	Logical Disk	NT_Logical_Disk	X					
	Memory	NT_Memory_64	X					

Enterprise Summary report

Name	Enterprise Summary
Description	This report shows the overall availability and utilization of all Windows, Linux and UNIX monitoring agents.
Purpose	You can use this report to compare different agent types in the environment. Note this report will run only when all 3 types of the OS agents are present in the environment.

Parameters	**Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_DV, NT_Memory_64_DV, NT_Logical_Disk_DV **Linux agent:** KLZ_CPU_DV, KLZ_VM_Stats_DV, KLZ_Disk_DV, KLZ_System_Statistics_DV **UNIX agent:** System_DV, Disk_DV, Unix_Memory_DV
Output	The output consists of a bar chart showing a comparison of the different attributes CPU, Disk, Memory and Availability for Windows, UNIX, and Linux.
Usage	The IT administrator can see the health of the entire environment and compare the different OS types.
Drill through	On each bar to Top Resources by Utilization for the selected resource only. **Note:** This link only works for CPU, disk, and memory.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux CPU	KLZ_CPU		X				
	Linux Disk	KLZ_Disk		X				
	Linux VM Stats	KLZ_VM_Stats		X				
	Linux System Statistics	KLZ_System_Statistics		X				
UNIX	System	System		X				
	Disk	Disk		X				
	UNIX Memory	UNIX_Memory		X				
Windows	System	NT_System		X				
	Logical Disk	NT_Logical_Disk		X				
	Memory	NT_Memory_64		X				

Top Resources by Availability

Name	Top Resources by Availability
Description	This report displays availability of the top N systems based on System Up time over a period of time.
Purpose	Helps identify which systems have the worst (or best) availability based on the percentage of time the system is up and running. Identifies which systems are inherently unstable.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Number of systems** The maximum number of systems to display. **Sort by** A drop-down list that you can use to choose how the top N list is sorted: • % Up Time • % Down Time
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_DV **Linux agent:** KLZ_System_Statistics_DV **UNIX agent:** System_DV
Output	Stacked bar chart showing average uptime and downtime for each system over the selected report period. The bar charts are interactive and let you drill through to a heat chart for system availability.
Usage	The manager responsible for meeting service levels based on server availability needs to receive a weekly report showing which servers are at risk of violating Service Level Agreements (SLAs).

Drill through	In the bar chart to Availability Heat Chart for Single Resource.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				
Linux	Linux System Statistics	KLZ_System_Statistics_DV		X				
Windows	System	NT_System_DV		X				
UNIX	System	System_DV		X				

Top Resources Utilization Summary Heat Chart report

Name	Top Resources Utilization Summary Heat Chart
Description	This report shows top resources by CPU, disk, or memory utilization in a summary heat chart. By clicking on the resource name or the utilization value, you can drill through to a heat chart showing CPU, disk and memory utilization for the selected resource over the same period of time. The time frame for the report data can be determined, in the standard way, by using the *Duration* and *Include shift periods* parameters. The type of operating system (Linux, UNIX, Windows) can be selected from a drop down menu.
Purpose	This report helps to compare the top servers by CPU, disk, and memory utilization.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Sorting Attribute** A drop-down list that you can use to choice what type of resource you would like to display: • CPU (Default) • Disk • Memory **Number of Systems** The maximum number of servers to show in the report. **Upper Limit for Good Status** Specifies the upper limit for good status. **Upper Limit for Fair Status** Specifies the upper limit for fair status. **Upper Limit for Warning Status** Specifies the upper limit for warning status. **Upper Limit for Bad Status and Lower Limit for Critical Status** Specifies the upper limit for bad status and the lower limit for critical status.

Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_HV, NT_Logical_Disk_HV, NT_Memory_64_HV **Linux agent:** KLZ_CPU_HV, KLZ_Disk_HV, KLZ_VM_Stats_HV **UNIX agent:** System_HV, Disk_HV, Unix_Memory_HV
Output	A heat chart with three columns for each server showing the CPU, disk, and memory utilization. The servers are sorted by CPU, disk, or memory utilization depending on the sorting attribute. The maximum number of servers shown is determined by the value of the *Number of systems* parameter.
Usage	The IT administrator or manager responsible for meeting the server service levels, needs to receive a daily report showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates which systems are over-utilized or under-utilized relative to a collection of systems.
Drill through	By clicking on the resource name or the utilization value, you can drill through to a heat chart showing CPU, disk, and memory utilization for the selected resource over the same period of time.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux CPU	KLZ_CPU	X					
	Linux Disk	KLZ_Disk	X					
	Linux VM Stats	KLZ_VM_Stats	X					
UNIX	System	System	X					
	Disk	Disk	X					
	UNIX Memory	UNIX_Memory	X					
Windows	System	NT_System	X					
	Logical Disk	NT_Logical_Disk	X					
	Memory	NT_Memory_64	X					

Top Resources by Availability (MTTR/MTBSI)

Name	Top Resources by Availability (MTTR/MTBSI)
Description	This report displays availability trending of the top N systems based on the Mean Time Before System Interruption (MTBSI) and Mean Time To Recovery (MTTR).
Purpose	Help identify which systems have the worst (or best) availability based on the amount of time the system is up/running and the amount of time it takes to bring a system back online following an outage. Identifies which systems are inherently unstable.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Number of systems** The maximum number of systems to display. **Sort by** A drop-down list that you can use to choose how the top N list is sorted: • Mean Time To Recovery (Default) • Mean Time Before System Interruption
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_DV **Linux agent:** KLZ_System_Statistics_DV **UNIX agent:** System_DV
Output	Stacked bar chart showing MTBSI and MTTR for each resource. An ordered table showing additional data .
Usage	The manager responsible for meeting service levels based on server availability needs to receive a weekly report showing which servers are at risk of violating Service Level Agreements (SLAs).
Drill through	None.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				
Linux	Linux System Statistics	KLZ_System_Statistics_DV		X				
Windows	System	NT_System_DV		X				
UNIX	System	System_DV		X				

Resource Availability Comparison

Name	Resource Availability Comparison
Description	This report shows availability comparison between two or more servers.
Purpose	Helps compare multiple systems based on availability.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_DV **Linux agent:** KLZ_System_Statistics_DV **UNIX agent:** System_DV
Output	Pie charts showing % Uptime and % Downtime for selected servers. A table showing the same availability information plus details on the number of days each system is available and unavailable.
Usage	The manager responsible for meeting service levels based on server availability needs to receive a weekly report showing which servers are at risk of violating Service Level Agreements (SLAs).
Drill through	None.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				
Linux	Linux System Statistics	KLZ_System_Statistics_DV		X				
Windows	System	NT_System_DV		X				
UNIX	System	System_DV		X				

Availability Heat Chart for Single Resource

Name	Availability Heat Chart for Single Resource
Description	This report helps identify patterns of resource availability over a period of time.
Purpose	Helps identify system performance of a system or server over a period of time. Shows daily patterns for availability or unavailability.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only **Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Attribute** A drop-down list that you can use to specify which pattern to display: • % Up Time (Default) • % Down Time **Upper Limit for Good Status** Specifies the upper limit for good status. **Upper Limit for Fair Status** Specifies the upper limit for fair status. **Upper Limit for Warning Status** Specifies the upper limit for warning status. **Upper Limit for Bad Status and Lower Limit for Critical Status** Specifies the upper limit for bad status and the lower limit for critical status.
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_HV **Linux agent:** KLZ_System_Statistics_HV **UNIX agent:** System_DV

Output	A heat chart. The first column shows dates during the selected time period and the other columns represent 24 hours during the day starting with 0. The report can also be reversed to show system downtime instead of uptime based on parameter selection. The thresholds for the colors can be specified in the parameters.
Usage	The IT administrator or manager can use this report to identify patterns of availability for a particular system over a period of time.
Drill through	None.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG_DV		X				
Linux	Linux System Statistics	KLZ_System_Statistics_HV	X					
Windows	System	NT_System_HV	X					
UNIX	System	System_DV	X					

CPU Utilization Comparison for Multiple Resources

Name	CPU Utilization Comparison for Multiple Resources
Description	This report shows CPU usage details for multiple systems, over a period of time, in three overlaid line charts for busy, user and system CPU usage on Linux and UNIX systems, and for total processor, user and privileged CPU usage on Windows systems. The time frame for the report data can be determined, in the standard way, by using the Duration and include the shift period parameters. The servers can be selected from a list of available servers using the *OS Type* and *Servers* parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on the linear trend computed over historical data.
Purpose	Helps to compare different system CPU usage behaviors to identify excessive CPU utilization, unbalanced workloads or wrong configurations.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or select from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and is selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type are displayed in a drop-down list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only

Parameters (Continued)	**Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_HV, NT_System_DV, NT_System_WV, NT_System_MV, NT_System_QV,NT_System_YV **Linux agent:** KLZ_CPU_HV, KLZ_CPU_DV, KLZ_CPU_WV, KLZ_CPU_MV, KLZ_CPU_QV,KLZ_CPU_YV **UNIX agent:** System_HV, System_DV, System_WV, System_MV, System_QV, System_YV
Output	Three overlaid line charts for selected systems, with each line representing the different systems. Each chart represents the behavior of a CPU aspect. A table, which can be collapsed, corresponds to each chart.
Usage	The IT administrator or manager responsible for meeting service levels based on server performance needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates which systems are over-utilized or under-utilized relative to a collection of systems. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	On legends to CPU Utilization for Single Resource.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux CPU	KLZ_CPU	X	X	X	X	X	X
Windows	System	NT_System	X	X	X	X	X	X
UNIX	System	System	X	X	X	X	X	X

CPU Utilization for Single Resource

Name	CPU Utilization for Single Resource

Description	This report shows CPU usage details for a specific system. A line chart is used to show the busy and idle CPU time trends. It also provides finer CPU metrics in a table. The time frame for the report data can be determined, in the standard way, by using the Duration and include the shift period parameters. The servers can be selected from a list of available server using the OS Type and Servers parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on the linear trend computed over historical data.
Purpose	Helps identify which systems are experiencing excessive CPU usage.
Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or select from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and is selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type are displayed in a drop-down list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only

Parameters (Continued)	**Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_System_HV, NT_System_DV, NT_System_WV, NT_System_MV, NT_System_QV,NT_System_YV **Linux agent:** KLZ_CPU_HV, KLZ_CPU_DV, KLZ_CPU_WV, KLZ_CPU_MV, KLZ_CPU_QV,KLZ_CPU_YV **UNIX agent:** System_HV, System_DV, System_WV, System_MV, System_QV, System_YV
Output	A line chart showing busy and idle CPU time trends. A line chart showing busy and idle CPU time trends.
Usage	The IT administrator or manager responsible for meeting service levels based on server performance needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates what is the CPU health of a single system systems and if it is over-utilized or under-utilized. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly.
Drill through	None.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux CPU	KLZ_CPU	X	X	X	X	X	X
Windows	System	NT_System	X	X	X	X	X	X
UNIX	System	System	X	X	X	X	X	X

Disk Utilization for Single Resource

Name	Disk Utilization for Single Resource

Description	This report shows the percentage of space usage for the logical disks of a particular server, over a period of time, in an overlaid line chart, along with a table that shows finer details on logical disks usage. The time frame for the report data can be determined, in the standard way, by using the Duration and include the shift period parameters. The server can be selected from a list of available servers by using the OS Type and Servers parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on linear trend computed over historical data.
Purpose	Helps to analyze the disk utilization details of a specific machine.
Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or select from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and is selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type are displayed in a drop-down list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only

Parameters (Continued)	**Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Include remote file systems** For Linux and UNIX systems only, it is possible to include remote file systems, such as NFS file systems, in the computation of the total average space usage percent and the total average space available in MB. **Include pseudo file systems** For Linux and UNIX systems only, it is possible to include the pseudo file systems, such as the proc file system, in the computation of the total average space usage percent and the total average space available in MB. **Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_Logical_Disk_HV, NT_Logical_Disk_DV, NT_Logical_Disk_WV, NT_Logical_Disk_MV, NT_Logical_Disk_QV, NT_Logical_Disk_YV **Linux agent:** KLZ_Disk_HV, KLZ_Disk_DV, KLZ_Disk_WV, KLZ_Disk_MV, KLZ_Disk_QV, KLZ_Disk_YV **UNIX agent:** Disk_HV, Disk_DV, Disk_WV, Disk_MV, Disk_QV, Disk_YV
Output	A line chart showing the average percent space usage plotted against time. A table showing finer disk utilization details.
Usage	The IT administrator or manager responsible for meeting the server service levels, needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates what is the disk utilization health of a single system and which file systems are over-utilized or under-utilized. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly. Note that the percent of disk usage in the report is calculated each time at run time. This approach is different from the approach used in the Tivoli Enterprise Portal Server workspace where the same metrics are instead taken directly from the % Used attribute of the Logical Disk attribute group. Due to the different units used and some rounding applied during the multiple calculations of average, the two values might vary slightly.
Drill through	None.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y

OS Type	Attribute Group	Table	Summarization					
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux DISK	KLZ_DISK	X	X	X	X	X	X
Windows	Logical Disk	NT_Logical_Disk	X	X	X	X	X	X
UNIX	Disk	Disk	X	X	X	X	X	X

Disk Utilization Comparison for Multiple Resources

Name	Disk Utilization Comparison for Multiple Resources
Description	This report shows disk usage details for multiple systems, over a period of time, in two overlaid line charts. The first overlaid line chart shows the total average space usage percent plotted against time. For example, the sum of the average space usage, over a period of time, for all the file systems of a single machine, in respect to the total size of all the file systems. A linear trending feature is also provided for the total average space usage percent and it is based on the selected forecast period. The second line chart shows the total space available in megabytes plotted against time. For example, the sum of all the average space available, over a period of time, for all the file systems of a machine. By clicking on the server names in the charts legends, you can drill-through to see the corresponding Disk Utilization for Single Resource report. The time frame for the report data can be determined, in the standard way, by using the Duration and include the shift period parameters. The servers can be selected from a list of available server using the OS Type and Servers parameters. The forecasts can also be shown for the given period. If set, all the charts show data that ends at that date, and missing samples are determined based on the linear trend computed over historical data.
Purpose	Helps to compare different file system usage behaviors to identify excessive file system utilization.

Parameters	**OS Type** Determines the type of agent to work on and should be selected from the drop-down list with the following items: • Linux • UNIX • Windows **Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or select from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Summarization Type** Determined by Summarization and Pruning and is selected from the drop-down list with the following items: • Daily (Default) • Hourly • Weekly • Monthly • Quarterly • Yearly **Servers** The server or system names for the selected OS Type are displayed in a drop-down list. **Include shift periods** A drop-down list that you can use to select the shift periods to be included. The Peak/Off-Peak Hours period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Shifts (Default) • Peak Hours Only • Off - Peak Hours Only

Parameters (Continued)	**Include vacation periods** A drop-down list that you can use to include or exclude vacation days. The Vacation period terms refer to definitions contained in Summarization and Pruning. The list contains the following options: • All Days (Default) • Work days • Vacation days **Include remote file systems** For Linux and UNIX systems only, it is possible to include remote file systems, such as NFS file systems, in the computation of the total average space usage percent and the total average space available in MB. **Include pseudo file systems** For Linux and UNIX systems only, it is possible to the pseudo file systems, such as the proc file system, in the computation of the total average space usage percent and the total average space available in MB. **Forecast Period** If forecast is enabled, specifies the forecast period. **Forecast** Specifies whether forecast is enabled using a drop-down list. The list contains the following options: • Use forecast • Do not use the forecast
Tables or views used	**General:** KSY_SUMMARIZATION_CONFIG_DV **Windows agent:** NT_Logical_Disk_HV, NT_Logical_Disk_DV, NT_Logical_Disk_WV, NT_Logical_Disk_MV, NT_Logical_Disk_QV, NT_Logical_Disk_YV **Linux agent:** KLZ_Disk_HV, KLZ_Disk_DV, KLZ_Disk_WV, KLZ_Disk_MV, KLZ_Disk_QV, KLZ_Disk_YV **UNIX agent:** Disk_HV, Disk_DV, Disk_WV, Disk_MV, Disk_QV, Disk_YV
Output	Two overlaid line charts are shown for the selected systems, with one line for each selected system that has some historical data stored in the Tivoli Data Warehouse. Each chart represents the behavior of a different file system aspect. A table, which can be collapsed, corresponds to each chart.
Usage	The IT administrator or manager responsible for meeting the server service levels, needs to receive periodic reports showing which servers are at risk of violating Service Level Agreements (SLAs). The report indicates which systems are over-utilized or under-utilized relative to a collection of systems. The report can be run hourly, daily, weekly, monthly, quarterly, and yearly. Note that the percent of disk usage in the report is calculated each time at run time. This approach is different from the approach used in the Tivoli Enterprise Portal Server workspace where the same metrics are instead taken directly from the % Used attribute of the Logical Disk attribute group. Due to the different units used and some rounding applied during the multiple calculations of average, the two values might vary slightly.
Drill through	By clicking on one of the system names on the legends, it is possible to drill through the corresponding Disk Utilization for Single Resource report.

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
All	KSY SUMMARIZATION CONFIG	KSY_ SUMMARIZATION_ CONFIG		X				
Linux	Linux Disk	KLZ_DISK	X	X	X	X	X	X
Windows	Logical Disk	NT_Logical_Disk	X	X	X	X	X	X
UNIX	Disk	Disk	X	X	X	X	X	X

Situations History report

Name	Situations History
Description	This report shows the distribution of situation events status in a pie chart, along with more detailed information on the history of situation events listed in a table. The time frame for the report data can be determined by using Duration.
Purpose	You can use this report to analyze the history of the IBM Tivoli Monitoring situation events.

Parameters	**Date Range** Determines the range of data shown on a report. Provide the value as two border dates (from and to) or selected from the drop-down list with the following options: • All • Date Range (below) • Today • Yesterday • Last 7 days • Last 30 days • Last 90 days • Last 355 days • Current week • Current month • Current Year to Date • Last week • Last month • Last Year **Status** You can apply a filter on the situations event data set by specifying the status in a multi-select value prompt where one or multiple status value can be selected from the following: • Acknowledged • Closed • Open • Reset • Stopped • Unknown **Managed System Filter** You can apply a filter on the situations events data set by specifying a regular expression that the managed system attribute should follow. This filter can contain the two following wildcard characters: the percent sign (%), which matches zero or more characters, and the underscore sign (_), which matches a single character. The default value for the regular expression is the percent sign, and, by default, all the managed system are selected. The escape character for the underscore and percent signs is the backslash character (\). The empty string for the Situation Name Filter can be specified through two single quotation marks (' '). **Situation Name Filter** You can apply a filter on the situations events data set by specifying a regular expression that the situation name attribute should follow. This filter can contain the two following wildcard characters: the percent sign (%), which matches zero or more characters, and the underscore sign (_), which matches a single character. The default value for the regular expression is the percent sign, and, by default, all the situation names are selected. The escape character for the underscore and percent signs is the backslash character (\).
Tables or views used	**General:** CCC Logs: STATUS_HISTORY (Raw Data)
Output	A pie chart showing the distribution of situation events status. A table showing more detailed information on situation status history.

Usage	The IT administrator or manager responsible for meeting the server service levels, needs to receive periodic reports showing which is the situation event status distribution.
Drill through	None

The following table includes information about the historical collection configuration:

OS Type	Attribute Group	Table	Summarization					
			H	D	W	M	Q	Y
CCC Logs	CCC Logs	STATUS_HISTORY						

Creating custom queries and reports

You can create your own queries and reports using the models and reports that have been documented in the subsections above by completing the following steps:

1. Read the instructions for enabling historical collection found in the *Tivoli Enterprise Portal User's Guide*.
2. Check in Table 3 below for the list of the attribute groups that are supported by the data model and are found in the Tivoli Data Warehouse database.
3. Enable historical collection for these supported attribute groups and configure the summarization settings. All of the summarization settings are supported.
4. After the database is populated, use the model leveraging in Query Studio and Report Studio.

Table 3. Attributes groups supported by the data model

Agent	Attribute groups	Tables
Linux	Linux CPU Averages	KLZ_CPU_Averages
	Linux CPU	KLZ_CPU
	Linux Disk	KLZ_Disk
	Linux Network	KLZ_Network
	Linux Process	KLZ_Process
	Linux VM Stats	KLZ_VM_Stats
	Linux Disk IO	KLZ_Disk_IO
	Linux Disk Usage Trends	KLZ_Disk_Usage_Trends
	Linux IO Ext	KLZ_IO_Ext
	Linux NFS Statistics	KLZ_NFS_Statistics
	Linux Process User Info	KLZ_Process_User_Info
	Linux RPC Statistics	KLZ_RPC_Statistics
	Linux Sockets Detail	KLZ_Sockets_Detail
	Linux Sockets Status	KLZ_Sockets_Status
	Linux Swap Rate	KLZ_Swap_Rate
	Linux System Statistics	KLZ_System_Statistics
	Linux User Login	KLZ_User_Login

Table 3. Attributes groups supported by the data model (continued)

Agent	Attribute groups	Tables
UNIX	Disk	Disk
	Network	Network
	Process	Process
	Unix Memory	Unix_Memory
	System	System
	Disk Performance	Disk_Performance
	NFS and RPC Statistics	N_F_S_and_R_P_C_Statistics
	SMP CPU	SMP_CPU
	Solaris Zones	Solaris_Zones
	User	User
Windows	Logical Disk Hourly	NT_Logical_Disk
	Memory Hourly	NT_Memory_64
	Network Interface Hourly	NT_Network_Interface
	Process Hourly	NT_Process_64
	Server Hourly	NT_Server
	System Hourly	NT_Process_64
	ICMP Statistics Hourly	ICMP_Statistics
	IP Statistics Hourly	IP_Statistics
	Cache Hourly	NT_Cache
	Device Dependencies Hourly	NT_Device_Dependencies
	Devices Hourly	NT_Devices
	Event Log Hourly	NT_Event_Log
	Monitored Logs Report Hourly	NT_Monitored_Logs_Report
	Network Port Hourly	NT_Network_Port
	Objects Hourly	NT_Objects
	Paging File Hourly	NT_Paging_File
	Physical Disk Hourly	NT_Physical_Disk
	Printer Hourly	NT_Printer
	Processor Hourly	NT_Processor
	Processor Summary Hourly	NT_Processor_Summary
	Redirector Hourly	NT_Redirector
	Server Work Queues Hourly	NT_Server_Work_Queues_64
	Service Dependencies Hourly	NT_Service_Dependencies
	Services Hourly	NT_Services
	Thread Hourly	NT_Thread
	Print Queue Hourly	Print_Queue
	Process IO Hourly	Process_IO
	TCP Statistics Hourly	TCP_Statistics
	UDP Statistics Hourly	UDP_Statistics

Note: There is a subset of tables that are visible in the model, but cannot be used in custom queries and reports. These tables are contained in the following folders:

- Forecast Hourly
- Forecast Daily
- Forecast Weekly
- Forecast Monthly
- Forecast Quarterly
- Forecast Yearly

Chapter 9. Troubleshooting

This chapter explains how to troubleshoot the IBM Tivoli Monitoring: Windows OS Agent. Troubleshooting, or problem determination, is the process of determining why a certain product is malfunctioning.

Note: You can resolve some problems by ensuring that your system matches the system requirements listed in Chapter 2, "Requirements for the monitoring agent," on page 5.

This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information. Also see "Support information" on page 352 for other problem-solving options.

Gathering product information for IBM Software Support

Before contacting IBM Software Support about a problem you are experiencing with this product, gather the following information that relates to the problem:

Table 4. Information to gather before contacting IBM Software Support

Information type	Description
Log files	Collect trace log files from failing systems. Most logs are located in a `logs` subdirectory on the host computer. See "Trace logging" on page 328 for lists of all trace log files and their locations. See the *IBM Tivoli Monitoring User's Guide* for general information about the IBM Tivoli Monitoring environment.
Operating system	Operating system version number and patch level. Use the systeminfo command to obtain information about the operating system.
Messages	Messages and other information displayed on the screen
Version numbers for IBM Tivoli Monitoring	Version number of the following members of the monitoring environment: • IBM Tivoli Monitoring. Also provide the patch level, if available. • IBM Tivoli Monitoring: Windows OS Agent Use the command *install_dir*\InstallITM\KinCinfo -i.
Screen captures	Screen captures of incorrect output, if any.

Built-in troubleshooting features

The primary troubleshooting feature in the IBM Tivoli Monitoring: Windows OS Agent is logging. *Logging* refers to the text messages and trace data generated by the IBM Tivoli Monitoring: Windows OS Agent. Messages and trace data are sent to a file.

Trace data captures transient information about the current operating environment when a component or application fails to operate as designed. IBM Software Support personnel use the captured trace information to determine the source of an error or unexpected condition. See "Trace logging" on page 328 for more information.

Problem classification

The following types of problems might occur with the IBM Tivoli Monitoring: Windows OS Agent:

- Installation and configuration
- General usage and operation
- Display of monitoring data

This chapter provides symptom descriptions and detailed workarounds for these problems, as well as describing the logging capabilities of the monitoring agent. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information.

Trace logging

Trace logs capture information about the operating environment when component software fails to operate as intended. The principal log type is the RAS (Reliability, Availability, and Serviceability) trace log. These logs are in the English language only. The RAS trace log mechanism is available for all components of IBM Tivoli Monitoring. Most logs are located in a `logs` subdirectory on the host computer. See the following sections to learn how to configure and use trace logging:

- "Principal trace log files" on page 329
- "Examples: using trace logs" on page 331
- "Setting RAS trace parameters" on page 332

Note: The documentation refers to the RAS facility in IBM Tivoli Monitoring as "RAS1".

IBM Software Support uses the information captured by trace logging to trace a problem to its source or to determine why an error occurred. The default configuration for trace logging, such as whether trace logging is enabled or disabled and trace level, depends on the source of the trace logging. Trace logging is always enabled.

Overview of log file management

Table 5 on page 330 provides the names, locations, and descriptions of RAS1 log files. The log file names adhere to the following naming convention:

hostname_product_program_timestamp-nn.log

where:

- *hostname* is the host name of the machine on which the monitoring component is running.
- *product* is the two-character product code. For Monitoring Agent for Windows OS, the product code is nt.
- *program* is the name of the program being run.
- *timestamp* is an 8-character hexadecimal timestamp representing the time at which the program started.
- *nn* is a rolling log suffix. See "Examples of trace logging" on page 329 for details of log rolling.

Examples of trace logging

For example, if a Microsoft Windows monitoring agent is running on computer "server01", the RAS log file for the Monitoring Agent for Windows OS might be named as follows:

```
server01_nt_kntcma_437fc59-01.log
```

For long-running programs, the *nn* suffix is used to maintain a short history of log files for that startup of the program. For example, the kntcma program might have a series of log files as follows:

```
server01_nt_kntcma_437fc59-01.log
server01_nt_kntcma_437fc59-02.log
server01_nt_kntcma_437fc59-03.log
```

As the program runs, the first log (*nn*=01) is preserved because it contains program startup information. The remaining logs "roll." In other words, when the set of numbered logs reach a maximum size, the remaining logs are overwritten in sequence.

Each time a program is started, a new timestamp is assigned to maintain a short program history. For example, if the Monitoring Agent for Windows OS is started twice, it might have log files as follows:

```
server01_nt_kntcma_437fc59-01.log
server01_nt_kntcma_437fc59-02.log
server01_nt_kntcma_437fc59-03.log

server01_nt_kntcma_537fc59-01.log
server01_nt_kntcma_537fc59-02.log
server01_nt_kntcma_537fc59-03.log
```

Each program that is started has its own log file. For example, the Monitoring Agent for Windows OS would have agent logs in this format:

```
server01_nt_kntcma_437fc59-01.log
```

Other logs, such as logs for collector processes and Take Action commands, have a similar syntax as in the following example:

```
server01_nt_kntpgm_447fc59-01.log
```

where **kntpgm** is the program name.

Note: When you communicate with IBM Software Support, you must capture and send the RAS1 log that matches any problem occurrence that you report.

Principal trace log files

Table 5 on page 330 contains locations, file names, and descriptions of trace logs that can help determine the source of problems with agents.

Table 5. Trace log files for troubleshooting agents

System where log is located	File name and path	Description
On the computer that hosts the monitoring agent See "Definitions of variables" on page 331 for descriptions of the variables in the file names in column two.	The RAS1 log files are named *hostname*_nt_*program_timestamp-nn*.log and are located in the *install_dir*\tmaitm6_x64\logs path if you have installed a 64-bit agent, or in the *install_dir*\tmaitm6\logs path if you have installed a 32-bit agent. **Note:** File names for RAS1 logs include a hexadecimal timestamp.	Traces activity of the monitoring agent. **Note:** Other logs, such as logs for Take Action commands (if available), have a similar syntax and are located in this directory path.
	The *.LG0 file is located in the *install_dir*\tmaitm6_x64\logs path if you have installed a 64-bit agent, or in the *install_dir*\tmaitm6\logs path if you have installed a 32-bit agent.	A new version of this file is generated every time the agent is restarted. IBM Tivoli Monitoring generates one backup copy of the *.LG0 file with the tag .LG1. View .LG0 to learn the following details regarding the current monitoring session: • Status of connectivity with the monitoring server. • Situations that were running. • The success or failure status of Take Action commands.
On the Tivoli Enterprise Monitoring Server See "Definitions of variables" on page 331 for descriptions of the variables in the file names in column two.	**On UNIX:** The candle_installation.log file in the *install_dir*/logs path. **On Windows:** The file in the *install_dir*\InstallITM path.	Provides details about products that are installed. **Note:** Trace logging is enabled by default. A configuration step is not required to enable this tracing.
	The Warehouse_Configuration.log file is located in the following path on Windows: *install_dir*\InstallITM.	Provides details about the configuration of data warehousing for historical reporting.
	The RAS1 log file is named *hostname*_ms_*timestamp-nn*.log and is located in the following path: • **On Windows:** *install_dir*\logs • **On UNIX:** *install_dir*/logs **Note:** File names for RAS1 logs include a hexadecimal timestamp **Also on UNIX, a log with a decimal timestamp is provided:** *hostname*_ms_*timestamp*.log and *hostname*_ms_*timestamp*.pid*nnnnn* in the *install_dir*/*logs* path, where *nnnnn* is the process ID number.	Traces activity on the monitoring server.
On the Tivoli Enterprise Portal Server See "Definitions of variables" on page 331 for descriptions of the variables in the file names in column two.	The RAS1 log file is named *hostname*_cq_*timestamp-nn*.log and is located in the following path: • **On Windows:** *install_dir*\logs **Note:** File names for RAS1 logs include a hexadecimal timestamp	Traces activity on the portal server.
	The TEPS_ODBC.log file is located in the following path on Windows: *install_dir*\InstallITM.	When you enable historical reporting, this log file traces the status of the warehouse proxy agent.

Table 5. Trace log files for troubleshooting agents (continued)

System where log is located	File name and path	Description
Definitions of variables for RAS1 logs: • *hostname* is the host name of the machine on which the agent is running. • *install_dir* represents the directory path where you installed the IBM Tivoli Monitoring component. *install_dir* can represent a path on the computer that hosts the monitoring server, the monitoring agent, or the portal server. • *product* is the two-character product code. For Monitoring Agent for Windows OS, the product code is nt. • *program* is the name of the program being run. • *timestamp* is an eight-character hexadecimal timestamp representing the time at which the program started. • *nn* is a rolling log suffix. See "Examples of trace logging" on page 329 for details of log rolling.		

See the *IBM Tivoli Monitoring Installation and Setup Guide* for more information on the complete set of trace logs that are maintained on the monitoring server.

Examples: using trace logs

Typically IBM Software Support applies specialized knowledge to analyze trace logs to determine the source of problems. However, you can open trace logs in a text editor such as **wordpad** to learn some basic facts about your IBM Tivoli Monitoring environment. You can use the **dir** command to list the log files in the *install_dir*/logs directories, sorted by time they were last updated.

Example one

This excerpt shows the typical log for a failed connection between a monitoring agent and a monitoring server with the host name **server1a**:

```
(Thursday, August 11, 2005, 08:21:30-{94C}kdcl0cl.c,105,"KDCL0_ClientLookup") status=1c020006,
    "location server unavailable", ncs/KDC1_STC_SERVER_UNAVAILABLE
(Thursday, August 11, 2005, 08:21:35-{94C}kraarreg.cpp,1157,"LookupProxy") Unable to connect to
    broker at ip.pipe:: status=0, "success", ncs/KDC1_STC_OK
(Thursday, August 11, 2005, 08:21:35-{94C}kraarreg.cpp,1402,"FindProxyUsingLocalLookup") Unable
    to find running CMS on CT_CMSLIST <IP.PIPE:#server1a>
```

Example two

The following excerpts from the trace log *for the monitoring server* show the status of an agent, identified here as "Remote node." The name of the computer where the agent is running is **SERVER5B**:

```
(42C039F9.0000-6A4:kpxreqhb.cpp,649,"HeartbeatInserter") Remote node Primary:SERVER5B:NT is ON-LINE.
. . .
(42C3079B.0000-6A4:kpxreqhb.cpp,644,"HeartbeatInserter") Remote node Primary:SERVER5B:NT is OFF-LINE.
```

Key points regarding the preceding excerpt:

- The monitoring server appends the **NT** product code to the server name to form a unique name (`Primary:SERVER5B:KNT`) for this instance of Monitoring Agent for Windows OS. This unique name enables you to distinguish multiple monitoring products that might be running on **SERVER5B**.
- The log shows when the agent started (ON-LINE) and later stopped (OFF-LINE) in the environment.
- For the sake of brevity an ellipsis (...) represents the series of trace log entries that were generated while the agent was running.
- Between the ON-LINE and OFF-LINE log entries, the agent was communicating with the monitoring server.
- The ON-LINE and OFF-LINE log entries are always available in the trace log. All trace levels that are described in "Setting RAS trace parameters" on page 332 provide these entries.

On Windows, you can use the following alternate method to view trace logs:

1. In the Windows **Start** menu, choose **Program Files > IBM Tivoli Monitoring > Manage Tivoli Monitoring Service**. The Manage Tivoli Enterprise Monitoring Services window is displayed.
2. Right-click a component and select **Advanced > View Trace Log** in the pop-up menu. The program displays the Select Log File window that lists the RAS1 logs for the monitoring agent.
3. Select a log file from the list and click **OK**. You can also use this viewer to access remote logs.

   Note: The viewer converts timestamps in the logs to a readable format.

Setting RAS trace parameters

Objective

Pinpoint a problem by setting detailed tracing of individual components of the monitoring agent and modules.

Background Information

Monitoring Agent for Windows OS uses RAS1 tracing and generates the logs described in Table 5 on page 330. The default RAS1 trace level is ERROR.

RAS1 tracing has control parameters to manage to the size and number of RAS1 logs. Use the procedure described in this section to set the parameters.

Note: The **KBB_RAS1_LOG** parameter also provides for the specification of the log file directory, log file name, and the inventory control file directory and name. Do not modify these values or log information can be lost.

Before you begin

See "Overview of log file management" on page 328 to ensure that you understand log rolling and can reference the correct log files when you managing log file generation.

After you finish

Monitor the size of the **logs** directory. Default behavior can generate a total of 45 to 60 MB for each agent that is running on a computer. For example, each database instance that you monitor could generate 45 to 60 MB of log data. See the "Procedure" section to learn how to adjust file size and numbers of log files to prevent logging activity from occupying too much disk space.

Regularly prune log files other than the RAS1 log files in the **logs** directory. Unlike the RAS1 log files which are pruned automatically, other log types can grow indefinitely, for example, the logs in Table 5 on page 330 that include a process ID number (PID).

Consider using collector trace logs (described in Table 5 on page 330) as an additional source of troubleshooting information.

Procedure

Specify RAS1 trace options in the **KNTENV** file. You also need specify tracing options for kcawd in the environment file, **KCAENV**. You can manually edit the **KNTENV** configuration file to set trace logging:

1. Open the trace options file: *install_dir*\tmaitm6_x64\KNTENV if you have installed a 64-bit agent or *install_dir*\tmaitm6\KNTENV if you have installed a 32-bit agent.

2. Edit the line that begins with **KBB_RAS1=** to set trace logging preferences.

   For example, if you want detailed trace logging, set the Maximum Tracing option:

   ```
   KBB_RAS1=ERROR (UNIT:knt ALL) (UNIT:kra ALL)
   ```

3. Edit the line that begins with **KBB_RAS1_LOG=** to manage the generation of log files:
   - Edit the following parameters to adjust the number of rolling log files and their size.
     - **MAXFILES**: the total number of files that are to be kept for all startups of a given program. Once this value is exceeded, the oldest log files are discarded. Default value is 9.
     - **LIMIT**: the maximum size, in megabytes (MB) of a RAS1 log file. Default value is 5.
   - IBM Software Support might guide you to modify the following parameters:
     - **COUNT**: the number of log files to keep in the rolling cycle of one program startup. Default value is 3.
     - **PRESERVE**: the number of files that are not to be reused in the rolling cycle of one program startup. Default value is 1.

   Note: The **KBB_RAS1_LOG** parameter also provides for the specification of the log file directory, log file name, and the inventory control file directory and name. Do not modify these values or log information can be lost.

4. Restart the monitoring agent so that your changes take effect.

(*Windows only*) **Alternate method to edit trace logging parameters:**

1. Open the Manage Tivoli Enterprise Monitoring Services window.
2. Right-click the icon of the monitoring agent whose logging you want to modify.
3. Select **Advanced** > **Edit Trace Parms**. The Tivoli Enterprise Monitoring Server Trace Parameters window is displayed.
4. Select a new trace setting in the pull-down menu in the **Enter RAS1 Filters** field or type a valid string.

   The selections are as follows:
   - No error tracing. `KBB_RAS1=-none-`
   - General error tracing. `KBB_RAS1=ERROR`
   - Intensive error tracing. `KBB_RAS1=ERROR (UNIT:knt ALL) (UNIT:knz ALL) (UNIT:knl ALL)`
   - Maximum error tracing. `KBB_RAS1=ERROR (UNIT:knt ALL) (UNIT:kra ALL)`

     Note: As this example shows, you can set multiple RAS tracing options in a single statement.

     Note: For more detailed tracing, you can substitute DETAIL for ERROR in the above selections.

5. Modify the value for "Maximum Log Size Per File (MB)" to change the log file size (changes LIMIT value).
6. Modify the value for "Maximum Number of Log Files Per Session" to change the number of logs files per startup of a program (changes COUNT value).
7. Modify the value for "Maximum Number of Log Files Total" to change the number of logs files for all startups of a program (changes MAXFILES value).

8. (*Optional*) Click Y (Yes) in the **KDC_DEBUG Setting** menu to log information that can help you diagnose communications and connectivity problems between the monitoring agent and the monitoring server.

   Note: The **KDC_DEBUG** setting and the Maximum error tracing setting can generate a large amount of trace logging. Use them only temporarily, while you are troubleshooting problems. Otherwise, the logs can occupy excessive amounts of hard disk space.
9. Click **OK**. You see a message reporting a restart of the monitoring agent so that your changes take effect.

Problems and workarounds

The following sections provide symptoms and workarounds for problems that might occur with Monitoring Agent for Windows OS:

- "Installation and configuration troubleshooting" on page 334
- "Agent troubleshooting" on page 338
- "Tivoli Enterprise Portal troubleshooting" on page 341
- "Workspace troubleshooting" on page 343
- "Troubleshooting for remote deployment" on page 342
- "Situation troubleshooting" on page 344

Note: You can resolve some problems by ensuring that your system matches the system requirements listed in Chapter 2, "Requirements for the monitoring agent," on page 5.

This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information.

Installation and configuration troubleshooting

This section provides tables that show solutions for installation, configuration, and uninstallation problems.

Table 6. Problems and solutions for installation and configuration

Problem	Solution
Unable to install the monitoring agent on a Windows 2008 64-bit Enterprise Edition system.	Confirm if you are at the supported level. For more information, see Chapter 2, "Requirements for the monitoring agent," on page 5. Increase the tracing on the Windows OS agent. Set maximum tracing on the agent. For instructions, see "Setting RAS trace parameters" on page 332.

Table 6. Problems and solutions for installation and configuration (continued)

Problem	Solution
A problem can arise when you install and configure a new monitoring agent to a computer where other agents are running as described in this example: • Agents are running on computer and communicating with a Tivoli Enterprise Monitoring Server, called **TEMS1**. • You install a new agent on the same computer and you want this agent to communicate with a different monitoring server, called **TEMS2**. • When you configure the new agent to communicate with **TEMS2**, all the existing agents are re-configured to communicate with **TEMS2**.	You must reconfigure the previously existing agents to restore their communication connection with **TEMS1**. For example, you can right-click the row for a specific agent in the Manage Tivoli Enterprise Monitoring Services, and select **Reconfigure**. See the *IBM Tivoli Monitoring Installation and Setup Guide* for more information on reconfiguration.
After upgrading to v6.2.2 Fix Pack 1, I found an error message in the log file.	Here is the found error message: `(4A952800.001C-458:kraacthi.cpp,985,"parseXMLfile") <0x38C53F0,0x1DB> XMLError: Parse error not well-formed (invalid token) in C:\IBM\ITM\TMAITM6\Primary_NC124022_NT_thresholds.xml, line 13: Could be there are multiple \r in the file (^M)`
Error Message - Could not open DNS registry key	This message is informational only. No action is required. The Windows agent reports the fact that it could not find a registry entry for the DNS Server Event Log. This means that the DNS Server is not installed.
The following problems occur in workspace views: • The Monitored Logs workspace shows a record count of zero (0). • The Event Logs workspace shows no records.	Windows security logging is not turned on by default. Normally, no data is collected in the security log unless the Windows administrator turns it on. The **Record Count = 0** data value that the monitoring agent returns in the Windows monitored logs report confirms that security logging is not turned on.
Diagnosing problems with product browse settings.	When you have problems with browse settings, perform the following steps: 1. Click on **Start > Programs > IBM Tivoli Monitoring > Manage Tivoli Enterprise Monitoring Services**. The Manage Tivoli Enterprise Monitoring Services is displayed. 2. Right-click the Windows agent and select **Browse Settings**. A text window is displayed. 3. Click **Save As** and save the information in the text file. If requested, you can forward this file to IBM Software Support for analysis.
A message similar to "Unable to find running CMS on CT_CMSLIST" in the log file is displayed.	If a message similar to "Unable to find running CMS on CT_CMSLIST" is displayed in the Log file, the agent is not able to connect to the monitoring server. Confirm the following points: • Do multiple network interface cards (NICs) exist on the system? • If multiple NICs exist on the system, find out which one is configured for the monitoring server. Ensure that you specify the correct host name and port settings for communication in the IBM Tivoli Monitoring environment.

Table 6. Problems and solutions for installation and configuration (continued)

Problem	Solution
The system is experiencing high CPU usage after you install or configure Monitoring Agent for Windows OS.	**Agent process:** View the memory usage of the KNTCMA process. If CPU usage seems to be excessive, recycle the monitoring agent. **Network Cards:** The network card configurations can decrease the performance of a system. Each of the stream of packets that a network card receives (assuming it is a broadcast or destined for the under-performing system) must generate a CPU interrupt and transfer the data through the I/O bus. If the network card in question is a bus-mastering card, work can be off-loaded and a data transfer between memory and the network card can continue without using CPU processing power. Bus-mastering cards are generally 32-bit and are based on PCI or EISA bus architectures.
You successfully migrate an OMEGAMON® monitoring agent to IBM Tivoli Monitoring, Version 6.2.0. However, when you configure historical data collection, you see an error message that includes, `Attribute name may be invalid, or attribute file not installed for warehouse agent`.	Install the agent's application support files on the Tivoli Enterprise Monitoring Server, using the following steps: 1. Open the Manage Tivoli Enterprise Monitoring Services window. 2. Right-click the name of the monitoring server. 3. Select **Advanced > Add TEMS Application Support** in the pop-up menu. Add application support if any for any agent that is missing from the list. See in IBM Tivoli Monitoring Installation and Setup Guide for more information on adding application support. Ensure that the agent's application support files are pushed to the system that houses the Warehouse Proxy Agent. The Warehouse Proxy must be able to access the short attribute names for tables and columns. That way, if the longer versions of these names exceed the limits of the Warehouse database, the shorter names can be substituted.

Table 7. General problems and solutions for uninstallation

Problem	Solution
On Windows, uninstallation of IBM Tivoli Monitoring fails to uninstall the entire environment.	Be sure that you follow the general uninstallation process described in the *IBM Tivoli Monitoring Installation and Setup Guide*: 1. Uninstall monitoring agents first, as in the following examples: • Uninstall a single monitoring agent for a specific database. —OR— • Uninstall all instances of a monitoring product, such as IBM Tivoli Monitoring for Databases. 2. Uninstall IBM Tivoli Monitoring. See the *IBM Tivoli Monitoring Troubleshooting Guide* and the section on installation problems for more information on how to remove the entire environment.
The way to remove inactive managed systems (systems whose status is OFFLINE) from the Enterprise navigation tree in the portal is not obvious.	When you want to remove a managed system from the navigation tree, complete the following steps: 1. Click **Enterprise** in the navigation tree. 2. Right-click **Workspace -> Managed System Status**. 3. Right-click the offline managed system and select **Clear offline entry**.

Unique names for monitoring components

You must decide how to name the monitoring agents. This name is intended to uniquely identify that monitoring agent. The agent's default name is composed of three qualifiers:

- Optional instance name
- Machine network host name
- Agent product node type

An agent name truncation problem can occur when the network domain name is included in the network host name portion of the agent name. For example, instead of just the host name myhost1 being used, the resulting host name might be myhost1.acme.north.prod.com. Inclusion of the network domain name causes the agent name in the example above to expand to SERVER1:myhost1.acme.north.prod.com:KXX. This resulting name is 39 characters long. It is truncated to 32 characters resulting in the name SERVER1:myhost1.acme.north.prod.

In general, create names that are short but meaningful within your environment. Use the following guidelines:

- Each name must be unique. One name cannot match another monitoring agent name exactly.
- Each name must begin with an alpha character.
- Do not use blanks or special characters, including $, #, and @.
- Each name must be between 2 and 32 characters in length.
- Monitoring agent naming is case-sensitive on all operating systems.

Create the names by completing the following steps:

1. Open the configuration file for the monitoring agent, which is located in *install_dir*\tmaitm6_x64\K*product_code*CMA.INI if you have installed a 64-bit agent or *install_dir*\tmaitm6\K*product_code*CMA.INI if you have installed a 32-bit agent. For example, the product code for the Monitoring Agent for Windows OS is NT and the file name is KNTCMA.INI.
2. Find the line the begins with **CTIRA_HOSTNAME=**.
3. Type a new name for host name that is a unique, shorter name for the host computer. The final concatenated name including the subsystem name, new host name, and NT, cannot be longer than 32 characters.

   Note: You must ensure that the resulting name is unique with respect to any existing monitoring component that was previously registered with the Tivoli Enterprise Monitoring Server.
4. Save the file.
5. Restart the agent.
6. If you do not find the files mentioned in Step 1, perform the workarounds listed in the next paragraph.

If you do not find the files mentioned in the preceding steps, perform the following workarounds:

1. Change **CTIRA_HOSTNAME** environment variable in the configuration file of the monitoring agent.
   - Find the KNTENV file in the same path mentioned in the preceding row.
2. If you cannot find the **CTIRA_HOSTNAME** environment variable, you must add it to the configuration file of the monitoring agent:

- **On Windows:** Use the **Advanced > Edit Variables** option.

3. Some monitoring agents (for example, the monitoring agent for MQ Series) do not reference the **CTIRA_HOSTNAME** environment variable to generate component names. Check the documentation for the monitoring agent that you are using for information on name generation. If necessary, contact IBM Software Support.

Agent troubleshooting

This section lists problems that might occur with agents.

This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information.

Table 8. Agent problems and solutions

Problem	Solution
The monitoring agent stops with the following error: `Unable to allocate 2147483642 bytes of memory. Agent is terminating...`	Delete the `TMAITM6\logs\khdexp.cfg` file then restart agent. Observe if your agent still terminates and sends the memory allocation error. If after deleting the `khdexp.cfg` file the agent still terminates with the same memory error, remove all the entries in `TMAITM6\logs` then restart the agent. You can move them to a temporary directory if you do not want to delete them. After removing all entries in `TMAITM6\logs` and restarting the agent, observe if your agent still sends the memory allocation error.

Table 8. Agent problems and solutions (continued)

Problem	Solution
A configured and running instance of the monitoring agent is not displayed in the Tivoli Enterprise Portal, but other instances of the monitoring agent on the same system do appear in the portal.	Tivoli Monitoring products use Remote Procedure Call (RPC) to define and control product behavior. RPC is the mechanism that allows a client process to make a subroutine call (such as GetTimeOfDay or ShutdownServer) to a server process somewhere in the network. Tivoli processes can be configured to use TCP/UDP, TCP/IP, SNA, and SSL as the desired protocol (or delivery mechanism) for RPCs. "IP.PIPE" is the name given to Tivoli TCP/IP protocol for RPCs. The RPCs are socket-based operations that use TCP/IP ports to form socket addresses. IP.PIPE implements virtual sockets and multiplexes all virtual socket traffic across a single physical TCP/IP port (visible from the netstat command). A Tivoli process derives the physical port for IP.PIPE communications based on the configured, well-known port for the HUB Tivoli Enterprise Monitoring Server. (This well-known port or BASE_PORT is configured using the 'PORT:' keyword on the KDC_FAMILIES / KDE_TRANSPORT environment variable and defaults to '1918'.) The physical port allocation method is defined as (BASE_PORT + 4096*N) where N=0 for a Tivoli Enterprise Monitoring Server process and N={1, 2, ..., 15} for a non-Tivoli Enterprise Monitoring Server. Two architectural limits result as a consequence of the physical port allocation method: • No more than one Tivoli Enterprise Monitoring Server reporting to a specific Tivoli Enterprise Monitoring Server HUB can be active on a system image. • No more that 15 IP.PIPE processes can be active on a single system image. A single system image can support any number of Tivoli Enterprise Monitoring Server processes (address spaces) provided that each Tivoli Enterprise Monitoring Server on that image reports to a different HUB. By definition, there is one Tivoli Enterprise Monitoring Server HUB per monitoring Enterprise, so this architecture limit has been simplified to one Tivoli Enterprise Monitoring Server per system image. No more that 15 IP.PIPE processes or address spaces can be active on a single system image. With the first limit expressed above, this second limitation refers specifically to Tivoli Enterprise Monitoring Agent processes: no more that 15 agents per system image. This limitation can be circumvented (at current maintenance levels, IBM Tivoli Monitoring V6.1 Fix Pack 4 and later) if the Tivoli Enterprise Monitoring Agent process is configured to use EPHEMERAL IP.PIPE. (This is IP.PIPE configured with the 'EPHEMERAL:Y' keyword in the KDC_FAMILIES / KDE_TRANSPORT environment variable). There is no limitation to the number of ephemeral IP.PIPE connections per system image. If ephemeral endpoints are used, the Warehouse Proxy Agent is accessible from the Tivoli Enterprise Monitoring Server associated with the agents using ephemeral connections either by running the Warehouse Proxy Agent on the same computer or by using the Firewall Gateway feature. (The Firewall Gateway feature relays the Warehouse Proxy Agent connection from the Tivoli Enterprise Monitoring Server computer to the Warehouse Proxy Agent computer if the Warehouse Proxy Agent cannot coexist on the same computer.)

Table 8. Agent problems and solutions (continued)

Problem	Solution

The agent goes off-line when collecting the network port attribute due to reverse DNS look-up time-out.	This agent can hang when querying network ports information and the DNS reverse lookup is disabled. Several errors similar to the following will be logged:
	`(4A7BDB8F.0000-1B90:knt67agt.cpp,243,"TakeSample") gethostbyaddr error <11004> for IP address error <11004> for IP address`
	`(4A7BDB94.0000-1B90:knt67agt.cpp,243,"TakeSample") gethostbyaddr error <11004> for IP address error <11004> for IP address`
	The agent appears to be off-line in the Tivoli Enterprise Portal, and does not report any data for any workspace. The environment variable REVERSE_LOOKUP_ACCEPTED_FAILURES that can be specified in the configuration file allows you to set the number of accepted failures in the reverse lookup. This action can reduce the hang time.

The process application components are available, but the Availability status shows PROCESS_DATA_NOT_ AVAILABLE.	This problem occurs because the PerfProc performance object is disabled. When this condition exists, IBM Tivoli Monitoring cannot collect performance data for this process. Do the following to confirm that this problem exists and resolve it: Choose Run in the Windows Start menu. Type perfmon.exe in the Open field of the Run window. The Performance window is displayed. Click the plus sign (+) in the tool bar located above the right pane. The Add Counters window is displayed. Look for Process in the Performance object pull-down menu. Perform one of the following actions: If you see Process in the pull-down menu, the PerfProc performance object is enabled and the problem is coming from a different source. You might need to contact IBM Software Support. If you do not see Process in the pull-down menu, use the Microsoft utility from the following Web site to enable the PerfProc performance object: `http://blogs.technet.com/mscom/archive/2008/12/18/ the-mystery-of-the-missing-process-performance- counter-in-perfmon.aspx` The Process performance object becomes visible in the Performance object pull-down menu of the Add Counters windows, and IBM Tivoli Monitoring is able to detect Availability data. Restart the monitoring agent.
The CPU of the Monitoring Agent for Windows OS is high	The PerfProc service is typically the one responsible for high CPU. Others, like TCPIP, might also need to be disabled. Using the exctrlst.exe that you can download from the Microsoft site, you can disable the PerfProc and TCPIP services. Run the exctrlst.exe command to bring up the Extensible Counter List, where all of the counters are listed. You can deselect the Performance Counters Enabled box while highlighting PerfProc. Click **Refresh** to save the change. The same method can be used to disable the TCPIP counter. If these two services are stopped, Tivoli Enterprise Portal workspaces or situations based on Process and Network attribute groups will no longer function.
The Long Queue Name is not matched with the row data collected from perfmon.	To allow the Long Queue Name to be matched with the row data collected from perfmon (all the remaining attributes for each MSMQ Queue) the first 63 bytes (characters) of the Queue Name must be unique. This is the only way that the queue name can be matched with the additional metrics that come back from perfmon (the source for the remaining attributes of the queue instance).
When you edit the configuration for an existing monitoring agent, the values displayed are not correct.	The original configuration settings might include non-ASCII characters. These values were stored incorrectly and result in the incorrect display. Enter new values using only ASCII characters.
Attributes do not allow non-ASCII input in the situation editor.	None. Any attribute that does not include "(Unicode)" might support only ASCII characters. For example "Attribute (Unicode)" will support unicode but "Attribute" without "(Unicode)" might only support ASCII characters.

Table 8. Agent problems and solutions (continued)

Problem	Solution
The Windows Agent accesses the root\cimv2 WMI namespace to collect its WMI data. The Security (Access Permissions) for allowing the agent to access these namespaces need to have Enable, Execute Methods, and Provider Write permissions for the Everyone account.	1. Click **Start -> Run**. 2. Type Wmimgmt.msc and click **OK**. 3. Right-click **Wmi Control** and choose properties. 4. Ensure that it says **successfully connected** in the General tab and then choose the Security tab. 5. Select Root folder and then click **Security** at the bottom of the screen. 6. Highlight **Everyone** and then ensure that the 'Enable Account', 'Execute Methods', 'Provider Write' option is Allowed. If it is not, then choose this option. 7. Highlight **Local Service** and then ensure that the 'Provider Write' option is Allowed. If it is not, then choose this option. 8. Click **OK**. 9. Reboot the server once.
No performance data is displayed in workspace views, no data is available for situations, and no data is available for historical logging.	When the Windows operating system detects a problem in one of its extensible performance monitoring DLL files, it marks the DLL as "disabled." Any DLL that is disabled cannot provide performance data through the Windows Performance Monitor interfaces (Perfmon or Performance Monitor APIs). This prevents IBM Tivoli Monitoring agents from gathering data supplied by the disabled DLL. For more information, see Microsoft Support Knowledge Base article 248993 at the following Web address: http://support.microsoft.com/default.aspx?scid=kb;EN-US;248993 Follow the Resolution instructions provided in this article (248993) to re-enable any performance monitoring extension DLL files disabled by Windows. Then, restart the monitoring agent.
Log data accumulates too rapidly.	Check the RAS trace option settings, which are described in “Setting RAS trace parameters” on page 332. The trace options settings that you can set on the `KBB_RAS1=` and `KDC_DEBUG=` lines potentially generate large amounts of data.
The system runs out of memory while the agent is collecting data.	Ensure that you have installed the newest Service Packs for the Microsoft .NET Framework. Depending on the level of the Windows operating system that you are using, the required Service Pack is as follows: • .NET Framework 1.0 SP3 —OR— • .NET Framework 1.1 SP1
Attributes Date Time Last Modified and Date Time Created in the File Change attribute group seem to have their positions switched in the situation editor when specifying a time comparison between these attributes, using the Compare time to a + or - delta function.	This can occur when creating a new situation that uses the attributes of Date Time Last Modified and Date Time Created in the File Change attribute group. If you then select the function Compare time to a + or - delta, it does not show the time attribute that is currently selected. This is working as designed. 'Compare time to a + or - delta' is to compare the current selected time attribute with other available time attributes with a delta, not with the selected time attribute itself. When you select Date Time Last Modified and Date Time Created, the "Time Attribute for Comparison" shows the available time attributes and it seemed as if the attribute names were switched.

Tivoli Enterprise Portal troubleshooting

Table 9 on page 342 lists problems that might occur with the Tivoli Enterprise Portal. This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information.

Table 9. Tivoli Enterprise Portal problems and solutions

Problem	Solution
Historical data collection is unavailable because of incorrect queries in the Tivoli Enterprise Portal.	The column, Sort By, Group By, and First/Last functions are not compatible with the historical data collection feature. Use of these advanced functions will make a query ineligible for historical data collection. Even if data collection has been started, you cannot use the time span feature if the query for the chart or table includes any column functions or advanced query options (Sort By, Group By, First / Last). To ensure support of historical data collection, do not use the Sort By, Group By, or First/Last functions in your queries. See the *IBM Tivoli Monitoring Administrator's Guide* the Tivoli Enterprise Portal online Help for information on the Historical Data Collection function.
When you use a long process name in the situation, the process name is truncated.	Truncation of process names in the portal display is the expected behavior. 64 bytes is the maximum name length.
Data is missing from the physical and logical disk views in the Tivoli Enterprise Portal.	Open a DOS Window, issue "diskperf -y" and then reboot the Windows system.

Troubleshooting for remote deployment

Table 10 lists problems that might occur with remote deployment. This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information.

This section describes problems and solutions for remote deployment and removal of agent software Agent Remote Deploy:

Table 10. Remote deployment problems and solutions

Problem	Solution
While you are using the remote deployment feature to install Monitoring Agent for Windows OS, an empty command window is displayed on the target computer. This problem occurs when the target of remote deployment is a Windows computer. (See the *IBM Tivoli Monitoring Installation and Setup Guide* for more information on the remote deployment feature.)	Do not close or modify this window. It is part of the installation process and will be dismissed automatically.
The removal of a monitoring agent fails when you use the remote removal process in the Tivoli Enterprise Portal desktop or browser.	This problem might happen when you attempt the remote removal process immediately after you have restarted the Tivoli Enterprise Monitoring Server. You must allow time for the monitoring agent to refresh its connection with the Tivoli Enterprise Monitoring Server before you begin the remote removal process.
The attempt to install an additional OS agent on the same machine fails.	On Windows, IBM Tivoli Monitoring does not support more than one OS agent installation on the same machine. You can not use different directories to install more than one OS agent on the same Windows machine.

Workspace troubleshooting

Table 11 shows problems that might occur with workspaces. This chapter provides agent-specific troubleshooting information. See the *IBM Tivoli Monitoring Troubleshooting Guide* for general troubleshooting information.

Table 11. Workspace problems and solutions

Problem	Solution
You see the following message: `KFWITM083W Default link is disabled for the selected object; please verify link and link anchor definitions.`	You see this message because some links do not have default workspaces. Right-click the link to access a list of workspaces to select.
The name of the attribute does not display in a bar chart or graph view.	When a chart or graph view that includes the attribute is scaled to a small size, a blank space is displayed instead of a truncated name. To see the name of the attribute, expand the view of the chart until there is sufficient space to display all characters of the attribute's name.
At the bottom of the views for the Historical Summarized Availability workspace, the Historical Summarized Capacity workspace, and the Historical Summarized Performance workspace, you see the following error: `KFWITM220E Request failed during execution`	Configure historical collection for these workspaces.
You start collection of historical data but the data cannot be seen.	Managing options for historical data collection: • Basic historical data collection populates the Warehouse with raw data. This type of data collection is turned off by default. See Chapter 2, "Requirements for the monitoring agent," on page 5 for information on managing this feature including how to set the interval at which data is collected. By setting a more frequent interval for data collection you reduce the load on the system incurred every time data is uploaded. • You use the Summarization and Pruning monitoring agent to summarize available raw data and store the summarizations in the database. Be aware that summarized data is not displayed until the Summarization and Pruning monitoring agent begins collecting the data. By default, this agent begins collection at 2 AM daily. At that point, data is visible in the workspace view. See the IBM Tivoli Monitoring Administrator's Guide to learn how to modify the default collection settings.
Regular (non-historical) monitoring data fails to be displayed.	Check the formation of the queries you use to gather capture data. For example, look for invalid SQL statements.
The Event Log workspace does not show complete event logs.	To maintain good system response times, the Event Log agent limits collection of events to 500 for each query . You can use the following procedure to control which 500 events are retrieved from the event log: 1. Click the Historical icon (the clock symbol in the upper left of the workspace). 2. Select the time span. 3. Reduce the amount of data that you retrieve, or restrict the time span. For example, you might capture the last 24 hours or you might select **Custom** and choose a shorter time interval.

Table 11. Workspace problems and solutions (continued)

Problem	Solution
The following problems occur in workspace views: • The Monitored Logs workspace shows a record count of zero (0). • The Event Logs workspace shows no records.	Windows security logging is not turned on by default. Normally, no data is collected in the security log unless the Windows administrator turns it on. The **Record Count = 0** data value that the monitoring agent returns in the Windows monitored logs report confirms that security logging is not turned on.
There is no data for a service-type workspace.	Ensure that the service is running. See Appendix B, "Workspaces additional information: requirements and scenarios," on page 367 for more information.
The Agents Management Services workspace provides the wrong IP loopback address in the IP Address column of the Agents' Runtime Status view.	Be aware that the IP loopback address in the Agents' Runtime Status view is for IPv4, instead of IPv6, even in IPv6 environments.

Situation troubleshooting

This section provides information about both specific situation problems and problems with the configuration of situations. See the *IBM Tivoli Monitoring Troubleshooting Guide* for more information about troubleshooting for situations.

Specific situation troubleshooting

Table 12 lists problems that might occur with specific situations.

Table 12. Specific situation problems and solutions

Problem	Solution
There is a high CPU load while any of the following 3 situations are turned on: • NT_Server_Error • NT_Invalid_Login • NT_Event_Log_Full In this case, an event log is receiving a large number of events, and the processing of these events for the enabled situations causes a high CPU load due to reading the events from the log, substituting the event strings in the descriptions, and finally sending them to the Tivoli Enterprise Monitoring Server. The large number of events can contain many duplicate events. Also, the Windows agent process, kntcma.exe, may show high CPU usage during Windows event log processing if a large number of events are being received in any of the Windows Event Logs.	To resolve the high CPU usage, enable a duplicate event throttle that drops duplicate events found during each reading of the event log. Duplicate events are matched based on event ID, type, category, source, and user ID. The description field of the event is not matched, thus any information unique to the description is lost. Select **Advanced -> Edit Parms** and add the desired parameters and values to the Env file. Save the file. Select **Yes** to the recycle agent prompt. The following environment variables can be set in the `KNTENV` file to enable this duplicate event dropping throttle: Apply to all event logs: • NT_LOG_THROTTLE=*x* Apply the following environment variable to each log separately: • NT_{*Event Log Name*}_LOG_THROTTLE=*x* Where: • *x*=0, event drop throttle disabled • *x*=1, drop all duplicate events every read cycle of the event log • *x*>1, drop all duplicate events in groups of *x* every read cycle of the event log For example, if *x*=50 then duplicate events are drop in groups of 50. You must specify the exact name of the event log you want to monitor. The Windows Registry Editor lists the event log name as a key in either of two paths: • *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog* • *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels* The name of the event log is the key listed under the Eventlog or Channels key. For example, the Application event log has the key: • *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application* Applying the Event Log Name to the environment variable, NT_{*Event Log Name*}_LOG_THROTTLE, requires the conversion of any invalid characters within the Event Log Name to a dash (-). Invalid characters include a space ( ), asterisk (*), pound sign (#), vertical bar (|), back slash (\), forward slash (/), colon (:), quote ("), less than sumbol (<), greater than symbol (>), and question mark (?). For example, if the Event Log Name is Microsoft-Windows-TaskScheduler/Operational, then the environment variable to use in the `KNTENV` file would be NT_Microsoft-Windows-TaskScheduler-Operational_LOG_THROTTLE=*x* where *x* is defined above and the forward slash (/) was changed to a dash (-).

Table 12. Specific situation problems and solutions (continued)

Problem	Solution
How do I collapse duplicate records for Event Log Reports (Query View Results) and enable the Event _Log Duplicate_Record_Count attribute?	The Windows Event Log workspace has been updated to include a 'Duplicate Record Count' column. This column by default is always zero unless the duplicate event log record processing is enabled. This enablement can be done on any of the Windows Event Logs. Duplicate events are matched based on event id, type, category, source, and user ID. The description field of the event is not matched, thus any information unique to the description is lost. The following environment variables can be set in the `KNTENV` file to enable the 'Duplicate Record Count' column. Apply to all event logs: • NT_LOG_DUPLICATE=*x* Apply the following environment variable to each log separately: • NT_{*Event Log Name*}_LOG_DUPLICATE=*x* Where: • *x*=0, event report duplicate disabled • *x*=1, event report duplicate enabled You must specify the exact name of the event log you want to monitor. The Windows Registry Editor lists the event log name as a key in either of two paths: • *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog* • *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels* The name of the event log is the key listed under the Eventlog or Channels key. For example, the Application event log has the key: • *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application* Applying the Event Log Name to the environment variable, NT_{*Event Log Name*}_LOG_DUPLICATE, requires the conversion of any invalid characters within the Event Log Name to a dash (-). Invalid characters include a space ( ), asterisk (*), pound sign (#), vertical bar (|), back slash (\), forward slash (/), colon (:), quote ("), less than sumbol (<), greater than symbol (>), and question mark (?). For example, if the Event Log Name is Microsoft-Windows-TaskScheduler/Operational, then the environment variable to use in the `KNTENV` file would be NT_Microsoft-Windows-TaskScheduler-Operational_LOG_DUPLICATE=*x* where *x* is defined above and the forward slash (/) was changed to a dash (-).
You want to change the appearance of situations when they are displayed in a Workspace view.	1. Right-click an item in the Navigation tree. 2. Select **Situations** in the pop-up menu. The Situation Editor window is displayed. 3. Select the situation that you want to modify. 4. Use the **Status** pull-down menu in the lower right of the window to set the status and appearance of the Situation when it triggers. **Note:** This status setting is not related to severity settings in IBM Tivoli Enterprise Console.

Table 12. Specific situation problems and solutions (continued)

Problem	Solution
Situations are triggered in the Tivoli Enterprise Monitoring Server, but events for the situation are not sent to the Tivoli Enterprise Console server. The Tivoli Enterprise Monitoring Server is properly configured for event forwarding, and events for many other situations are sent to the event server.	This condition can occur when a situation is only monitoring the status of other situations. The event forwarding function requires an attribute group reference in the situation in order to determine the correct event class to use in the event. When the situation only monitors other situations, no attribute groups are defined and the event class cannot be determined. Because the event class cannot be determined, no event is sent. This is a limitation of the Tivoli Enterprise Monitoring Server event forwarding function. Situations that only monitor other situations do not send events to the event server.
A situation that is referencing percent disk time returns values that are greater than 100 percent.	Windows Performance Monitoring (perfmon) generates these metrics, including percentage values that sometimes exceed 100. This behavior is determined by the operating system and cannot be changed.
Monitoring activity requires too much disk space.	Check the RAS trace logging settings that are described in "Setting RAS trace parameters" on page 332. For example, trace logs grow rapidly when you apply the **ALL** logging option. Historical logging can consume large amounts of disk space. Be moderate in your use of historical logging.
Monitoring activity requires too many system resources.	Table 13 on page 348 describes the performance impact of specific attribute groups. If possible, decrease your use of the attribute groups that require greater system resources.
A formula that uses mathematical operators is displayed to be incorrect. For example, if you were monitoring Linux, a formula that calculates when **Free Memory** falls under 10 percent of **Total Memory** does not work: `LT #'Linux_VM_Stats.Total_Memory' / 10`	This formula is incorrect because situation predicates support only logical operators. Your formulas cannot have mathematical operators. **Note:** The Situation Editor provides alternatives to math operators. Regarding the example, you can select **% Memory Free** attribute and avoid the need for math operators.
If you are running a Version 350 Monitoring Agent for Windows OS and you choose to alter the views to include a Version 610 UNICODE attribute, be aware that data for this attribute is not displayed and you see a blank column in this view.	To enable Unicode and other features, upgrade the monitoring agent to IBM Tivoli Monitoring, Version 6.2.0.
You see the 'Unable to get attribute name' error in the Tivoli Enterprise Monitoring Server log after creating a situation.	Install the agent's application support files on the Tivoli Enterprise Monitoring Server, using the following steps: 1. Open the Manage Tivoli Enterprise Monitoring Services window. 2. Right-click the name of the monitoring server. 3. Select **Advanced > Add TEMS Application Support** in the pop-up menu. Add application support if any for any agent that is missing from the list. See in IBM Tivoli Monitoring Installation and Setup Guide for more information on adding application support.
Events received at the Tivoli Enterprise Console server from IBM Tivoli Monitoring do not have values for all event attributes (slots) even though the values are visible in workspace views.	The problem is due to a limitation in the IBM Tivoli Monitoring interface code that generates Tivoli Enterprise Console events from situations. The situation results are provided in a chain of buffers of 3000 bytes each. The interface code currently extracts event information from only the first buffer. When situations or agent table data expands in to a second buffer, this additional data is not examined, and it is not included in events sent to the Tivoli Enterprise Console server.

Table 12. Specific situation problems and solutions (continued)

Problem	Solution
Tivoli Enterprise Console events from IBM Tivoli Monitoring 6.2 for IBM Tivoli Monitoring 5.x migrated situations receive parsing errors in the Tivoli Enterprise Console server.	Complete the following two steps: 1. Ensure that you have the IBM Tivoli Monitoring 6.2 Event Sync installed on your Tivoli Enterprise Console server. 2. Obtain updated baroc files from IBM Tivoli Monitoring 6.2 for the monitoring agent's events. Updated baroc files are on the Tivoli Enterprise Monitoring Server in the *CANDLEHOME*/CMS/TECLIB/itm5migr directory.
You are receiving Tivoli Business Systems Management events that cannot be associated due to application_oid and application_class not being set.	The problem is due to IBM Tivoli Monitoring 6.2 sending Tivoli Enterprise Console events for IBM Tivoli Monitoring 5.x migrated situations. These events are not able to set the cited slot values. Replace the agent forwarding script on the Tivoli Enterprise Console server with the version of this file from the Tivoli Enterprise Monitoring Server in the *CANDLEHOME*/CMS/TECLIB/itm5migr directory.

Consider performance impact of each attribute group: Table 13 lists the impact on performance (high, medium, or low) of each attribute group. The multiple-instance attributes have been classified at the lowest level. That is, the performance overhead will increase if you do not specify compare values for one or more key values.

When you want to prevent impact on performance by any of the attribute groups listed in Table 13 you must avoid referencing that attribute group, as suggested in this list:

- Avoid over use of the attribute group.
- Use caution when selecting workspaces that reference the attribute group.
- Avoid over use of the situations that reference the attribute group by using the "Undistributed situations" option in the Situation Editor.
- Use caution when enabling historical reporting that references the attribute group.
- Avoid using the "Auto Refresh" refresh feature in a Workspace because this option causes a refresh of data for all attribute groups.

  Note: If pre-defined situations are running against the NT_Event_Log attribute group, and there is a high frequency of events, enhance the filtering criteria to prevent high CPU utilization.

See the *IBM Tivoli Monitoring User's Guide* for additional information on controlling attribute group usage.

Table 13. Performance Impact by attribute group

Attribute group	High	Medium	Low
Active Server Pages			✓
DHCP Server			✓
DNS Dynamic Update			✓
DNS Memory			✓
DNS Query			✓
DNS WINS			✓
DNS Zone Transfer			✓
FTP Server Statistics			✓

Table 13. Performance Impact by attribute group (continued)

Attribute group	High	Medium	Low
FTP Service			✓
HTTP Content Index			✓
HTTP Service			✓
ICMP Statistics			✓
IIS Statistics			✓
Indexing Service Filter			✓
Indexing Service			✓
IP Statistics			✓
Job Object Details			✓
Job Object		✓	
Mount Point		✓	
MSMQ Information Store			✓
MSMQ Queue			✓
MSMQ Service			✓
MSMQ Sessions			✓
Network Interface			✓
Network Segment			✓
NNTP Commands			✓
NNTP Server			✓
NT_BIOS Information	✓		
NT_Cache			✓
NT_Computer Information	✓		
NT_Device Dependencies		✓	
NT_Devices		✓	
NT_Event Log The performance impact of the NT_Event Log attribute group is high when you display reports in the workspace, due to the time it takes to perform the queries. The performance impact is low when a situation targets a single item in the Event Log attribute group.		✓	
NT_File Change		✓	
NT_File Trend		✓	
NT_IP Address		✓	
NT_Logical Disk			✓
NT_Memory			✓
NT_Monitored Logs			✓
NT_Network Port		✓	
NT_Objects		✓	
NT_Paging File			✓

Table 13. Performance Impact by attribute group (continued)

Attribute group	High	Medium	Low
NT_Physical Disk			✓
NT_Port	✓		
NT_Print Job			✓
NT_Printer			✓
NT_Processor		✓	
NT_Processor_Information		✓	
NT_Processor Summary		✓	
NT_Redirector	✓		
NT_Registry			✓
NT_Server			✓
NT_Server Work Queues			✓
NT_Service Dependencies		✓	
NT_Services		✓	
NT_System			✓
NT_Thread		✓	
Print Queue			✓
Process IO		✓	
RAS Port			✓
RAS Total			✓
SMTP Server			✓
TCP Statistics			✓
UDP Statistics			✓
Web Service			✓

Problems with configuration of situations

Table 14 lists problems that might occur with situations.

This section provides information for troubleshooting for agents. Be sure to consult the *IBM Tivoli Monitoring Troubleshooting Guide* for more general troubleshooting information.

Table 14. Problems with configuring situations that you solve in the Situation Editor

Problem	Solution
Note: To get started with the solutions in this section, perform these steps: 1. Launch the Tivoli Enterprise Portal. 2. Click **Edit > Situation Editor**. 3. In the tree view, choose the agent whose situation you want to modify. 4. Choose the situation in the list. The Situation Editor view is displayed.	
The situation for a specific agent is not visible in the Tivoli Enterprise Portal.	Open the Situation Editor. Access the All managed servers view. If the situation is absent, confirm that application support for Monitoring Agent for Windows OS has been added to the monitoring server. If not, add application support to the server, as described in the *IBM Tivoli Monitoring Installation and Setup Guide.*
The monitoring interval is too long.	Access the Situation Editor view for the situation that you want to modify. Check the **Sampling interval** area in the **Formula** tab. Adjust the time interval as needed.

Table 14. Problems with configuring situations that you solve in the Situation Editor (continued)

Problem	Solution
The situation did not activate at startup.	Manually recycle the situation as follows: 1. Right-click the situation and choose **Stop Situation**. 2. Right-click the situation and choose **Start Situation**. **Note:** You can permanently avoid this problem by placing a check mark in the **Run at Startup** option of the Situation Editor view for a specific situation.
The situation is not displayed.	Click the **Action** tab and check whether the situation has an automated corrective action. This action can occur directly or through a policy. The situation might be resolving so quickly that you do not see the event or the update in the graphical user interface.
An Alert event has not occurred even though the predicate has been properly specified.	Check the logs, reports, and workspaces.
A situation fires on an unexpected managed object.	Confirm that you have distributed and started the situation on the correct managed system.
The product did not distribute the situation to a managed system.	Click the **Distribution** tab and check the distribution settings for the situation.
The situation does not fire. Incorrect predicates are present in the formula that defines the situation. For example, the managed object shows a state that normally triggers a monitoring event, but the situation is not true because the wrong attribute is specified in the formula.	In the **Formula** tab, analyze predicates as follows: 1. Click the *fx* icon in the upper-right corner of the Formula area. The Show formula window is displayed. a. Confirm the following details in the **Formula** area at the top of the window: • The attributes that you intend to monitor are specified in the formula. • The situations that you intend to monitor are specified in the formula. • The logical operators in the formula match your monitoring goal. • The numerical values in the formula match your monitoring goal. b. (*Optional*) Click the **Show detailed formula** check box in the lower left of the window to see the original names of attributes in the application or operating system that you are monitoring. c. Click **OK** to dismiss the Show formula window. 2. (*Optional*) In the Formula area of the **Formula** tab, temporarily assign numerical values that will immediately trigger a monitoring event. The triggering of the event confirms that other predicates in the formula are valid. **Note:** After you complete this test, you must restore the numerical values to valid levels so that you do not generate excessive monitoring data based on your temporary settings.

Table 15. Problems with configuration of situations that you solve in the Workspace area

Problem	Solution
Situation events are not displayed in the Events Console view of the workspace.	Associate the situation with a workspace. **Note:** The situation does not need to be displayed in the workspace. It is sufficient that the situation be associated with any workspace.
You do not have access to a situation.	**Note:** You must have administrator privileges to perform these steps. 1. Select **Edit** > **Administer Users** to access the Administer Users window. 2. In the Users area, select the user whose privileges you want to modify. 3. In the Permissions tab, Applications tab, and Navigator Views tab, select the permissions or privileges that correspond to the user's role. 4. Click **OK**.

Table 15. Problems with configuration of situations that you solve in the Workspace area (continued)

Problem	Solution
A managed system seems to be offline.	1. Select Physical View and highlight the Enterprise Level of the navigator tree. 2. Select **View** > **Workspace** > **Managed System Status** to see a list of managed systems and their status. 3. If a system is offline, check network connectivity and status of the specific system or application.

Table 16. Problems with configuration of situations that you solve in the Manage Tivoli Enterprise Monitoring Services window

Problem	Solution
After an attempt to restart the agents in the Tivoli Enterprise Portal, the agents are still not running.	For UNIX, NetWare, or Windows, log on to the applicable system and perform the appropriate queries.
The Tivoli Enterprise Monitoring Server is not running.	Check the system status and check the appropriate IBM Tivoli Monitoring logs.
The managed objects you created are firing on incorrect managed systems.	Check the managed system distribution on both the situation and the managed object settings sheets.

Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

Online
Go to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions.

IBM Support Assistant
The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, go to http://www.ibm.com/software/support/isa.

Accessing terminology online

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at the following Web address:

http://www.ibm.com/software/globalization/terminology

Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Documentation Central Web site at http://www.ibm.com/tivoli/documentation.

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File &rarrow; Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

Ordering publications

You can order many Tivoli publications online at http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site at http://www.ibm.com/software/tivoli/education.

Tivoli user groups

Tivoli user groups are independent, user-run membership organizations that provide Tivoli users with information to assist them in the implementation of Tivoli Software solutions. Through these groups, members can share information and learn from the knowledge and experience of other Tivoli users. Tivoli user groups include the following members and groups:

- 23,000+ members
- 144+ groups

Access the link for the Tivoli Users Group at www.tivoli-ug.org.

Appendix A. Upgrading for warehouse summarization

The Monitoring Agent for Windows OS made changes to the warehouse collection and summarization characteristics for some agent attribute groups. These changes correct and improve the way warehouse data is summarized, producing more meaningful historical reports. This appendix explains those changes and the implications to your warehouse collection and reporting.

Note: This upgrade is only available from IBM Tivoli Monitoring v6.1.0 to v6.2.1, and is not necessary for upgrading from IBM Tivoli Monitoring v6.2 to v6.2.1.

Warehouse summarization is controlled on a per-table basis. How the rows in each table are summarized is determined by a set of attributes in each table that are designated as primary keys. There is always one primary key representing the monitored resource, and data is minimally summarized based on this value. For all agents, this primary key is represented internally by the column name, ORIGINNODE; however, the external attribute name varies with each monitoring agent.

One or more additional primary keys are provided for each attribute group to further refine the level of summarization for that attribute group. For example, in an OS agent disk attribute group, a primary key might be specified for the logical disk name that allows historical information to be reported for each logical disk in a computer.

Tables in the warehouse

For a monitoring agent, there are two main types of warehouse tables:

- Raw tables:

  These tables contain the raw information reported by a monitoring agent and written to the warehouse by the Warehouse Proxy agent. Raw tables are named for the attribute group that they represent, for example, NT_Services.
- Summary tables:

  These tables contain summarized information based on the raw tables and written to the warehouse by the Summarization and Pruning agent. Summarization provides aggregation results over various reporting intervals, for example, hours, days, and so on. Summary table names are based on the raw table name with an appended suffix, for example, NT_Services_H, NT_Services_D, and so on.

Effects on summarized attributes

When tables are summarized in the warehouse, the summary tables and summary views are created to include additional columns to report summarization information. Table 17 contains a list of the time periods and the suffixes for the summary tables and views.

Table 17. Time periods and suffixes for summary tables and views

Data collection time period	Summary table suffixes	Summary view suffixes
Hourly	_H	_HV

Table 17. Time periods and suffixes for summary tables and views (continued)

Data collection time period	Summary table suffixes	Summary view suffixes
Daily	_D	_DV
Weekly	_W	_WV
Monthly	_M	_MV
Quarterly	_Q	_QV
Yearly	_Y	_YV

Table 18 shows the expansion to summary columns of some of the most commonly used attribute types.

Table 18. Additional columns to report summarization information

Attribute name	Aggregation type	Additional summarization columns
MyGauge	GAUGE	MIN_MyGauge MAX_MyGauge SUM_MyGauge AVG_MyGauge
MyCounter	COUNTER	TOT_MyCounter HI_MyCounter LO_MyCounter LAT_MyCounter
MyProperty	PROPERTY	LAT_Property

These additional columns are provided only for attributes that are not primary keys. In the cases when an existing attribute is changed to be a primary key, the Summarization and Pruning agent no longer creates summarization values for the attributes, but the previously created column names remain in the table with any values already provided for those columns. These columns cannot be deleted from the warehouse database, but as new data is collected, these columns will not contain values. Similarly, when the primary key for an existing attribute has its designation removed, that attribute has new summarization columns automatically added. As new data is collected, it is used to populate these new column values, but any existing summarization records do not have values for these new columns.

The overall effect of these primary key changes is that summarization information is changing. If these changes result in the old summarization records no longer making sense, you can delete them. As a part of warehouse upgrade, summary views are dropped. The views will be recreated by the Summarization and Pruning agent the next time it runs. Dropping and recreating the views ensure that they reflect the current table structure.

Upgrading your warehouse with limited user permissions

The IBM Tivoli Monitoring warehouse agents (Warehouse Proxy and Summarization and Pruning agents) can dynamically adjust warehouse table definitions based on attribute group and attribute information being loaded in to the warehouse. These types of table changes must be done for this monitoring agent for one or both of the following conditions:

- The monitoring agent has added new attributes to an existing attribute group and that attribute group is included in the warehouse.

- The monitoring agent has added a new attribute group and that attribute group is included in the warehouse.

For the warehouse agents to automatically modify the warehouse table definitions, they must have permission to alter warehouse tables. You might not have granted these agents these permissions, choosing instead to manually define the raw tables and summary tables needed for the monitoring agents. Or, you might have granted these permissions initially, and then revoked them after the tables were created.

You have two options to effect the required warehouse table changes during the upgrade process:

- Grant the warehouse agents temporary permission to alter tables

  If using this option, grant the permissions, start historical collection for all the desired tables, allow the Warehouse Proxy agent to add the new data to the raw tables, and allow the Summarization and Pruning agent to summarize data for all affected tables. Then, remove the permission to alter tables
- Make the warehouse table updates manually

  If using this option, you must determine the table structures for the raw and summary tables. If you manually created the tables in the earlier warehouse definition, you already have a methodology and tools to assist you in this effort. You can use a similar technique to update and add new tables for this warehouse migration.

  For a method of obtaining raw table schema, refer to the IBM Redbook,*Tivoli Management Services Warehouse and Reporting*, January 2007, SG24-7290. The chapter that explains warehouse tuning includes a section on creating data tables manually.

Types of table changes

The following types of table changes affect warehouse summarization:

Case 1 - New attribute added to an attribute group and defined as a primary key.

Case 2 - Existing attribute defined as a primary key or had primary key designation removed.

Case 3 - Moving some tables from 4K tablespaces to 8K tablespaces when using DB2 as the warehouse database.

Case 1 and Case 2 are primary key changes. In both cases, new summarization records will not match existing summarized data:

- A new attribute was added to an attribute group and that attribute was defined as a primary key:

  New summarization records will provide more accurate summarization or greater granularity than previous records. Existing summarization records are still available but contain less granular detail if default values are not assigned for the new primary keys.
- An existing attribute was defined as a primary key or the primary key designation was removed:

  If a new key was added, then the new summarization records will provide more accurate summarization or greater granularity than previous records. If a key was removed, then the new summarization records will provide less granularity than previous records, but with the intent of providing more meaningful summarization. Existing summarization records are still available.

Case 3 requires that you move some tables from 4K tablespaces to 8K tablespaces when using DB2 as the warehouse database to avoid errors during summarization and pruning processing.

Table summary

Table 19 provides information to help you determine the effects of primary key and warehouse changes for this monitoring agent. The table shows each attribute group, the current primary keys (in addition to ORIGINNODE) for the attribute group, primary keys that were removed, and whether this table is being included in warehouse reporting.

Table 19. Primary key and warehouse changes for the Monitoring Agent for Windows OS

Attribute group (the attribute group name as it is displayed in the Tivoli Enterprise Portal)	**Current primary keys**	**Removed primary keys**	**Warehoused**
Active_Server_Pages (Active Server Pages)			Yes
DHCP_Server (DHCP Server)			Yes
DNS_Dynamic_Update (DNS Dynamic Update)			Yes
DNS_Memory (DNS Memory)			Yes
DNS_Query (DNS Query)			Yes
DNS_WINS (DNS WINS)			Yes
DNS_Zone_Transfer (DNS Zone Trasnfer)			Yes
FTP_Server_Statistics (FTP Server Statistics)			Yes
FTP_Service (FTP Service)	FTP_Site		Yes
Gopher_Service (Gopher Service)			Yes
HTTP_Content_Index (HTTP Content Index)			Yes
HTTP_Service (HTTP Service)			Yes
ICMP_Statistics (ICMP Statistics)			Yes
IIS_Statistics (IIS Statistics)			Yes
IP_Statistics (IP Statistics)			Yes
Indexing_Service_Filter (Indexing Service Filter)	Index_U		Yes
Indexing_Service (Indexing Service)	Index_U		Yes
Job_Object_Details (Job Object Details)	ID_Process		Yes
Job_Object_Details_64 (Job Object Details)	ID_Process		Yes

Table 19. Primary key and warehouse changes for the Monitoring Agent for Windows OS (continued)

Attribute group (the attribute group name as it is displayed in the Tivoli Enterprise Portal)	Current primary keys	Removed primary keys	Warehoused
Job_Object (Job Object)	Name_U		Yes
MSMQ_Information_Store (MSMQ Information Store)			Yes
MSMQ_Queue (MSMQ Queue)	Queue_Instance		Yes
MSMQ_Service (MSMQ Service)			Yes
MSMQ_Sessions (MSMQ Sessions)	Session		Yes
NNTP_Commands (NNTP Commands)	NNTP_Server		Yes
NNTP_Server (NNTP Server)	NNTP_Server		Yes
NT_BIOS_Information (BIOS Information)			Yes
NT_Cache (Cache)			Yes
NT_Computer_Information (Computer Information)			Yes
NT_Device_Dependencies (Device Dependencies)	Dependency and Device_Name		Yes
NT_Devices (Devices)	Device_Name		Yes
NT_Event_Log (Event Log)	Log_Name_U		Yes
NT_FILE_CHANGE (File Change)	Watch_File_U		No
NT_FILE_TREND (File Trend)	Watch_File_U		No
NT_IP_Address (IP Address)	IP_Address		Yes
NT_Logical_Disk (Logical Disk)	Disk_Name		Yes
NT_Memory (Memory)			Yes
NT_Memory_64 (Memory)	Server_Name		Yes
NT_Monitored_Logs (Monitored Logs)	Log_Name_U		Yes
NT_Mount_Point (Mount Point)			No
NT_Network_Port (Network Port)			Yes
NT_Objects (Objects)			Yes
NT_Paging_File (Paging File)	Pagefile_Name_U		Yes
NT_Physical_Disk (Physical Disk)	Disk_Name		Yes
NT_Print_Job (Print Job)	Document_Name_U Printer_Name_U		Yes

Table 19. Primary key and warehouse changes for the Monitoring Agent for Windows OS (continued)

Attribute group (the attribute group name as it is displayed in the Tivoli Enterprise Portal)	Current primary keys	Removed primary keys	Warehoused
NT_Printer (Printer)	Printer_Name_U		Yes
NT_Processor_Information (Processor Information)			Yes
NT_Processor_Summary (Processor Summary)			Yes
NT_Processor (Processor)	Processor		Yes
NT_Process (Process)	ID_Process		Yes
NT_Process_64 (Process)	ID_Process		Yes
NT_Redirector (Redirector)			Yes
NT_Registry (Registry)		Path_Name Root_Key_Name	No
NT_Server_Work_Queues (Server Work Queues)	Work_Queue_Name		Yes
NT_Server_Work_Queues_64 (Server Work Queues)	Work_Queue_Name		Yes
NT_Server (Server)			Yes
NT_Service_Dependencies (Service Dependencies)	Dependency and Service_Name		Yes
NT_Services (Services)	Service_Name_U and Service_Name		Yes
NT_System (System)			Yes
NT_Thread (Thread)	Thread_Instance		Yes
Network_Interface (Network Interface)	Network_Interface_Instance_ Unicode and Network_Interface_Instance		Yes
Network_Interface_64 (Network Interface)	Network_Interface_Instance		Yes
Network_Segment (Network Segment)	Network_Segment_Instance		Yes
Print_Queue (Print Queue)	Name_U		Yes
Process_IO (Process IO)	ID_Process		Yes
RAS_Port (RAS Port)	Port_Instance		Yes
RAS_Total (RAS Total)			Yes
SMTP_Server (SMTP Server)	SMTP_Server		Yes
TCP_Statistics (TCP Statistics)			Yes
UDP_Statistics (UDP Statistics)			Yes
Web_Service (Web Service)	Web_Site		Yes

Upgrading your warehouse for primary key and tablespace changes

Upgrading your warehouse includes making the following types of changes:

- Case 1 - New attribute is added and is designated as a primary key
  - New attribute and a default value must be added to the raw table and the summarization tables.

    If the attribute group name is not too large for the underlying database, the table name corresponds to the attribute group name. If the attribute group name is too long, a short name is used. The mapping of attribute group names to table names is stored in the WAREHOUSEID table.
  - Case-1 scripts that perform the following actions are provided to assist in this change:
    - Alter existing raw tables
    - Alter existing summary tables
    - Drop existing summary views
  - These changes must be done before the monitoring agent is started and begins exporting data to the Warehouse Proxy agent.
- Case-2 - Existing attributes are changed to either add or remove primary key designation.
  - Existing data is of limited value and should be deleted.
  - Case-2_Truncate scripts that perform the following actions are provided to assist in this change:
    - Remove all records from existing summary tables, preserving existing table definitions
    - Delete the raw data marker allowing raw data to be resummarized
  - Case-2_Drop scripts that perform the following actions are provided to assist in this change:
    - Drop existing summary views
    - Drop existing summary tables
    - Delete the raw data marker allowing raw data to be resummarized
  - These changes are optional, but result in more accurate summarized information.
- Case 3 - Move tables from 4K tablespace to 8K tablespace for selected agents
  - Special processing for selected agents, to move tables from a 4K tablespace to an 8K tablespace.
  - Individual scripts are provided for each summary table to be changed.

Affected attribute groups and supporting scripts

Table 20 shows the attribute groups and summary tables affected for this monitoring agent, the names of the SQL scripts provided to assist in the upgrade process, the types of warehouse databases for which the scripts must be run, and the types of changes (cases) to which the scripts apply.

Table 20. Scripts for affected attribute groups and summary tables for the Monitoring Agent for Windows OS

Attribute group or summary table	File	DB2	Oracle	MS SQL Server	Case 1	Case 2
NT_Services	knt_61migr_Windows_OS_Agent _Case-1.sql	X	X	X	X	

Table 20. Scripts for affected attribute groups and summary tables for the Monitoring Agent for Windows OS (continued)

Attribute group or summary table	File	DB2	Oracle	MS SQL Server	Case 1	Case 2
Network_Interface	knt_61migr_Windows_OS_Agent _Case-1.sql	X	X	X	X	

The following types of warehouse objects are affected by these scripts. Review the scripts before running them:

- Case-1.sql

  These scripts affect raw tables, summary tables, and summary views.
- Case-2_Drop.sql

  These scripts affect the summary tables, summary views, and the Summarization and Pruning agent WAREHOUSEMARKER table.
- Case-2_Truncate.sql

  These scripts affect the summary tables and the Summarization and Pruning agent WAREHOUSEMARKER table.

Procedures

The warehouse can be hosted on any of three databases: DB2, Oracle, or Microsoft SQL Server. There are different sets of script files for each type of database. These scripts are provided as part of the monitoring agent Tivoli Enterprise Portal Server support file installation. After installing the Tivoli Enterprise Portal Server support files for the monitoring agent, the files are located on the Tivoli Enterprise Portal Server computer in *install_dir*/CNPS/SQLLIB/WAREHOUSE. There is a subdirectory for each type of database: DB2 for DB2, Oracle for Oracle, and SQLServer for Microsoft SQL Server.

The scripts provide commands for all affected tables and views. If you do not have summarization enabled for some periods, for example, quarterly or yearly, you will not have the corresponding summary tables (_Q, _Y) and summary views (_QV, _YV) in your warehouse database. If you run the scripts that are provided, the database reports errors for these missing objects. The scripts continue to run the remaining commands. Similarly, if you rerun the scripts, all commands are attempted. If the objects do not exist, or the command cannot be run (especially for the ALTER commands), the scripts continue processing the remaining commands.

DB2 warehouse database procedure

1. Stop *all* running Warehouse Proxy agent instances and the Summarization and Pruning agent.
2. Back up your warehouse database.
3. Copy the scripts from the Tivoli Enterprise Portal Server in one of the following directories to a temporary directory on the system where the warehouse database is located:
   - Windows:

     install dir\CNPS\SQLLIB\WAREHOUSE\DB2
   - UNIX and Linux:

     install dir/*arch*/cq/sqllib/WAREHOUSE/DB2
4. On the system where the warehouse database is located, change to the directory where you placed the script files in Step 3. Then, connect to the

warehouse database through the DB2 command line with a user ID that has the authorization to load and alter tables and drop views. Run commands based on the following example to connect, set the schema, and save the script to an output file:

```
db2 connect to WAREHOUS user ITMUSER using ITMPASS
db2 set current schema="ITMUSER"
db2 -tv -z log/script.sql.log -f script.sql
```

These parameters are used in the example:

- WAREHOUS is the database name.
- ITMUSER is the user name used by the Warehouse Proxy agent.
- ITMPASS is the password used by the Warehouse Proxy agent.
- *script.sql* is the name of the script file. See Table 20 on page 361 for the script file names.
- *script.sql*.log is the name of the output file.

Notes: You might receive error messages such the following from DB2:

- SQL0204N "*schema name.table name*" is an undefined name. SQLSTATE=42704

  This message indicates that the table named *table name* does not exist and cannot be altered or dropped. This happens if you do not have warehousing or summarization enabled for the given table. For example if you only have hourly and daily summarization enabled, you see this message for the weekly, monthly, quarterly, and yearly summarization tables because these tables do not exist.

- SQL3304N The table does not exist.

  This message indicates that the table does not exist and cannot be loaded. This happens if you do not have warehousing or summarization enabled for the given table. For example if you only have hourly and daily summarization enabled, you see this message for the weekly, monthly, quarterly, and yearly summarization tables because these tables do not exist.

Oracle warehouse database procedure

1. Stop *all* running Warehouse Proxy agent instances and the Summarization and Pruning agent.
2. Back up your warehouse database.
3. Copy the scripts from The Tivoli Enterprise Portal Server in one of the following directories to a temporary directory on the system where the warehouse database is located:
   - Windows

     install dir\CNPS\SQLLIB\WAREHOUSE\Oracle
   - UNIX and Linux

     install dir/*arch*/cq/sqllib/WAREHOUSE/Oracle
4. On the system where the warehouse database is located, change to the directory where you placed the script files in Step 3. Then, connect to the warehouse database through the Oracle command line with the same user that the Warehouse Proxy agent uses to connect to the warehouse, and run the script. To run the script, the user ID must have authorization to alter tables and drop views, or to drop tables when using Case 2 Drop, or truncate tables when using Case 2 Truncate. The output is saved to a file named *script name*.log. Run the following command:

```
sqlplus ITMUSER/ITMPASS@WAREHOUS @script.sql
```

These parameters are used in the example:

- WAREHOUS is the connect identifier.
- ITMUSER is the user name used by the Warehouse Proxy agent.
- ITMPASS is the password used by the Warehouse Proxy agent.
- *script.sql* is the name of this script file. See Table 20 on page 361 for the script file names.

Note: You might receive error messages such as the following from Oracle:
```
ORA-00942: table or view does not exist
```

This message indicates that the table does not exist and cannot be altered, dropped, or truncated. This happens if you do not have warehousing or summarization enabled for the given table. For example if you only have hourly and daily summarization enabled, you see this message for the weekly, monthly, quarterly, and yearly summarization tables because these tables do not exist.

MS SQL warehouse database procedure

1. Stop *all* running Warehouse Proxy agent instances and the Summarization and Pruning agent.
2. Back up your warehouse database.
3. Copy the scripts from the Tivoli Enterprise Portal Server in the one of the following directories to a temporary directory on the system where the warehouse database is located:
   - Windows:

     install dir\CNPS\SQLLIB\WAREHOUSE\SQLServer
   - UNIX and Linux:

     install dir/*arch*/cq/sqllib/WAREHOUSE/SQLServer
4. On the system where the warehouse database is located, change to the directory where you placed the script files in Step 3. Then, connect to the warehouse database through the SQL Server command line with the same user that the Warehouse Proxy agent uses to connect to the warehouse, and run the script. To run the script, the user ID must have authorization to alter tables and drop views, or to drop tables when using Case 2 Drop, or truncate tables when using Case 2 Truncate. The output is saved to a file named *script name*.log. Run the following command:

   ```
   osql -I -S SQLHOST[\SQLINST] -U ITMUSER -P ITMPASS -d WAREHOUS
      -m-1 -n -o log/script.sql.log -i script.sql
   ```

   These parameters are used in the example:

   - WAREHOUS is the database name.
   - ITMUSER is the user name used by the Warehouse Proxy agent.
   - ITMPASS is the password used by the Warehouse Proxy agent.
   - *script.sql* is the name of this script file.
   - SQLHOST is the SQL server name.
   - SQLINST is the optional SQL instance name.

Note: You might receive error messages from the SQL Server such as the following: `Msg 4902, Level 16, State 1, Server ENTERPRISE, Line 1 Cannot find the object "table name" because it does not exist or you do not have permissions.`

This message indicates that the table named *table name* does not exist and cannot be dropped or truncated. This happens if you do not have warehousing or summarization enabled for the given table. For example if you only have hourly and daily summarization enabled, you see this message for the weekly, monthly, quarterly, and yearly summarization tables because these tables do not exist.

Appendix B. Workspaces additional information: requirements and scenarios

This appendix provides requirements and scenarios for many of the Monitoring Agent for Windows OS workspaces.

Disk group

The Microsoft Windows disk monitoring command enables and disables data collection for logical and physical disk performance. This command is available in Windows 2000 or higher within a Command Prompt session. In Windows 2000 or higher environments, disk monitoring is disabled by default. In order to collect logical and physical disk performance data in Windows 2000 systems, you must run the disk monitoring command.

Enabling collection of disk performance data

Use this procedure to enable the collecting of disk performance data or to verify that collection is enabled.

Note: Execute DISKPERF -Y when DISKPERF is disabled and when Monitoring Agent for Windows OS displays no data for logical and physical disk performance. For more information about this command, type DISKPERF in a Command Prompt session.

1. Open a Command Prompt session.
2. Run the command DISKPERF -Y.
3. Reboot the server.

Disabling collection of disk performance data

Use this procedure to disable the collecting of disk performance data.

1. Open a Command Prompt session.
2. Run the command DISKPERF -N.
3. Reboot the server.

Logical Disk workspace scenario

A physical hard disk can be partitioned in to one or more logical drives. Some processes write information to the hard disk. If no more space is available because the disk is full, then some process that is running might abort and cause problems with the system.

You can create a situation using the Free Megabytes attribute. This attribute determines the amount of free megabytes of space left on a logical disk. Based on the space required for the particular disk, you can set a threshold for a particular value and get an alert. For example, if, you need to have at least 20 MB of disk space for a process to run, you can set a threshold a little above that and receive an alert if the space drops below 25 MB.

Note: The reporting of the real physical disk number for mounted disks is not supported.

Physical Disk workspace scenario

The two major factors affecting performance in a system are available memory and efficient transfer of data to and from the disk. In database and file systems that do a lot of input and output to disk, it is even more important to measure the rate of disk transfers and to optimize this element of the system.

If the percentage of time a disk drive is busy servicing read or write requests is more than sixty-five percent, make adjustments to the system. If the sustained queue length is greater than two over the current I/O process, you have a bottleneck in the system and need to make changes.

You can use the Disk Reads/Sec and the Disk Writes/Sec attributes in situations to monitor the performance of the physical disk.

Enterprise Services group

Active Server Pages workspace

To see data in this workspace, you must install the Active Server Pages software from the Internet Information Services (IIS) on the managed system.

Scenario

Use the attributes in the Active Server Pages group to create situations that monitor information on Active Server Page requests, session information, and memory allocation.

For example, you can find out the number of requests that failed because of errors, such as connection errors, compile errors, and runtime errors. To do this, you can create a situation using the Request Errors/sec attribute. A situation created with this attribute triggers an alert when the number of requests that are failing reaches a maximum threshold set by you.

Open the Active Server Pages workspace and review the Request Errors/sec field. If the number in this field is high for your environment, you might need to redistribute traffic to another server.

FTP Server Statistics workspace

To see data in this workspace, you must install the FTP Service software from the Internet Information Services (IIS) on the managed system.

Scenario one

Use the attributes in the FTP Server Statistics group to create situations that monitor information on traffic and connection activity.

For example, you can create a situation using the Current Anonymous Users attribute. This situation triggers an alert if the number of users exceeds a maximum threshold set by you.

Open the FTP Server Statistics workspace and check the **Current Anonymous Users** field. A high number in this field indicates that there is a large group of users currently accessing the system.

Scenario two

You can create another situation using the Files Sent and the Files Received attributes. This complex situation monitors the number of files sent by the FTP server and the number of files received by the FTP server.

Open the FTP Server Statistics workspace and review the **Files Sent** field and the **Files Received** field. If both the number of files sent and the number of files received are high, this indicates that the volume of traffic is very high. If this is a daily occurrence, you might need to upgrade your system to accommodate this flow of traffic.

FTP Server workspace

To see data in this workspace, you must install the FTP Service software from the Internet Information Services (IIS) on the managed system.

Scenario one

Use the attributes in the FTP Server group to create situations that monitor information on traffic and connection activity.

For example, you can create a situation using the Current Anonymous Users attribute. This situation triggers an alert if the number of users exceed a maximum threshold set by you.

Open the FTP Server workspace and check the **Current Anonymous Users** field. A high number in this field indicates that there is a large group of users currently accessing the system.

Scenario two

You can create another situation using the Total Files Sent and the Total Files Received attributes. This complex situation monitors the number of files sent by the FTP server and the number of files received by the FTP server.

Open the FTP Server workspace and review the **Total Files Sent** field and the **TotalFiles Received** field. If both the number of files sent and the number of files received are high, this indicates that the volume of traffic is very high. If this is a daily occurrence, you might need to upgrade your system to accommodate this flow of traffic.

HTTP Content Index workspace

To see data in this workspace, you must install the Worldwide Web Service software from the Internet Information Services (IIS) on the managed system.

Scenario

Use the attributes in the HTTP Content Index group to create situations that monitor information on queries received by an HTTP server.

For example, you might create a situation using the Queries Per Minute attribute. A situation created with this attribute sets off an alert when the number of queries taking place per minute exceeds a certain amount.

Open the HTTP Content Index workspace and review the **Queries Per Minute** field. If queries are taking a long time, this indicates that a high number of users are conducting searches.

HTTP Service workspace

To see data in this workspace, you must install Worldwide Web Service software from Internet Information Services (IIS) on the managed system.

Scenario

Use the attributes in the HTTP Service group to create situations that monitor information on traffic and connection activity for an HTTP server.

For example, you can find out the number of requests that failed because a requested document were not found. To do this, you can create a situation using the Not Found Errors attribute. A situation created with this attribute triggers an alert when the number of requests that are failing because of this type of error reaches a maximum threshold set by you.

Open the HTTP Service workspace and review the **Not Found Errors** field. If the number in this field is high for your environment, you might need to determine why this is occurring.

IIS Statistics workspace

To see data in this workspace, you must install Internet Information Services (IIS) on the managed system.

Scenario

Use the attributes in the IIS Server Statistics group to create situations that monitor information on memory usage and connection data for the Internet Information Server.

For example, you can create a situation using the Cache Used attribute. A situation created with this attribute triggers an alert when the total number of bytes containing data in the shared memory cache exceeds a set limit.

Open the IIS Server Statistics workspace and review the **Cache Used** field and the **Cache Size** field. From these two fields, you can determine how much memory you used and what amount of memory is left for you to use.

Also look at the **Cache Hits %** field. This field contains the ratio of cache hits to all cache requests. If this percentage is low, this indicates that there is a problem. Somehow, a high percentage of your cache requests are not succeeding. You might need to increase the size of the memory cache.

Indexing Service workspace

To see data in this workspace, you must install, configure, and start Indexing Service software on the managed system.

Scenario

Windows Indexing Service manages indices used to improve the performance of document searches. This workspace can help identify cases where this service impacts overall performance of the server. For example, if the total size of indices on a system grows too large, they can eventually fill the volumes on which they reside. If this occurs, applications can fail for lack of work space. Monitoring the Index Size (MB) attribute allows you to set a maximum limit on the size of these indices and to disable Indexing Service if this value is exceeded.

Monitoring the Running Queries attribute can help give an indication of how much load is placed on a system by document searches. By comparing this metric

over time, you can improve capacity planning. For example, schedule any upgrades before users see any degradation in service.

MSMQ Information Store workspace

To see data in this workspace, you must install Microsoft Message Queue Service (MSMQ) software on the managed system, and it must be running.

Scenario

Use the attributes in the MSMQ Information Store group to create situations that monitor session information relating to the Information Store.

For example, you can use the Errors Returned to Application attribute in a situation to monitor the total number of MSMQ Information Store accesses that resulted in an error reply by the MSMQ Information Store. You can set the threshold for this situation to a number that is appropriate for your environment.

Open the MSMQ Information Store workspace and check the **Errors Returned to Application** field. If the number is this field is excessive, you might need to try to determine what types of problems are causing this state. The system might be disconnected, or the configuration of the system was modified and messages are not reaching their destination.

MSMQ Queue workspace

To see data in this workspace, you must install Microsoft Message Queue Server (MSMQ) software on the managed system, and it must be running.

Scenario

Use the attributes in the MSMQ Queue group to create situations that monitor message queue data.

For example, you can use the Messages in Queue attribute in combination with the Queue Instance attribute. This situation monitors the total number of messages that currently reside in the queue for this managed system. This queue represents the dead letter queue. You can set the threshold for this situation to a number that is appropriate for your environment.

Open the MSMQ Queue workspace and check the **Messages in Queue** field for a particular managed system. If the number is this field is excessive, you might need to try to determine what types of problems are causing this state. The system might be disconnected, or the configuration of the system was modified and messages are not reaching their destination.

MSMQ Service workspace

To see data in this workspace, you must install Microsoft Message Queue Server (MSMQ) software on the managed system, and it must be running.

Scenario

Use the attributes in the MSMQ Service group to create situations that monitor message Service data.

For example, you can use the Incoming Messages/sec attribute in a situation to monitor the rate of incoming MSMQ messages being handled by the MSMQ Service. You can set the threshold for this situation to a number that is appropriate for your environment.

Open the MSMQ Service workspace and check the **Incoming Messages/sec** field. If the number in this field is high, and if there are a lot of messages in the queue waiting to be processed, this might indicate that system performance is degraded. You might need to upgrade your server to handle the volume of traffic.

MSMQ Sessions workspace

To see data in this workspace, you must install Microsoft Message Queue Service (MSMQ) software on the managed system, and it must be running.

Scenario

Use the attributes in the MSMQ Sessions group to create situations that monitor message data for a particular session.

For example, you can use the Incoming Messages/sec attribute in a situation, along with the Session attribute to monitor the rate of incoming MSMQ messages being handled during a particular session. You can set the threshold for this situation to a number that is appropriate for your environment.

Open the MSMQ Sessions workspace and check the **Incoming Messages/sec** field for that session. If the number is this field is high, and if there are a lot of messages in the queue waiting to be processed, this might indicate that system performance is degraded. You might need to upgrade your server to handle the volume of traffic.

NNTP Commands workspace

To see data in this workspace, you must install NNTP Service software from Internet Information Services (IIS) on the managed system.

Scenario

This workspace lets you monitor the network news message activity of a Windows server running the Network News Transfer Protocol (NNTP). NNTP is a TCP/IP protocol designed to distribute news articles across NNTP servers and clients (newsreaders) on the Internet.

The NTTP Commands workspace helps you monitor the performance of client commands. When users are connecting successfully, the **Logon Failures/Sec** field is zero, and the **Logon Failures** field is a small fraction of the **Logon Attempts** field. If your NNTP server is not available to the public and the **Logon Failures/Sec** field contains a high value, this might indicate that unauthorized users are trying to gain access.

NNTP Server workspace

To see data in this workspace, you must install NNTP Service software from Internet Information Services (IIS) on the managed system.

Scenario

This workspace lets you monitor the network news message activity of a Windows server running the Network News Transfer Protocol (NNTP). NNTP is a TCP/IP protocol designed to distribute news articles across NNTP servers and clients (newsreaders) on the Internet.

The NNTP Server workspace helps you monitor the network performance and activity of the NNTP service. When active users are connected to your Windows 2000 NNTP server, the **Bytes Total/Sec** and **Current Connections** fields must be greater than zero.

SMTP Server workspace

To see data in this workspace, you must install SMTP Service software from Internet Information Services (IIS) on the managed system.

Scenario

This workspace lets you monitor the message activity of a Windows server running the Simple Mail Transfer Protocol (SMTP). SMTP is a TCP/IP protocol that governs the exchange of electronic mail between message transfer agents.

The SMTP Server workspace helps you monitor message processing and connections of your Windows server. The **Local Queue Length** field displays the number of messages that are currently in the local queue. A positive value indicates that the server is receiving more messages than it can process. If the value steadily increases, then something in the server is causing a delay in message processing. The **Inbound Connections Current** field displays the number of connections currently inbound. A value of zero for an extended time can indicate network problems.

Web Service workspace

To see data in this workspace, you must install Worldwide Web Service software from Internet Information Services (IIS) on the managed system.

Scenario

This workspace lets you monitor the performance of a Windows server equipped with Internet Information Server (IIS) software that uses the HTTP Internet protocol to respond to Web client requests on a TCP/IP network.

If you are running one or more Web sites on your Windows server, you can monitor the bandwidth of each Web site individually. Monitoring and adjusting the bandwidth of individual sites assures that bandwidth is available for all the sites sharing the network card. Checking the **Total Connection Attempts** field of this workspace gives you an idea of the overall activity on your site. The **Connection Attempts/sec** field allows you to identify congestion problems at peak times.

Memory group

Cache workspace

Scenario

Use the attributes in the Cache group to create situations that monitor cache statistics.

For example, you can use the Fast Read Resource Misses/sec attribute in a situation to monitor the number of time a process was unable to write data to the disk cache because of the lack of available resources.

You can set the threshold for a situation using this attribute to a high number that is appropriate for your environment.

Open the Cache workspace and check the **Fast Read Resource Misses/sec** field. If the number in this field is high, this might indicate that the size of the disk cache is not adequate for your system. You might need to increase the size of the disk cache.

Memory Overview workspace

Scenario

You can use the Memory Pages/Sec attribute in a situation to monitor system memory. This attribute determines the number of pages read from the disk, or written to the disk, to resolve memory references to pages that were not in RAM at the time of the reference. As a rule, you can assume that if the average of this counter is consistently greater than 5, then memory is probably becoming a bottleneck in the system. When this counter starts to average consistently at 10 or above, performance is significantly degraded and disk thrashing is probably occurring.

If the actual size of the page file is greater than its initial size, time is being spent growing the page file and dealing with page file fragmentation. It is best that the page file not be required to grow during the operation of the system, because it adds time to the paging processes. Additional disk accesses occur to allocate the needed sectors, update any allocation, and free sector tables used by the various file systems.

Another result of this behavior is fragmentation, causing the file to be in non-contiguous areas of the disk. The initial page file is created using contiguous disk space. This fragmentation can grow over time.

Paging File workspace

Paging File Scenario

In a multi-tasking system, it is possible and desirable to have multiple tasks running at the same time. At some point, however, a limit of the available RAM might be reached and some portions of memory swapped to disk in to the paging file.

You can use the % Usage attribute in a situation to ensure that the paging file does not reach its limit. You want the situation to set an alert if the paging file usage reaches 80 percent or higher of its total capacity.

Network group

DHCP Server workspace

To see data in this workspace, you must install DHCP Service software on the managed system, and it must be running.

Scenario

This workspace lets you monitor how your Windows server maintains centralized management of network IP addresses using the Dynamic Host Configuration Protocol (DHCP). DCHP is a TCP/IP service protocol that offers dynamic leased configuration of host IP addresses and distributes other configuration parameters to eligible network clients. DHCP provides safe, reliable, and simple TCP/IP network configuration, prevents address conflicts, and helps conserve the use of client IP addresses over the network.

A large value on the **Packets Received/sec** field indicates that there is heavy DHCP-related message traffic to the server. A large value on the **Packets Expired/sec** field indicates that the server is either taking too long to process some packets while other packets are queued and becoming stale, or traffic on the

network is too high for the server to manage. A large value on the **Declines/sec** field indicates that several clients have found their address to be in conflict, possibly indicating network trouble. A sudden or unusual increase on the **Discovers/sec** field indicates that a large number of clients are attempting to initialize and obtain an IP address lease from the server. This situation might arise when a large number of client computers are started at a given time.

DNS workspaces

To see data in these workspace, you must install DNS Service software on the managed system, and it must be running.

DNS Memory workspace scenario

The DNS workspaces help you monitor the performance of your Windows server as a Domain Name System (DNS) server. DNS is a static, hierarchical name service for TCP/IP hosts. The network administrator configures the DNS with a list of host names and IP addresses, allowing users of workstations configured to query the DNS to specify remote systems by host names rather than IP addresses.

You can use the DNS Memory workspace for measuring system memory usage and memory allocation patterns created by operating the server computer as a Windows 2000 DNS server. You can use the DNS Zone Transfer workspace for measuring all zone transfer (AXFR), incremental zone transfer (IXFR), and DNS zone update notification activity. You can use the DNS Dynamic Update workspace for measuring registration and update activity generated by dynamic clients. You can use the DNS Query workspace for measuring queries and responses when the DNS Server service uses recursion to look up and fully resolve DNS names on behalf of requesting clients. Finally, you can use the DNS WINS workspace for measuring queries and responses made to WINS servers when the WINS lookup integration features of the DNS Server service are used.

ICMP Statistics workspace

There are no special requirements for using this workspace.

Scenario

Use the attributes in the ICMP Statistics group to create situations that monitor information on message traffic.

For example, to find out how many times messages were dropped from transmission, you can create a situation using the Sent Time Exceeded attribute. A situation created with this attribute triggers an alert when the number of times messages are dropped reaches a maximum threshold set by you.

Open the ICMP Statistics workspace and review the **Sent Time Exceeded** field. If the number in this field is high, this indicates that the destination server was not directly accessible and messages are being dropped. You might want to delay sending any additional messages until the destination server is accessible.

IP Statistics workspace

There are no special requirements for using this workspace.

Scenario

Use the attributes in the IP Statistics group to create situations that monitor information on traffic statistics and fragmentation statistics.

For example, if your system is running poorly, you can create a situation using the Datagrams/sec attribute. A situation created with this attribute triggers an alert if the rate of transmission for datagrams being sent and received exceeds a threshold set by you.

You can open the IP Statistics workspace and verify the Datagrams/sec field. If the total is quite large, this indicates that there is a high volume of traffic taking place.

However, if your system is running poorly, and the total rate of transmission is not high, this indicates that some other problem is causing this state.

You might try to analyze system performance during both normal and peak periods, and make adjustments as needed.

Network Interface workspace

There are no special requirements for using this workspace.

Scenario one

Use the attributes in the Network Interface group to create situations that monitor bandwidth statistics and transmission rates.

For example, you can create a situation using the Bytes Received/sec and the Bytes Sent/sec attributes. This situation triggers an alert if the rates that bytes are received and sent per second exceed a set threshold.

Open the Network Interface workspace and verify the **Bytes Received/sec** and the **Bytes Sent/sec** fields. If the rates of transmission are about equal, then you can assume that traffic flow is proceeding smoothly. If the rates are unequal, that is, if the rate that bytes are received is much lower than the rate that bytes are sent, this can indicate a problem in your network interface.

Scenario two

You can also use the Current Bandwidth attribute in a situation to determine an estimate of the current bandwidth for the interface in bits per second (bps). This situation can measure the speed of transmission of your token ring connection.

Open the Network Interface review and review the Current Bandwidth field. If the number is high, this can mean that you are running near capacity. It might be time to upgrade your system. You might also try to redirect traffic elsewhere.

Network Segment workspace

To see data in this workspace, you must install Network Monitor Agent software from Internet Information Services (IIS) on the managed system, and it must be running. This workspace supplies data only for Windows NT systems and earlier.

Scenario

Use the attributes in the Network Segment group to create situations that monitor information on traffic statistics and bandwidth utilization.

For example, you can use the % Network Utilization attribute in a situation to monitor the percentage of network utilization on a particular segment.

Open the Network Segment workspace and check the **% Network Utilization** field. This field indicates how much of the network bandwidth this segment is using.

TCP Statistics workspace

There are no special requirements for using this workspace.

Scenario

Use the attributes in the TCP Statistics group to create situations that monitor information on connection statistics and segment traffic data.

For example, you might create a situation that contains the Connection Failures attribute. When you create a situation with this attribute, an alert is triggered when the number of times TCP/IP connections failed reaches a maximum threshold set by you.

Open the TCP Statistics workspace and review the **Connection Failures** field. A high number in this field lets you know that there is a problem with your TCP/IP connection.

Perhaps your TCP/IP connection was not set up properly. You might try to determine if this is the case. For example, try to issue a PING command to the workstation and see if it succeeds.

UDP Statistics workspace

There are no special requirements for using this workspace.

Scenario

Use the attributes in the UDP Statistics group to create situations that monitor information on datagram statistics.

For example, if your system is running slowly, you can create a situation using the Datagrams/sec attribute. A situation created with this attribute triggers an alert if the rate of transmission for datagrams being sent and received exceeds a threshold set by you.

You can open the UDP Statistics workspace and verify the **Datagrams/sec** field. If the total is large, this indicates that there is a high volume of traffic occurring.

However, if your system is running poorly, and the total rate of transmission is not high, this indicates that some other problem is causing this state. Analyze system performance during both normal and peak periods, and make adjustments as needed.

Printer group

Print Queue workspace scenario

You can use the Jobs attribute in a situation to monitor the number of jobs in the queue for a particular printer. You can also use the Name attribute in this situation to monitor a specific printer.

You can set the threshold for a situation using this attribute to a number that is appropriate for the printer that you are using.

Open the Printers workspace and check the **Jobs** field. If the number in this field is high, this might indicate that too many jobs are in the queue and that your printer is experiencing a problem. ensure that your printer is functioning properly.

Printer Overview workspace scenario

Use the attributes in the Printer group to create situations that monitor the status of the printer that you are using.

For example, you can use the Number of Jobs attribute in a situation to monitor the number of jobs in the queue for a particular printer. You can also use the Printer Name attribute in this situation to monitor a specific printer.

You can set the threshold for a situation using this attribute to a number that is appropriate for the printer that you are using.

Open the Printer Overview workspace and check the **Number of Jobs** field. If the number in this field is high, this might indicate that too many jobs are in the queue and that your printer is experiencing a problem. Ensure that your printer is functioning properly.

Process group

Job Object workspace scenario

This workspace lets you monitor the system resources a job consumes and the number of processes the job contains.

Windows job objects encapsulate Windows processes. Many of the concepts related to the Process workspace can be applied to these objects.

When a Windows job object is running, this workspace contains information about the resource consumption rate of the job. If processes associated with a job begin consuming a large percentage of Kernel Mode time, this might be an indication that those processes are not functioning correctly (and are probably placing the rest of the system under stress). Check the **Current % Kernel Mode Time** field of this workspace. This information can be used to help decide if a job must be cancelled to allow the rest of system to recover and continue providing services.

Job Object Details workspace scenario

This workspace lets you monitor details of individual job objects, including system resources a job consumes and resources used by each of the processes that job contains.

Windows job objects encapsulate Windows processes, so many of the concepts related to Process workspace can be applied to these objects.

When a Windows job object is running, this workspace contains information about the resource consumption rate of job and those processes it contains. Using the Job Object workspace it is possible to identify jobs that might be misbehaving. With the Job Object Details workspace it is possible to identify which process within a job is causing a problem. For example, if you observe that a job is using large amounts of CPU, then this workspace can be used to see which of its processes is using most. (The likelihood is that a single process is consuming resources and locks out all other processes within the job.) This information can be useful in helping a job supplier to isolate and resolve the problem.

Process Overview workspace

The Process Overview workspace displays the percentage of processor time used for a single process on all processors. The total is based on 100 times P, where P is equal to the number of processors in use.

Scenario

This workspace lets you monitor the name of a process, the number of threads that are currently active in a process, and how much time is spent executing instructions in user or in privileged mode.

When a program is running, the Process Overview workspace contains information about the elapsed time that a selected process has been running. If a process were to grab the CPU and not let it go, this might cause problems with other threads that need to run, especially time-sensitive ones like a communications program. Monitor any software that monopolized the CPU by checking for a high value in the **Percent of Processor Time** field of the workspace provides this information.

Note: There is an inconsistency between the way that the NT Process workspace calculates the percentage of processor time used by a process and the way that the Performance Monitor calculates this percentage.

The Process Overview workspace displays the percentage of processor time used for a single process on all processors. The total is based on 100 times P, where P is equal to the number of processors in use.

Processor group

Processor Overview workspace

Scenario

Different devices compete for processor time, and they do so by sending a signal to the CPU to interrupt the current process. It is important that you detect when a device is using an excessive number of interrupts.

To disable this behavior (> 100% for multi-processor system), see the following link:

`http://support.microsoft.com/default.aspx/kb/167050`

You can monitor the number of interrupts per second and identify a device that is using a high number. For example, you can create a situation using the Interrupts/Sec attribute, with the threshold set to a specific limit. This situation triggers an alert when the device interrupts are three thousand per second or higher.

System group

Devices and Device Dependencies workspaces scenario

NT Devices are device drivers and file system drivers run by the operating system as background processes.

Use the attributes in the Devices group to create situations that monitor the status of the device drivers and file system drivers that you are using.

Note: Only the Current State attribute in this group is dynamic. All other attributes are informational and contain static data.

For example, you can use the Current State attribute in a situation to monitor the current state of a particular device. You can also use the Display Name attribute in this situation to monitor a specific device.

Open the Devices workspace and check the **Current State** field. If the current state is Stopped, then the device you are monitoring is experiencing a problem. You might need to determine why this particular device driver stopped running.

File Change workspace scenarios

The main purpose of this workspace is to display changes to files/directories that are currently being monitored by an active subset of your running situations.

Scenario One

Use the attributes in the File Change group to create situations that monitor the latest changes to your files and directories.

For example, to ensure that you are notified when a file is deleted, you might want to create a situation using the Watch File (Unicode) attribute and the Watch Directory (Unicode) attribute in conjunction with the Action attribute. The Action attribute lets you determine the types of changes that recently occurred to a specific file.

A situation created with the Action attribute, and selecting the File Removed value that specifies whether the file being monitored was deleted, triggers an alert when the file is deleted. You can also use this attribute with other settings, to be alerted when a file is removed, modified, or renamed.

Scenario Two

The File Change group of attributes contains the Monitor All Conditions attribute. This powerful attribute combines different types of filter criteria, allowing you to monitor the latest changes to a specific file or to a directory. You use this attribute in a situation that also contains the Watch Directory (Unicode) and Watch File (Unicode) attributes.

You can use the Monitor All Conditions attribute to trigger monitoring for all of the following attributes/conditions:

- Change Attributes: a change in attributes
- Change Create: when a file and directory were created
- Change Directory Name: when a directory was renamed
- Change File Name: when a file was renamed
- Change Last Access: when a file and directory were last accessed
- Change Last Write: when a file and directory were last written to
- Change Security: when the security for a file and directory changed
- Change Size: when the size of a file and directory changed

You can also use the above listed attributes in individual situations to monitor for one or more conditions, such as a recent change to the file name or when a file was last accessed. Then, you can open the File Change workspace to see all of the most recent changes to your files/directories.

File Trend workspace scenarios

Scenario One

You can use the attributes in this group to monitor for file and directory size changes.

For example, you can create a situation using the Watch Directory (Unicode), Watch File (Unicode), Size Change, and Sampling Number attributes to monitor for a change in size in a specific file. If the file increases in size over a threshold set by you, for example, by 10 bytes, the situation triggers an alert.

You can set the sampling interval such that the situation monitors this condition every 10 seconds. Open the settings notebook for the situation and select the **Interval** settings sheet. Choose a monitoring interval for the situation. Make this number small so that you see data quickly.

If you do not want the situation to fire so frequently, you can use an attribute such as % Change Total. The situation triggers an alert only when the percentage of change exceeds the threshold that you set.

Scenario Two

Use the attributes in the File Trend group to create situations that monitor information on file and directory statistics.

For example, you can create a situation using the Watch File (Unicode), Watch Directory (Unicode), and the Free Space Exhausted Hours attributes. A situation created with the Free Space Exhausted Hours attribute triggers an alert before the amount of free space on a volume for a particular file is exhausted. This attribute uses trends to estimate how many hours remain until the free space is used up.

Be aware that this estimate is based solely on the rate of growth for a particular file only. This estimate does not include volume activity for other files that might be running and consuming space on a volume.

Open the File Trend workspace and review the **Free Space Exhausted Hours** field for the file being monitored. If the number in this field is low for your environment, you can move files and directories or delete some files and directories to free up space.

Analyze system performance during both normal and peak periods, and make adjustments as needed.

Monitored Logs and Event Log workspace scenarios

Scenario One

If a DNS Server is installed on your system, you can monitor DNS Server events by checking the DNS Server log. Whenever the DNS Sever starts or stops, an event is sent to the DNS Server log. Other events (conditions) that can be monitored include the DNS Server not being able to open a socket for an address or the Server lacking a primary DNS suffix configuration.

Scenario Two

Each of the different kinds of events logged are valuable and you can monitor them with ease. Security for a system is often a problem. There is an easy way to check to see if someone is trying to break in to a system by trying multiple

passwords. Each time a certain number of attempts to log onto the system fail, a message is produced that is included in the Security log file.

You can set up an alert to notify of any unusual activity by checking the log file and noting which system it is. You can monitor the events and receive timely notification to take precautions.

Scenario Three

If the individual users are using a browser to access an intranet or the Internet, an entry in the System log is created each time the browser is started. If you have a network that can run TCP/IP, you can monitor how many times a particular computer started up this protocol.

Scenario Four

You can monitor application programs that are started by checking the Application log. If the system administrator sets up an anti-virus program to run periodically to scan for viruses in the middle of the night, you can check the Application log to verify that the program ran on schedule.

Objects workspace scenario

This workspace lets you monitor different types of Windows objects using the Objects workspace. Two object types, *Process* and *Thread*, have a particularly close relationship. A Windows process is created when a program runs. Threads are objects within processes that execute program instructions. They allow concurrent operations within a process and enable one process to execute different parts of its program on different processors simultaneously.

You can create a situation using the Processes attribute to monitor the number of active processes on a system at the time of data collection.

Instances of the Process object type appear as numbers if they are internal system processes. Other types of processes are identified by the name of the executable file.

You can also use the Threads attribute in situations to raise alarms on processes.

RAS Port workspace

To see data in this workspace, you must install Remote Access Service (RAS) software from Internet Information Services (IIS) on the managed system, and it must be running.

Scenario

Use the attributes in the RAS Port group to create situations that monitor Remote Access Service statistics.

For example, you can use the Serial Overrun Errors attribute in a situation to monitor the serial overrun errors for this connection. Serial overrun errors occur when the hardware cannot handle the rate at which data is received.

You can set the threshold for a situation using this attribute to a number that is appropriate for your environment.

Open the RAS Port workspace and check the **Serial Overrun Errors** field. If the number in this field is high, this might indicate that system performance is degraded. You might need to upgrade your server to handle the volume of data.

RAS Total workspace

To see data in this workspace, you must install Remote Access Service (RAS) software from Internet Information Services (IIS) on the managed system, and it must be running.

Scenario

Use the attributes in the RAS Total group to create situations that monitor Total Remote Access Service statistics.

For example, you can use the Buffer Overrun Errors attribute in a situation to monitor the total number of buffer overrun errors for a particular connection. Buffer overrun errors occur when the software cannot handle the rate at which data is received.

You can set the threshold for a situation using this attribute to a number that is appropriate for your environment.

Open the RAS Total workspace and check the **Buffer Overrun Errors** field. If the number in this field is high, this might indicate that system performance is degraded. You might need to upgrade your server to handle the volume of data.

Services and Service Dependencies workspace scenario

Use the attributes in the Services group to create situations that monitor the status of the service that you are using.

Note: Only the Current State attribute in this group is dynamic. All other attributes are informational and contain static data.

For example, you can use the Current State attribute in a situation to monitor the current state of a particular service. You can also use the Display Name attribute in this situation to monitor a specific service.

Open the Services workspace and check the **Current State** field. If the current state is Stopped, then the service you are monitoring is experiencing a problem. You might need to determine why this particular service stopped running.

System Overview workspace scenario

A potential problem in a system is for the processor or processors to be overloaded. One measure of the load is the average amount of time the CPU is busy executing instructions. If your CPUs are busy ninety percent of the time or more, consider rearranging the system to prevent it from overloading.

One field in the System Timings workspace is named **Percent Total Processor Time**. If the value displayed in this column reaches 90 percent or more, this might indicate that the CPU is overloaded and the system needs to be changed.

Appendix C. IBM Tivoli Enterprise Console event mapping

Specific event mapping is provided for those monitoring agents that support Distributed Monitoring migration. The specific event mapping creates Distributed Monitoring events for Distributed Monitoring migrated situations. For a list of these situations and their related event classes, see Table 21.

For resource model migration information, see the *IBM Tivoli Monitoring: Upgrading from 5.1.2 Guide*.

Generic event mapping provides useful event class and attribute information for situations that do not have specific event mapping defined. Each event class corresponds to an attribute group in the monitoring agent. For a description of the event slots for each event class, see Table 22 on page 394. For more information about mapping attribute groups to event classes, see the *IBM Tivoli Monitoring Administrator's Guide*.

BAROC files are found on the Tivoli Enterprise Monitoring Server in the installation directory in TECLIB (that is, *installation directory*/cms/TECLIB for Windows systems and *installation directory*/tables/*TEMS_hostname*/TECLIB for UNIX systems). For information on the current version of the BAROC file, see the *IBM Tivoli Monitoring Installation and Setup Guide*. IBM Tivoli Enterprise Console event synchronization provides a collection of ready-to-use rule sets that you can deploy with minimal configuration. Be sure to install IBM Tivoli Enterprise Console event synchronization to access the correct Sentry.baroc, which is automatically included during base configuration of IBM Tivoli Enterprise Console rules if you indicate that you want to use an existing rulebase. See the *IBM Tivoli Monitoring Installation and Setup Guide* for details.

Table 21. Overview of Distributed Monitoring migrated situations

Situation	IBM Tivoli Enterprise Console event class
NT_LDDBPS*	w2k_LogDskDskBytesPerSec
NT_LDDQL*	w2k_LogDskDskQueLen
NT_LDDRBPS*	w2k_LogDskDskRdBytesPerSec
NT_LDDRPS*	w2k_LogDskDskRdPerSec
NT_LDDTPS*	w2k_LogDskDskTranPerSec
NT_LDDWBPS*	w2k_LogDskDskWrBytesPerSec
NT_LDDWPS*	w2k_LogDskDskWrPerSec
NT_LDFM*	w2k_LogDskFreeMegabytes
NT_LDPDRT*	w2k_LogDskPrcDskRdTime
NT_LDPDT*	w2k_LogDskPrcDskTime
NT_LDPDWT*	w2k_LogDskPrcDskWrTime
NT_LDPFS*	w2k_LogDskPrcFreeSpace
NT_NIBRPS*	w2k_NetInterBytesRcvPerSec
NT_NIBSPS*	w2k_NetInterBytesSentPerSec
NT_NIBTPS*	w2k_NetInterBytesTotPerSec
NT_NICB*	w2k_NetInterCurrentBandwidth

Table 21. Overview of Distributed Monitoring migrated situations (continued)

Situation	IBM Tivoli Enterprise Console event class
NT_NIOQL*	w2k_NetInterOutputQueLen
NT_NIPOD*	w2k_NetInterPktsOutDiscarded
NT_NIPOE*	w2k_NetInterPktsOutErrors
NT_NIPRD*	w2k_NetInterPktsRcvDiscarded
NT_NIPRE*	w2k_NetInterPktsRcvErrors
NT_NIPRNUPS*	w2k_NetInterPktsRcvNonUcastPerSec
NT_NIPRUPS*	w2k_NetInterPktsRcvUcastPerSec
NT_NIPRU*	w2k_NetInterPktsRcvUnknown
NT_NIPRPS*	w2k_NetInterPktsRcvPerSec
NT_NIPSNUPS*	w2k_NetInterPktsSentNonUcastPerSec
NT_NIPSUPS*	w2k_NetInterPktsSentUcastPerSec
NT_NIPSPS*	w2k_NetInterPktsSentPerSec
NT_NIPPS*	w2k_NetInterPktsPerSec
NT_PDADBPR*	w2k_PhyDskAvgDskBytesPerRd
NT_PDDBPS*	w2k_PhyDskDskBytesPerSec
NT_PDDQL*"	w2k_PhyDskDskQueLen
NT_PDDRBPS*	w2k_PhyDskDskRdBytesPerSec
NT_PDDRPS*	w2k_PhyDskDskRdPerSec
NT_PDDTPS*	w2k_PhyDskDskTranPerSec
NT_PDDWBPS*	w2k_PhyDskDskWrBytesPerSec
NT_PDDWPS*	w2k_PhyDskDskWrPerSec
NT_PDPDRT*	w2k_PhyDskPrcDskRdTime
NT_PDPDT*	w2k_PhyDskPrcDskTime
NT_PDPDWT*	w2k_PhyDskPrcDskWrTime
NT_CACRPS*	w2k_CacheAsyncCopyRdPerSec
NT_CADMPS*	w2k_CacheAsyncDataMapsPerSec
NT_CAFRPS*	w2k_CacheAsyncFastRdPerSec
NT_CAMDLRPS*	w2k_CacheAsyncMDLRdPerSec
NT_CAPRPS*	w2k_CacheAsyncPinRdPerSec
NT_CCRHP*	w2k_CacheCopyRdHitsPrc
NT_CCRPS*	w2k_CacheCopyRdPerSec
NT_CDFPPS*	w2k_CacheDataFlushPagPerSec
NT_CDFPS*	w2k_CacheDataFlushPerSec
NT_CDMHP*	w2k_CacheDataMapHitsPrc
NT_CDMPPS*	w2k_CacheDataMapPinsPerSec
NT_CDMPS*	w2k_CacheDataMapsPerSec
NT_CFRNPPS*	w2k_CacheFastRdNotPossPerSec
NT_CFRRMPS*	w2k_CacheFastRdResMissPerSec
NT_CFRPS*	w2k_CacheFastRdPerSec
NT_CLWFPS*	w2k_CacheLazyWrFlushPerSec

Table 21. Overview of Distributed Monitoring migrated situations (continued)

Situation	IBM Tivoli Enterprise Console event class
NT_CLWPPS*	w2k_CacheLazyWrPagPerSec
NT_CMDLRHP*	w2k_CacheMDLRdHitsPrc
NT_CMDLRPS*	w2k_CacheMDLRdPerSec
NT_CPRHP*	w2k_CachePinRdHitsPrc
NT_CPRPS*	w2k_CachePinRdPerSec
NT_CSCRPS*	w2k_CacheSyncCopyRdPerSec
NT_CSDMPS*	w2k_CacheSyncDataMapsPerSec
NT_CSFRPS*	w2k_CacheSyncFastRdPerSec
NT_CSMDLRPS*	w2k_CacheSyncMDLRdPerSec
NT_CSPRPS*	w2k_CacheSyncPinRdPerSec
NT_ELApFail*	w2k_Appfailevent
NT_ELApSucc*	w2k_Appsuccevent
NT_ELApErr*	w2k_Apperrevent
NT_ELApEvnt*	w2k_Appevent
NT_ELAppNum*	w2k_Appnumevent
NT_ELApInfo*	w2k_Appinfoevent
NT_ELAppSrc*	w2k_Appinfoevent
NT_ELApWarn*	w2k_Appwarnevent
NT_ELSeFail*	w2k_Secfailevent
NT_ELSeSucc*	w2k_Secsuccevent
NT_ELSeErr*	w2k_Secerrevent
NT_ELSeEvnt*	w2k_Secevent
NT_ELSecNum*	w2k_Secnumevent
NT_ELSeInfo*	w2k_Secinfoevent
NT_ELSecSrc*	w2k_Secinfoevent
NT_ELSeWarn*	w2k_Secwarnevent
NT_ELSyFail*	w2k_Sysfailevent
NT_ELSySucc*	w2k_Syssuccevent
NT_ELSyErr*	w2k_Syserrevent
NT_ELSyEvnt*	w2k_Sysevent
NT_ELSysNum*	w2k_Sysnumevent
NT_ELSyInfo*	w2k_Sysinfoevent
NT_ELSysSrc*	w2k_Sysinfoevent
NT_ELSyWarn*	w2k_Syswarnevent
NT_ICMPMOE*	w2k_ICMPMessagesOutErrors
NT_ICMPMRE*	w2k_ICMPMessagesRcvErrors
NT_ICMPMRPS*	w2k_ICMPMessagesRcvPerSec
NT_ICMPMSPS*	w2k_ICMPMessagesSentPerSec
NT_ICMPMPS*	w2k_ICMPMessagesPerSec
NT_ICMPRAM*	w2k_ICMPRcvAddressMask

Table 21. Overview of Distributed Monitoring migrated situations (continued)

Situation	IBM Tivoli Enterprise Console event class
NT_ICMPRAMR*	w2k_ICMPRcvAddressMaskReply
NT_ICMPRDU*	w2k_ICMPRcvDestUnreachable
NT_ICRERPS*	w2k_ICMPRcvEchoReplyPerSec
NT_ICMPREPS*	w2k_ICMPRcvEchoPerSec
NT_ICMPRPP*	w2k_ICMPRcvParamProb
NT_ICMPRRPS*	w2k_ICMPRcvRedirectPerSec
NT_ICMPRSQ*	w2k_ICMPRcvSrcQuench
NT_ICMPRTE*	w2k_ICMPRcvTimeExceeded
NT_ICRTRPS*	w2k_ICMPRcvTimestampReplyPerSec
NT_ICMPRTPS*	w2k_ICMPRcvTimestampPerSec
NT_ICMPSAM*	w2k_ICMPSentAddressMask
NT_ICMPSAMR*	w2k_ICMPSentAddressMaskReply
NT_ICMPSDU*	w2k_ICMPSentDestUnreachable
NT_ICSERPS*	w2k_ICMPSentEchoReplyPerSec
NT_ICMPSEPS*	w2k_ICMPSentEchoPerSec
NT_ICMPSPP*	w2k_ICMPSentParamProb
NT_ICMPSRPS*	w2k_ICMPSentRedirectPerSec
NT_ICMPSSQ*	w2k_ICMPSentSrcQuench
NT_ICMPSTE*	w2k_ICMPSentTimeExceeded
NT_ICSTRPS*	w2k_ICMPSentTimestampReplyPerSec
NT_ICMPSTPS*	w2k_ICMPSentTimestampPerSec
NT_IPGFPS*	w2k_IPGramsForwardedPerSec
NT_IPGOD*	w2k_IPGramsOutDiscarded
NT_IPGONR*	w2k_IPGramsOutNoRoute
NT_IPGRAE*	w2k_IPGramsRcvAddrErrors
NT_IPGRDPS*	w2k_IPGramsRcvDelPerSec
NT_IPGRD*	w2k_IPGramsRcvDiscarded
NT_IPGRHE*	w2k_IPGramsRcvHeaderErrors
NT_IPGRUP*	w2k_IPGramsRcvUnkProtocol
NT_IPGSPS*	w2k_IPGramsSentPerSec
NT_IPGRPS*	w2k_IPGramsRcvPerSec
NT_IPGPS*	w2k_IPGramsPerSec
NT_IPFRF*	w2k_IPFragReassemFailures
NT_IPFF*	w2k_IPFragFailures
NT_IPFGPS*	w2k_IPFragGramsPerSec
NT_IPFCPS*	w2k_IPFragCreatedPerSec
NT_IPFRPS*	w2k_IPFragReassemPerSec
NT_IPFRPS*	w2k_IPFragRcvPerSec
NT_MAB*	w2k_MemAvailBytes
NT_MCachByt*	w2k_MemCacheBytes

Table 21. Overview of Distributed Monitoring migrated situations (continued)

Situation	IBM Tivoli Enterprise Console event class
NT_MCachBP*	w2k_MemCacheBytesPeak
NT_MCFPS*	w2k_MemCacheFltsPerSec
NT_MCL*	w2k_MemCommitLimit
NT_MCommByt*	w2k_MemCommittedBytes
NT_MDZFPS*	w2k_MemDemZeroFltsPerSec
NT_MFSPTE*	w2k_MemFreeSysPgTableEntries
NT_MPFPS*	w2k_MemPgFltsPerSec
NT_MPRPS*	w2k_MemPgRdPerSec
NT_MPWPS*	w2k_MemPgWrPerSec
NT_MPIPS*	w2k_MemPagesInputPerSec
NT_MPOPS*	w2k_MemPagesOutputPerSec
NT_MPPS*	w2k_MemPagesPerSec
NT_MPNA*	w2k_MemPoolNonpagedAllocs
NT_MPNB*	w2k_MemPoolNonpagedBytes
NT_MPPA*	w2k_MemPoolPagedAllocs
NT_MPPB*	w2k_MemPoolPagedBytes
NT_MPPRB*	w2k_MemPoolPagedResBytes
NT_MSCachRB*	w2k_MemSysCacheResBytes
NT_MSCodeRB*	w2k_MemSysCodeResBytes
NT_MSCTB*	w2k_MemSysCodeTotBytes
NT_MSDRB*	w2k_MemSysDriverResBytes
NT_MSDTB*	w2k_MemSysDriverTotBytes
NT_MTFPS*	w2k_MemTranFltsPerSec
NT_MWCPS*	w2k_MemWrCopiesPerSec
NT_OMutex*	w2k_ObjectsMutexes
NT_OProcess*	w2k_ObjectsProcesses
NT_OSection*	w2k_ObjectsSections
NT_OSemapho*	w2k_ObjectsSemaphores
NT_OThreads*	w2k_ObjectsThreads
NT_PFPU*	w2k_PagingFilePrcUsage
NT_PFPUP*	w2k_PagingFilePrcUsagePeak
NT_PET*	w2k_ProcElapsedTime
NT_PHC*	w2k_ProcHandleCnt
NT_PIDP*	w2k_ProcIDProc
NT_PPFPS*	w2k_ProcPgFltsPerSec
NT_PPFB*	w2k_ProcPgFileBytesPeak
NT_PPFBP*	w2k_ProcPgFileBytesPeak
NT_PPctPriT*	w2k_ProcPrcPrivTime
NT_PPctTim*	w2k_ProcPrcCpuTime
NT_PPctUseT*	w2k_ProcPrcUsrTime

Table 21. Overview of Distributed Monitoring migrated situations (continued)

Situation	IBM Tivoli Enterprise Console event class
NT_PPNB*	w2k_ProcPoolNonpagedBytes
NT_PPPB*	w2k_ProcPoolPagedBytes
NT_PPriBase*	w2k_ProcPriorityBase
NT_PPrivByt*	w2k_ProcPrivateBytes
NT_PTC*	w2k_ProcThreadCnt
NT_PVB*	w2k_ProcVirtBytesPeak
NT_PVBP*	w2k_ProcVirtBytesPeak
NT_PWS*	w2k_ProcWorkingSetPeak
NT_PWSP*	w2k_ProcWorkingSetPeak
NT_PNS*	w2kServices
NT_PAPCBPS*	w2k_CpuAPCBypassesPerSec
NT_PDPCBPS*	w2k_CpuDPCBypassesPerSec
NT_PDPCR*	w2k_CpuDPCRate
NT_PDPCQPS*	w2k_CpuDPCsQuePerSec
NT_PIPS*	w2k_CpuIntsPerSec
NT_PPDPCT*	w2k_CpuPrcDPCTime
NT_PPIT*	w2k_CpuPrcIntTime
NT_PRPctPrT*	w2k_CpuPrcPrivTime
NT_PRPctTim*	w2k_CpuPrcCpuTime
NT_PRPctUsT*	w2k_CpuPrcUsrTime
NT_RFDOPS*	w2k_RedrFileDataOperPerSec
NT_RFROPS*	w2k_RedrFileRdOperPerSec
NT_RFWOPS*	w2k_RedrFileWrOperPerSec
NT_SBRR*	w2k_SrvBlockingReqRej
NT_SBRPS*	w2k_SrvBytesRcvPerSec
NT_SBTPS*	w2k_SrvBytesTotPerSec
NT_SBTPS*	w2k_SrvBytesTransPerSec
NT_SCBQPS*	w2k_SrvCntxtBlocksQuePerSec
NT_SEAP*	w2k_SrvErrorsAccessPerm
NT_SEGA*	w2k_SrvErrorsGrantedAccess
NT_SEL*	w2k_SrvErrorsLogon
NT_SES*	w2k_SrvErrorsSys
NT_SFDS*	w2k_SrvFileDirSearches
NT_SFO*	w2k_SrvFilesOpenedTot
NT_SFOT*	w2k_SrvFilesOpenedTot
NT_SLT*	w2k_SrvLogonTot
NT_SLPS*	w2k_SrvLogonPerSec
NT_SPNB*	w2k_SrvPoolNonpagedBytes
NT_SPNF*	w2k_SrvPoolNonpagedFailures
NT_SPNP*	w2k_SrvPoolNonpagedPeak

Table 21. Overview of Distributed Monitoring migrated situations (continued)

Situation	IBM Tivoli Enterprise Console event class
NT_SPPB*	w2k_SrvPoolPagedBytes
NT_SPPF*	w2k_SrvPoolPagedFailures
NT_SPPP*	w2k_SrvPoolPagedPeak
NT_SSS*	w2k_SrvSrvSessions
NT_SSEO*	w2k_SrvSessionsErroredOut
NT_SSFO*"	w2k_SrvSessionsForcedOff
NT_SSLO*	w2k_SrvSessionsLoggedOff
NT_SSTO*	w2k_SrvSessionsTimedOut
NT_SWIS*	w2k_SrvWorkItemShort
NT_SWQActTh*	w2k_SrvWorkQueActiveThreads
NT_SWQAvaTh*	w2k_SrvWorkQueAvailThreads
NT_SWQAWI*	w2k_SrvWorkQueAvailWorkItems
NT_SWQBWI*	w2k_SrvWorkQueBorrowedWorkItems
NT_SWQBRPS*	w2k_SrvWorkQueBytesRcvPerSec
NT_SWQBSPS*	w2k_SrvWorkQueBytesSentPerSec
NT_SWQBTPS*	w2k_SrvWorkQueBytesTransPerSec
NT_SWQCBQPS*	w2k_SrvWorkQueCntxtBlocksQuePerSec
NT_SWQCC*	w2k_SrvWorkQueCurrentClients
NT_SWQQL*	w2k_SrvWorkQueQueLen
NT_SWQRBPS*	w2k_SrvWorkQueRdBytesPerSec
NT_SWQROPS*	w2k_SrvWorkQueRdOperPerSec
NT_SWQTBPS*	w2k_SrvWorkQueTotBytesPerSec
NT_SWQTOPS*	w2k_SrvWorkQueTotOperPerSec
NT_SWQWIS*	w2k_SrvWorkQueWorkItemShort
NT_SWQWBPS*	w2k_SrvWorkQueWrBytesPerSec
NT_SWQWOPS*	w2k_SrvWorkQueWrOperPerSec
NT_SAFPS*	w2k_SysAlignFixupsPerSec
NT_SCSPS*	w2k_SysCntxtSwtchPerSec
NT_SEDPS*	w2k_SysExceptDispPerSec
NT_SFCBPS*	w2k_SysFileCtrlBytesPerSec"
NT_SFCOPS*	w2k_SysFileCtrlOperPerSec"
NT_SFDOPS*	w2k_SysFileDataOperPerSec
NT_SFRBPS*	w2k_SysFileRdBytesPerSec
NT_SFROPS*	w2k_SysFileRdOperPerSec
NT_SFWBPS*	w2k_SysFileWrBytesPerSec
NT_SFWOPS*	w2k_SysFileWrOperPerSec
NT_SFEPS*	w2k_SysFloatEmulPerSec
NT_SCQL*	w2k_SysCpuQueLen
NT_SRN*	w2k_SysRegistryNumber
NT_SRS*	w2k_SysRegistryString

Table 21. Overview of Distributed Monitoring migrated situations (continued)

Situation	IBM Tivoli Enterprise Console event class
NT_SSCPS*	w2k_SysSysCallsPerSec
NT_SSUT*	w2k_SysSysUpTime
NT_STIPS*	w2k_SysSysUpTime
NT_TCPCA*	w2k_TCPConnActive
NT_TCPCE*	w2k_TCPConnEstablished
NT_TCPCP*	w2k_TCPConnPassive
NT_TCPCR*	w2k_TCPConnReset
NT_TCPSRPS*	w2k_TCPSegRcvPerSec
NT_TCPSRPS*	w2k_TCPSegRetranPerSec
NT_TCPSSPS*	w2k_TCPSegSentPerSec
NT_TCPSPS*	w2k_TCPSegPerSec"
NT_TCSPS*	w2k_ThreadCntxtSwtchPerSec
NT_TET*	w2k_ThreadElapsedTime
NT_TIDP*	w2k_ThreadIDProc
NT_TIDT*	w2k_ThreadIDThread
NT_TPPT*	w2k_ThreadPrcPrivTime
NT_TPCT*	w2k_ThreadPrcCpuTime
NT_TPUT*	w2k_ThreadPrcUsrTime
NT_TPB*	w2k_ThreadPriorityBase
NT_TPC*	w2k_ThreadPriorityCurrent
NT_TSA*	w2k_ThreadStartAddress
NT_TTS*	w2k_ThreadThreadState
NT_TTWR*	w2k_ThreadThreadWaitReason
NT_UDPGNPPS*	w2k_UDPGramsNoPortPerSec
NT_UDPGRE*	w2k_UDPGramsRcvErrors
NT_UDPGRPS*	w2k_UDPGramsRcvPerSec
NT_UDPGSPS*	w2k_UDPGramsSentPerSec
NT_UDPGPS*	w2k_UDPGramsPerSec

To determine what event class is sent when a given situation is triggered, look at the first referenced attribute group in the situation predicate. The event class that is associated with that attribute group is the one that is sent. This is true for both pre-packaged situations and user-defined situations. See the table below for attribute group to event classes and slots mapping information.

For example, if the situation is monitoring the Operating System Type attribute from the NT_System attribute group, the event class that is sent once the situation is triggered is ITM_NT_System.

Note: There are cases where these mappings generate events that are too large for the Tivoli Enterprise Console. In these cases, the event class names and the event slot names are the same, but some of the event slots are omitted.

Each of the event classes is a child of KNT_Base. The KNT_Base event class can be used for generic rules processing for any event from the Monitoring Agent for Windows OS.

Table 22. Overview of attribute groups to event classes and slots

Attribute group	event class and slots
NT_System	ITM_NT_System event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • user_name: STRING • operating_system_type: STRING • operating_system_version: STRING • network_address: STRING • network_address_enum: STRING • network_address_ipv6: STRING • network_address_ipv6_enum: STRING • number_of_processors: INTEGER • number_of_processors_enum: STRING • processor_type: INTEGER • processor_type_enum: STRING • page_size: INTEGER • page_size_enum: STRING • pct__total_privileged_time: INTEGER • pct__total_privileged_time_enum: STRING • pct__total_processor_time: INTEGER • pct__total_processor_time_enum: STRING • pct__total_user_time: INTEGER • pct__total_user_time_enum: STRING • context_switches_per_sec: INTEGER • context_switches_per_sec_enum: STRING • file_control_bytes_per_sec: INTEGER • file_control_bytes_per_sec_enum: STRING • file_control_operations_per_sec: INTEGER • file_control_operations_per_sec: STRING • file_data_operations_per_sec: INTEGER • file_data_operations_per_sec_enum: STRING • file_read_bytes_per_sec: INTEGER • file_read_bytes_per_sec_enum: STRING • file_read_operations_per_sec: INTEGER • file_read_operations_per_sec_enum: STRING • file_write_bytes_per_sec: INTEGER • file_write_bytes_per_sec_enum: STRING • file_write_operations_per_sec: INTEGER • file_write_operations_per_sec_enum: STRING • processor_queue_length: INTEGER • processor_queue_length_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_System (Continued)	• system_calls_per_sec: INTEGER • system_calls_per_sec_enum: STRING • system_up_time: INTEGER • system_up_time_enum: STRING • total_interrupts_per_sec: INTEGER • total_interrupts_per_sec_enum: STRING • alignment_fixups_per_sec: INTEGER • alignment_fixups_per_sec_enum: STRING • exception_dispatches_per_sec: INTEGER • exception_dispatches_per_sec_enum: STRING • floating_emulations_per_sec: INTEGER • floating_emulations_per_sec_enum: STRING • user_name_u: STRING • system_up_days: INTEGER • system_up_days_enum: STRING • total_memory_size: INTEGER • total_memory_size_enum: STRING • page_file_size: INTEGER • page_file_size_enum: STRING • processor_queue_length_excess: INTEGER • processor_queue_length_excess_enum: STRING • network_address_ipv6: STRING • network_address_ipv6_enum: STRING • file_control_bytes_per_sec_64: INTEGER • file_control_bytes_per_sec_64_enum: STRING • file_read_bytes_per_sec_64: INTEGER • file_read_bytes_per_sec_64_enum: STRING • file_write_bytes_per_sec_64: INTEGER • file_write_bytes_per_sec_64_enum: STRING • system_up_time_64: INTEGER • system_up_time_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Memory_64	ITM_NT_Memory_64 event class with these slots: • server_name: STRING • timestamp: STRING • available_bytes: INTEGER • available_bytes_enum: STRING • available_kbytes: INTEGER • available_kbytes_enum: STRING • available_usage_percentage: INTEGER • available_usage_percentage_enum: STRING • cache_bytes: INTEGER • cache_bytes_enum: STRING • cache_bytes_peak: INTEGER • cache_bytes_peak_enum: STRING • cache_kbytes: INTEGER • cache_kbytes_enum: STRING • cache_kbytes_peak: INTEGER • cache_kbytes_peak_enum: STRING • cache_faults_per_sec: INTEGER • cache_faults_per_sec_enum: STRING • cache_usage_percentage: INTEGER • cache_usage_percentage_enum: STRING • commit_avail_kbytes: INTEGER • commit_avail_kbytes_enum: STRING • commit_limit: INTEGER • commit_limit_enum: STRING • commit_limit_kb: INTEGER • commit_limit_kb_enum: STRING • committed_bytes: INTEGER • committed_bytes_enum: STRING • committed_kbytes: INTEGER • committed_kbytes_enum: STRING • pct__committed_bytes_in_use: INTEGER • demand_zero_faults_per_sec: INTEGER • demand_zero_faults_per_sec_enum: STRING • free_system_page_table_entries: INTEGER • free_system_page_table_entries_enum: STRING • memory_usage_percentage: INTEGER • memory_usage_percentage_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Memory_64 (Continued)	• page_faults_per_sec: INTEGER • page_faults_per_sec_enum: STRING • page_reads_per_sec: INTEGER • page_reads_per_sec_enum: STRING • page_writes_per_sec: INTEGER • page_writes_per_sec_enum: STRING • pages_input_per_sec: INTEGER • pages_input_per_sec_enum: STRING • pages_output_per_sec: INTEGER • pages_output_per_sec_enum: STRING • pages_per_sec: INTEGER • pages_per_sec_enum: STRING • pool_nonpaged_allocs: INTEGER • pool_nonpaged_allocs_enum: STRING • pool_nonpaged_bytes: INTEGER • pool_nonpaged_bytes_enum: STRING • pool_nonpaged_kbytes: INTEGER • pool_nonpaged_kbytes_enum: STRING • pool_paged_allocs: INTEGER • pool_paged_allocs_enum: STRING • pool_paged_bytes: INTEGER • pool_paged_bytes_enum: STRING • pool_paged_kbytes: INTEGER • pool_paged_kbytes_enum: STRING • pool_paged_resident_bytes: INTEGER • pool_paged_resident_bytes_enum: STRING • system_cache_resident_bytes: INTEGER • system_cache_resident_bytes_enum: STRING • system_code_total_bytes: INTEGER • system_code_total_bytes_enum: STRING • system_driver_resident_bytes: INTEGER • system_driver_resident_bytes_enum: STRING • system_driver_total_bytes: INTEGER • system_driver_total_bytes_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Memory_64 (Continued)	• total_memory_bytes: INTEGER • total_memory_bytes_enum: STRING • total_memory_kbytes: INTEGER • total_memory_kbytes_enum: STRING • total_memory_mbytes: INTEGER • total_memory_mbytes_enum: STRING • total_working_set_bytes: INTEGER • total_working_set_bytes_enum: STRING • total_working_set_kbytes: INTEGER • total_working_set_kbytes_enum: STRING • total_working_set_usage_percentage: INTEGER • total_working_set_usage_percentage _enum: STRING • transition_faults_per_sec: INTEGER • transition_faults_per_sec_enum: STRING • write_copies_per_sec: INTEGER • write_copies_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Memory	ITM_NT_Memory event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • available_bytes: INTEGER • available_bytes_enum: STRING • cache_bytes: INTEGER • cache_bytes_enum: STRING • cache_bytes_peak: INTEGER • cache_bytes_peak_enum: STRING • cache_faults_per_sec: INTEGER • cache_faults_per_sec_enum: INTEGER • commit_limit: INTEGER • commit_limit_enum: STRING • committed_bytes: INTEGER • committed_bytes_enum: STRING • demand_zero_faults_per_sec: INTEGER • demand_zero_faults_per_sec_enum: STRING • free_system_page_table_entries: INTEGER • free_system_page_table_entries_enum: STRING • page_faults_per_sec: INTEGER • page_faults_per_sec_enum: STRING • page_reads_per_sec: INTEGER • page_reads_per_sec_enum: STRING • page_writes_per_sec: INTEGER • page_writes_per_sec_enum: STRING • pages_input_per_sec: INTEGER • pages_input_per_sec_enum: STRING • pages_output_per_sec: INTEGER • pages_output_per_sec_enum: STRING • pages_per_sec: INTEGER • pages_per_sec_enum: STRING • pool_paged_allocs: INTEGER • pool_paged_allocs_enum: STRING • pool_paged_bytes: INTEGER • pool_paged_bytes_enum: STRING • pool_nonpaged_allocs: INTEGER • pool_nonpaged_allocs_enum: STRING • pool_nonpaged_bytes: INTEGER • pool_nonpaged_bytes_enum: STRING • transition_faults_per_sec: INTEGER • transition_faults_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Memory (continued)	• write_copies_per_sec: INTEGER • write_copies_per_sec_enum: STRING • available_kbytes: INTEGER • available_kbytes_enum: STRING • cache_kbytes: INTEGER • cache_kbytes_enum: INTEGER • cache_kbytes_peak: INTEGER • cache_kbytes_peak_enum: INTEGER • commit_limit_kb: INTEGER • commit_limit_kb_enum: INTEGER • committed_kbytes: INTEGER • committed_kbytes_enum: INTEGER • pool_paged_kbytes: INTEGER • pool_paged_kbytes_enum: INTEGER • pool_nonpaged_kbytes: INTEGER • pool_nonpaged_kbytes_enum: INTEGER • pool_paged_resident_bytes: INTEGER • pool_paged_resident_bytes_enum: STRING • system_cache_resident_bytes: INTEGER • system_cache_resident_bytes_enum: STRING • system_code_total_bytes: INTEGER • system_code_total_bytes_enum: STRING • system_driver_resident_bytes: INTEGER • system_driver_resident_bytes_enum: STRING • system_driver_total_bytes: INTEGER • system_driver_total_bytes_enum: STRING • total_working_set_bytes: INTEGER • total_working_set_bytes_enum: STRING • total_working_set_usage_percentage: INTEGER • total_working_set_usage_percentage_enum : STRING • cache_usage_percentage: INTEGER • cache_usage_percentage_enum: STRING • available_usage_percentage: INTEGER • available_usage_percentage_enum: STRING • memory_usage_percentage: INTEGER • memory_usage_percentage_enum: STRING • commit_avail_kbytes: INTEGER • commit_avail_kbytes_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Memory (continued)	• pct__committed_bytes_in_use: INTEGER • total_working_set_kbytes: INTEGER • total_working_set_kbytes_enum: STRING • total_memory_bytes: INTEGER • total_memory_bytes_enum: STRING • total_memory_kbytes: INTEGER • total_memory_kbytes_enum: STRING • total_memory_mbytes: INTEGER • total_memory_mbytes_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Logical_Disk	ITM_NT_Logical_Disk event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • disk_name: STRING • pct__disk_read_time: INTEGER • pct__disk_time: INTEGER • pct__disk_write_time: INTEGER • avg_disk_ms_per_read: INTEGER • avg_disk_ms_per_read_enum: STRING • disk_bytes_per_sec: INTEGER • disk_bytes_per_sec_enum: STRING • disk_queue_length: INTEGER • disk_queue_length_enum: STRING • disk_read_bytes_per_sec: INTEGER • disk_read_bytes_per_sec_enum: STRING • disk_reads_per_sec: INTEGER • disk_reads_per_sec_enum: STRING • disk_transfers_per_sec: INTEGER • disk_transfers_per_sec_enum: STRING • disk_writes_per_sec: INTEGER • disk_writes_per_sec_enum: STRING • disk_write_bytes_per_sec: INTEGER • disk_write_bytes_per_sec_enum: STRING • free_megabytes: INTEGER • free_megabytes_enum: STRING • total_size: INTEGER • pct__used: INTEGER • pct__free: INTEGER • physical_disk_number: STRING • physical_disk_number_enum: STRING • avg_disk_queue_length: REAL • avg_disk_queue_length_enum: STRING • avg_disk_read_queue_length: REAL • avg_disk_read_queue_length_enum: STRING • avg_disk_write_queue_length: REAL • avg_disk_write_queue_length_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Logical_Disk (Continued)	• disk_bytes_per_sec_64: INTEGER • disk_bytes_per_sec_64_enum: STRING • disk_read_bytes_per_sec_64: INTEGER • disk_read_bytes_per_sec_64_enum: STRING • disk_write_bytes_per_sec_64: INTEGER • disk_write_bytes_per_sec_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Physical_Disk	ITM_NT_Physical_Disk event class with these slots: • server_name: STRING • timestamp: STRING • disk_name: STRING • pct__disk_read_time: INTEGER • pct__disk_time: INTEGER • pct__disk_write_time: INTEGER • avg_disk_bytes_per_read: INTEGER • avg_disk_bytes_per_read_enum: STRING • disk_bytes_per_sec: INTEGER • disk_bytes_per_sec_enum: STRING • disk_queue_length: INTEGER • disk_queue_length_enum: STRING • disk_read_bytes_per_sec: INTEGER • disk_read_bytes_per_sec_enum: STRING • disk_reads_per_sec: INTEGER • disk_reads_per_sec_enum: STRING • disk_transfers_per_sec: INTEGER • disk_transfers_per_sec_enum: INTEGER • disk_writes_per_sec: INTEGER • disk_writes_per_sec_enum: STRING • disk_write_bytes_per_sec: INTEGER • disk_write_bytes_per_sec_enum: STRING • pct__disk_idle_time: INTEGER • disk_number: STRING • avg_disk_bytes_per_write: INTEGER • avg_disk_bytes_per_write_enum: STRING • avg_disk_bytes_per_transfer: INTEGER • avg_disk_bytes_per_transfer_enum: STRING • avg_disk_milliseconds_per_read: INTEGER • avg_disk_milliseconds_per_read_enum: STRING • avg_disk_milliseconds_per_write: INTEGER • avg_disk_milliseconds_per_write_enum: STRING • avg_disk_milliseconds_per_transfer: INTEGER • avg_disk_milliseconds_per_transfer_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Physical_Disk (Continued)	• avg_disk_queue_length: REAL • avg_disk_queue_length_enum: STRING • avg_disk_read_queue_length: REAL • avg_disk_read_queue_length_enum: STRING • avg_disk_write_queue_length: REAL • avg_disk_write_queue_length_enum: STRING • avg_disk_bytes_per_read_64: INTEGER • avg_disk_bytes_per_read_64_enum: STRING • avg_disk_bytes_per_transfer_64: INTEGER • avg_disk_bytes_per_transfer_64_enum: STRING • avg_disk_bytes_per_write_64: INTEGER • avg_disk_bytes_per_write_64_enum: STRING • disk_bytes_per_sec_64: INTEGER • disk_bytes_per_sec_64_enum: STRING • disk_read_bytes_per_sec_64: INTEGER • disk_read_bytes_per_sec_64_enum: STRING • disk_write_bytes_per_sec_64: INTEGER • disk_write_bytes_per_sec_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Process_64	ITM_NT_Process_64 event class with these slots: • server_name: STRING • timestamp: STRING • process_name: STRING • pct__privileged_time: INTEGER • pct__processor_time: INTEGER • pct__user_time: INTEGER • avg_pct__processor_time: INTEGER • binary_path: STRING • elapsed_time: INTEGER • elapsed_time_enum: STRING • handle_count: INTEGER • handle_count_enum: STRING • id_process: INTEGER • page_faults_per_sec: INTEGER • page_faults_per_sec_enum: STRING • page_file_bytes: INTEGER • page_file_bytes_enum: STRING • page_file_bytes_peak: INTEGER • page_file_bytes_peak_enum: STRING • page_file_kbytes: INTEGER • page_file_kbytes_enum: STRING • page_file_kbytes_peak: INTEGER • page_file_kbytes_peak_enum: STRING • pool_nonpaged_bytes: INTEGER • pool_nonpaged_bytes_enum: STRING • pool_paged_bytes: INTEGER • pool_paged_bytes_enum: STRING • priority_base: INTEGER • priority_base_enum: STRING • private_bytes: INTEGER • private_bytes_enum: STRING • private_kbytes: INTEGER • private_kbytes_enum: STRING • process_count: INTEGER • process_count_enum: STRING • thread_count: INTEGER • thread_count_enum: STRING • user: STRING • virtual_bytes: INTEGER • virtual_bytes_enum: STRING • virtual_bytes_peak: INTEGER • virtual_bytes_peak_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Process_64 (Continued)	• virtual_kbytes: INTEGER • virtual_kbytes_enum: STRING • virtual_kbytes_peak: INTEGER • virtual_kbytes_peak_enum: STRING • working_set: INTEGER • working_set_enum: STRING • working_set_peak: INTEGER • working_set_peak_enum: STRING • working_set_kbytes: INTEGER • working_set_kbytes_enum: STRING • working_set_kbytes_peak: INTEGER • working_set_kbytes_peak_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Process	ITM_NT_Process event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • process_name: STRING • pct__privileged_time: INTEGER • pct__processor_time: INTEGER • pct__user_time: INTEGER • elapsed_time: INTEGER • elapsed_time_enum: STRING • id_process: INTEGER • page_faults_per_sec: INTEGER • page_faults_per_sec_enum: STRING • page_file_bytes: INTEGER • page_file_bytes_peak: INTEGER • pool_nonpaged_bytes: INTEGER • pool_nonpaged_bytes_enum: STRING • pool_paged_bytes: INTEGER • pool_paged_bytes_enum: STRING • priority_base: INTEGER • priority_base_enum: STRING • private_bytes: INTEGER • thread_count: INTEGER • thread_count_enum: STRING • virtual_bytes: INTEGER • virtual_bytes_enum: STRING • virtual_bytes_peak: INTEGER • virtual_bytes_peak_enum: STRING • working_set: INTEGER • working_set_enum: STRING • working_set_peak: INTEGER • working_set_peak_enum: STRING • page_file_kbytes: INTEGER • page_file_kbytes_enum: STRING • page_file_kbytes_peak: INTEGER • page_file_kbytes_peak_enum: STRING • private_kbytes: INTEGER • private_kbytes_enum: STRING • virtual_kbytes: INTEGER • virtual_kbytes_enum: STRING • virtual_kbytes_peak: INTEGER • virtual_kbytes_peak_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Process (Continued)	• handle_count: INTEGER • handle_count_enum: STRING • binary_path: STRING • avg_pct__processor_time: INTEGER • user: STRING • working_set_kbytes: INTEGER • working_set_kbytes_enum: STRING • process_count: INTEGER • process_count_enum: STRING
NT_Processor	ITM_NT_Processor event class with these slots: • server_name: STRING • timestamp: STRING • processor: STRING • pct__privileged_time: INTEGER • pct__processor_time: INTEGER • pct__user_time: INTEGER • interrupts_per_sec: INTEGER • interrupts_per_sec_enum: STRING • apc_bypasses_per_sec: INTEGER • apc_bypasses_per_sec_enum: STRING • dpc_bypasses_per_sec: INTEGER • dpc_bypasses_per_sec_enum: STRING • dpc_rate: INTEGER • dpc_rate_enum: STRING • dpc_queued_per_sec: INTEGER • dpc_queued_per_sec_enum: STRING • pct__dpc_time: INTEGER • pct__interrupt_time: INTEGER
NT_Paging_File	ITM_NT_Paging_File event class with these slots: • server_name: STRING • timestamp: STRING • pagefile_name: STRING • pct__usage: INTEGER • pct__usage_peak: INTEGER • pagefile_name_u: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Objects	ITM_NT_Objects event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • events: INTEGER • events_enum: STRING • mutexes: INTEGER • mutexes_enum: STRING • processes: INTEGER • processes_enum: STRING • sections: INTEGER • sections_enum: STRING • semaphores: INTEGER • semaphores_enum: STRING • threads: INTEGER • threads_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Monitored_Logs_Report	ITM_NT_Monitored_Logs_Report event class with these slots: • server_name: STRING • timestamp: STRING • log_name: STRING • log_type: INTEGER • log_type_enum: STRING • date_last_modified: STRING • time_last_modified: STRING • max_size: INTEGER • max_size_enum: STRING • current_size: INTEGER • current_size_enum: STRING • pct__usage: INTEGER • record_count: INTEGER • record_count_enum: STRING • retention: INTEGER • retention_enum: STRING • path: STRING • date_time_last_modified: STRING • log_name_u: STRING • path_u: STRING • date_time_last_modified: STRING • log_name_u: STRING • path_u: STRING • current_size_64: INTEGER • current_size_64_enum: STRING • max_size_64: INTEGER • max_size_64_enum: STRING • record_count_64: INTEGER • record_count_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Event_Log	ITM_NT_Event_Log event class with these slots: • server_name: STRING • timestamp: STRING • log_name: STRING • entry_time: STRING • knt_date: STRING • time: STRING • knt_source: STRING • type: STRING • category: STRING • user: STRING • computer: STRING • event_id: INTEGER • description: STRING • log_name_u: STRING • source_u: STRING • category_u: STRING • user_u: STRING • description_u: STRING • event_id_string: STRING • duplicate_record_count: INTEGER • duplicate_record_count_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Active_Server_Pages	ITM_Active_Server_Pages event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • requests_total: INTEGER • requests_total_enum: STRING • request_total_bytes_in: INTEGER • request_total_bytes_in_enum: STRING • request_total_bytes_out: INTEGER • request_total_bytes_out_enum: STRING • total_queue_length: INTEGER • total_queue_length_enum: STRING • requests_current: INTEGER • requests_current_enum: STRING • requests_per_sec: INTEGER • requests_per_sec_enum: STRING • browser_requests_executing: INTEGER • browser_requests_executing_enum: STRING • requests_executed: INTEGER • requests_executed_enum: STRING • request_execution_time: INTEGER • request_execution_time_enum: STRING • requests_failed: INTEGER • requests_failed_enum: STRING • requests_rejected: INTEGER • requests_rejected_enum: STRING • requests_timed_out: INTEGER • requests_timed_out_enum: STRING • communication_failed: INTEGER • communication_failed_enum: STRING • request_errors_per_sec: INTEGER • request_errors_per_sec_enum: STRING • request_wait_time: INTEGER • request_wait_time_enum: STRING • sessions_current: INTEGER • sessions_current_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
	• sessions_timed_out: INTEGER • sessions_timed_out_enum: STRING • session_timed_out_requests_executing: INTEGER • session_timed_out_requests_ executing_enum: STRING • sessions_timed_out_requests_in_queue: INTEGER • sessions_timed_out_requests_in_ queue_enum: STRING • allocated_memory_in_free_list: INTEGER • allocated_memory_in_used_list: INTEGER • allocated_memory: INTEGER • thread_pool_current: INTEGER • free_script_engines_in_cache: INTEGER • free_script_engines_in_cache_enum: STRING • debugging_requests: INTEGER • errors_during_script_runtime: INTEGER • errors_from_asp_preprocessor: INTEGER • errors_from_script_compilers: INTEGER • requests_not_authorized: INTEGER • requests_not_found: INTEGER • session_duration: INTEGER
Active_Server_Pages (continued)	• sessions_total: INTEGER • template_cache_hit_rate: INTEGER • template_notifications: INTEGER • templates_cached: INTEGER • transactions_aborted: INTEGER • transactions_committed: INTEGER • transactions_pending: INTEGER • transactions_total: INTEGER • transactions_per_sec: INTEGER

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
HTTP_Content_Index	ITM_HTTP_Content_Index event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • active_queries: INTEGER • active_queries_enum: STRING • total_queries: INTEGER • total_queries_enum: STRING • queries_per_minute: INTEGER • queries_per_minute_enum: STRING • current_requests_queued_enum: STRING • current_requests_queued: INTEGER • total_requests_rejected: INTEGER • total_requests_rejected_enum: STRING • pct__cache_hits: INTEGER • pct__cache_misses: INTEGER • cache_items: INTEGER • cache_items_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
HTTP_Service	ITM_HTTP_Service event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • connection_attempts: INTEGER • connection_attempts_enum: STRING • connections_per_sec: INTEGER • connections_per_sec_enum: STRING • current_connections: INTEGER • current_connections_enum: STRING • maximum_connections: INTEGER • maximum_connections_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • files_sent: INTEGER • files_sent_enum: STRING • files_received: INTEGER • files_received_enum: STRING • files_total: INTEGER • files_total_enum: STRING • not_found_errors: INTEGER • not_found_errors_enum: STRING • cgi_requests: INTEGER • cgi_requests_enum: STRING • current_cgi_requests: INTEGER • current_cgi_requests_enum: STRING • maximum_cgi_requests: INTEGER • maximum_cgi_requests_enum: STRING • get_requests: INTEGER • get_requests_enum: STRING • post_requests: INTEGER • post_requests_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
HTTP_Service (Continued)	• isapi_extension_requests: INTEGER • isapi_extension_requests_enum: STRING • current_isapi_extension_requests: INTEGER • current_isapi_extension_requests_enum: STRING • maximum_isapi_extension_requests: INTEGER • maximum_isapi_extension_requests_enum: STRING • head_requests: INTEGER • head_requests_enum: STRING • other_requests: INTEGER • other_requests_enum: STRING • logon_attempts: INTEGER • logon_attempts_enum: STRING • current_anonymous_users: INTEGER • current_anonymous_users_enum: STRING • current_nonanonymous_users: INTEGER • current_nonanonymous_users_enum: STRING • total_anonymous_users: INTEGER • total_anonymous_users_enum: STRING • total_nonanonymous_users: INTEGER • total_nonanonymous_users_enum: STRING • maximum_anonymous_users: INTEGER • maximum_anonymous_users_enum: STRING • maximum_nonanonymous_users: INTEGER • maximum_nonanonymous_users_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
ITM_FTP_Server_Statistics	FTP_Server_Statistics attribute group • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • total_bytes_per_sec: INTEGER • total_bytes_per_sec_enum: STRING • files_received: INTEGER • files_received_enum: STRING • files_sent: INTEGER • files_sent_enum: STRING • total_files: INTEGER • total_files_enum: STRING • current_anonymous_users: INTEGER • current_anonymous_users_enum: STRING • current_non_anonymous_users: INTEGER • current_non_anonymous_users_enum: STRING • current_connections: INTEGER • current_connections_enum: STRING • total_anonymous_users_since_ftp_start: INTEGER • total_anonymous_users_since_ftp_start_enum: STRING • total_non_anonymous_users_since_ftp_start: INTEGER • total_non_anonymous_users_since_ftp_start_enum: STRING • connection_attempts_since_ftp_start: INTEGER • connection_attempts_since_ftp_start_enum: STRING • logon_attempts_since_ftp_start: INTEGER • logon_attempts_since_ftp_start_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
ITM_FTP_Server_Statistics (Continued)	• maximum_anonymous_users: INTEGER • maximum_anonymous_users_enum: STRING • maximum_non_anonymous_users: INTEGER • maximum_non_anonymous_users_enum: STRING • maximum_connections: INTEGER • maximum_connections_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
IIS_Statistics	ITM_IIS_Statistics event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • measured_async_io_bandwidth_usage: INTEGER • measured_async_io_bandwidth_usage _enum: STRING • current_blocked_async_io_requests: INTEGER • current_blocked_async_io_requests_enum: STRING • total_blocked_async_io_requests: INTEGER • total_blocked_async_io_requests_enum: STRING • total_allowed_async_requests: INTEGER • total_allowed_async_requests_enum: STRING • total_rejected_async_requests: INTEGER • total_rejected_async_requests_enum: STRING • cache_size: INTEGER • cache_size_enum: STRING • cache_used: INTEGER • cache_used_enum: STRING • cache_hits_pct: INTEGER • cache_hits_pct_enum: STRING • cache_hits: INTEGER • cache_hits_enum: STRING • cache_misses: INTEGER • cache_misses_enum: STRING • cached_objects: INTEGER • cached_objects_enum: STRING • cached_directory_listings: INTEGER • cached_directory_listings_enum: STRING • cached_file_handles: INTEGER • cached_file_handles_enum: STRING • cache_flushes: INTEGER • cache_flushes_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
UDP_Statistics	ITM_UDP_Statistics event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • datagrams_per_sec: INTEGER • datagrams_per_sec_enum: STRING • datagrams_received_per_sec: INTEGER • datagrams_received_per_sec_enum: STRING • datagrams_sent_per_sec: INTEGER • datagrams_sent_per_sec_enum: STRING • datagrams_received_errors: INTEGER • datagrams_received_errors_enum: STRING • datagrams_no_port_per_sec: INTEGER • datagrams_no_port_per_sec_enum: STRING
TCP_Statistics	ITM_TCP_Statistics event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • connection_failures: INTEGER • connection_failures_enum: STRING • connections_active: INTEGER • connections_active_enum: STRING • connections_established: INTEGER • connections_established_enum: STRING • connections_passive: INTEGER • connections_passive_enum: STRING • connections_reset: INTEGER • connections_reset_enum: STRING • segments_per_sec: INTEGER • segments_per_sec_enum: STRING • segments_received_per_sec: INTEGER • segments_received_per_sec_enum: STRING • segments_sent_per_sec: INTEGER • segments_sent_per_sec_enum: STRING • segments_retransmitted_per_sec: INTEGER • segments_retransmitted_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
IP_Statistics	ITM_IP_Statistics event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • datagrams_per_sec: INTEGER • datagrams_per_sec_enum: STRING • datagrams_received_per_sec: INTEGER • datagrams_received_per_sec_enum: STRING • datagrams_sent_per_sec: INTEGER • datagrams_sent_per_sec_enum: STRING • datagrams_forwarded_per_sec: INTEGER • datagrams_forwarded_per_sec_enum: STRING • datagrams_outbound_discarded: INTEGER • datagrams_outbound_discarded_enum: STRING • datagrams_received_discarded: INTEGER • datagrams_received_discarded_enum: STRING • datagrams_outbound_no_route: INTEGER • datagrams_outbound_no_route_enum: STRING • datagrams_received_address_errors: INTEGER • datagrams_received_address_errors_enum: STRING • datagrams_received_delivered_per_sec: INTEGER • datagrams_received_delivered_per_sec _enum: STRING • datagrams_received_header_errors: INTEGER • datagrams_received_header_errors_enum: STRING • datagrams_received_unknown_protocol: INTEGER • datagrams_received_unknown_protocol _enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
IP_Statistics (Continued)	• fragmented_datagrams_per_sec: INTEGER • fragmented_datagrams_per_sec_enum: STRING • fragments_received_per_sec: INTEGER • fragments_received_per_sec_enum: STRING • fragmentation_failures: INTEGER • fragmentation_failures_enum: STRING • fragments_created_per_sec: INTEGER • fragments_created_per_sec_enum: STRING • fragment_re-assembly_failures: INTEGER • fragment_re-assembly_failures_enum: STRING • fragments_re-assembled_per_sec: INTEGER • fragments_re-assembled_per_sec_enum: STRING • datagram_fragmentation_percentage: INTEGER • datagram_fragmentation_percentage_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
ICMP_Statistics	ITM_ICMP_Statistics event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • messages_per_sec: INTEGER • messages_per_sec_enum: STRING • messages_received_per_sec: INTEGER • messages_received_per_sec_enum: STRING • messages_sent_per_sec: INTEGER • messages_sent_per_sec_enum: STRING • messages_received_errors: INTEGER • messages_received_errors_enum: STRING • messages_outbound_errors: INTEGER • messages_outbound_errors_enum: STRING • received_time_exceeded: INTEGER • received_time_exceeded_enum: STRING • sent_time_exceeded: INTEGER • sent_time_exceeded_enum: STRING • received_timestamp_per_sec: INTEGER • received_timestamp_per_sec_enum: STRING • sent_timestamp_per_sec: INTEGER • sent_timestamp_per_sec_enum: STRING • received_timestamp_reply_per_sec: INTEGER • received_timestamp_reply_per_sec_enum: STRING • sent_timestamp_reply_per_sec: INTEGER • sent_timestamp_reply_per_sec_enum: STRING • received_destination_unreachable: INTEGER • received_destination_unreachable_enum: STRING • send_destination_unreachable: INTEGER • send_destination_unreachable_enum: STRING • received_redirect_per_sec: INTEGER • received_redirect_per_sec_enum: STRING • sent_redirect_per_sec: INTEGER • sent_redirect_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
ICMP_Statistics (Continued)	• received_parameter_problem: INTEGER • received_parameter_problem_enum: STRING • sent_parameter_problem: INTEGER • sent_parameter_problem_enum: STRING • received_echo_per_sec: INTEGER • received_echo_per_sec_enum: STRING • sent_echo_per_sec: INTEGER • sent_echo_per_sec_enum: STRING • received_echo_reply_per_sec: INTEGER • received_echo_reply_per_sec_enum: STRING • sent_echo_reply_per_sec: INTEGER • sent_echo_reply_per_sec_enum: STRING • received_address_mask: INTEGER • received_address_mask_enum: STRING • sent_address_mask: INTEGER • sent_address_mask_enum: STRING • received_address_mask_reply: INTEGER • received_address_mask_reply_enum: STRING • sent_address_mask_reply: INTEGER • sent_address_mask_reply_enum: STRING • received_source_quench: INTEGER • received_source_quench_enum: STRING • sent_source_quench: INTEGER • sent_source_quench_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_FILE_CHANGE	ITM_NT_FILE_CHANGE event class with these slots: • server_name: STRING • timestamp: STRING • watch_directory: STRING • watch_file: STRING • action: INTEGER • action_enum: STRING • date_created: STRING • time_created: STRING • date_last_modified: STRING • time_last_modified: STRING • current_size: INTEGER • current_size_enum: STRING • attributes: INTEGER • total_hits: INTEGER • total_hits_enum: STRING • watch_tree: STRING • watch_tree_enum: STRING • monitor_all_conditions: STRING • monitor_all_conditions_enum: STRING • change_file_name: STRING • change_file_name_enum: STRING • change_directory_name: STRING • change_directory_name_enum: STRING • change_attributes: STRING • change_attributes_enum: STRING • change_size: STRING • change_size_enum: STRING • change_last_write: STRING • change_last_write_enum: STRING • change_last_access: STRING • change_last_access_enum: STRING • change_create: STRING • change_create_enum: STRING • change_security: STRING • change_security_enum: STRING • date_time_created: STRING • date_time_last_modified: STRING • watch_directory_u: STRING • watch_file_u: STRING • current_size_64: INTEGER • current_size_64_enum: STRING • total_hits_64: INTEGER • total_hits_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_FILE_TREND	ITM_NT_FILE_TREND event class with these slots: • server_name: STRING • timestamp: STRING • watch_directory: STRING • watch_file: STRING • date_created: STRING • time_created: STRING • date_last_modified: STRING • time_last_modified: STRING • attributes: INTEGER • attributes_enum: STRING • current_size: INTEGER • current_size_enum: STRING • pct__used: INTEGER • pct__used_enum: STRING • sampling_interval: INTEGER • sampling_interval_enum: STRING • sampling_number: INTEGER • pct__change_lasthour: INTEGER • pct__change_lasthour_enum: STRING • pct__change_last_interval: INTEGER • pct__change_average: INTEGER • pct__change_total: INTEGER • size_change_lasthour: INTEGER • size_change_lastinterval: INTEGER • size_change_average: INTEGER • size_change_total: INTEGER • free_space_exhuasted_hours: INTEGER • date_time_created: STRING • date_time_last_modified: STRING • watch_directory_u: STRING • watch_file_u: STRING • current_size_64: INTEGER • current_size_64_enum: STRING • size_change_average_64: INTEGER • size_change_average_64_enum: STRING • size_change_lasthour_64: INTEGER • size_change_lasthour_64_enum: STRING • size_change_lastinterval_64: INTEGER • size_change_lastinterval_64_enum: STRING • size_change_total_64: INTEGER • size_change_total_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Network_Interface	ITM_NT_Network_Interface event class with these slots: • system_name: STRING • timestamp: STRING • network_interface_instance: STRING • bandwidth_utilization_percentage: INTEGER • bandwidth_utilization_percentage_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • current_bandwidth: INTEGER • current_bandwidth_enum: STRING • ipv4_address: STRING • ipv4_address_enum: STRING • ipv6_global_address: STRING • ipv6_global_address_enum: STRING • ipv6_link_local_address: STRING • ipv6_link_local_address_enum: STRING • output_queue_length: INTEGER • output_queue_length_enum: STRING • output_queue_length_kpackets: INTEGER • output_queue_length_kpackets_enum: STRING • packets_outbound_discarded: INTEGER • packets_outbound_discarded_enum: STRING • packets_outbound_errors: INTEGER • packets_outbound_errors_enum: STRING • packets_per_sec: INTEGER • packets_per_sec_enum: STRING • packets_received_per_sec: INTEGER • packets_received_per_sec_enum: STRING • packets_received_discarded: INTEGER • packets_received_discarded_enum: STRING • packets_received_errors: INTEGER • packets_received_errors_enum: STRING • packets_received_non-unicast_per_sec: INTEGER • packets_received_non-unicast_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Network_Interface (Continued)	• packets_received_unicast_per_sec: INTEGER • packets_received_unicast_per_sec_enum: STRING • packets_received_unknown: INTEGER • packets_received_unknown_enum: STRING • packets_sent_per_sec: INTEGER • packets_sent_per_sec_enum: STRING • packets_sent_non-unicast_per_sec: INTEGER • packets_sent_non-unicast_per_sec_enum: STRING • packets_sent_unicast_per_sec: INTEGER • packets_sent_unicast_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Network_Interface	ITM_Network_Interface event class with these slots: • system_name: STRING • timestamp: STRING • network_interface_instance: STRING • current_bandwidth: INTEGER • current_bandwidth_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • packets_per_sec: INTEGER • packets_per_sec_enum: STRING • packets_received_per_sec: INTEGER • packets_received_per_sec_enum: STRING • packets_sent_per_sec: INTEGER • packets_sent_per_sec_enum: STRING • output_queue_length: INTEGER • output_queue_length_enum: STRING • packets_received_errors: INTEGER • packets_received_errors_enum: STRING • packets_outbound_errors: INTEGER • packets_outbound_errors_enum: STRING • packets_received_unknown: INTEGER • packets_received_unknown_enum: STRING • packets_received_discarded: INTEGER • packets_received_discarded_enum: STRING • packets_outbound_discarded: INTEGER • packets_outbound_discarded_enum: STRING • packets_received_unicast_per_sec: INTEGER • packets_received_unicast_per_sec_enum: STRING • packets_sent_unicast_per_sec: INTEGER • packets_sent_unicast_per_sec_enum: STRING • packets_received_non-unicast_per_sec: INTEGER • packets_received_non-unicast_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Network_Interface (Continued)	• packets_sent_non-unicast_per_sec: INTEGER • packets_sent_non-unicast_per_sec_enum: STRING • output_queue_length_kpackets: INTEGER • output_queue_length_kpackets: INTEGER • bandwidth_utilization_percentage_enum: STRING • ipv4_address: STRING • ipv4_address_enum: STRING • ipv6_global_address: STRING • ipv6_global_address_enum: STRING • ipv6_link_local_address: STRING • ipv6_link_local_address_enum: STRING • network_interface_instance_unicode: STRING
Network_Segment	ITM_Network_Segment event class with these slots: • system_name: STRING • timestamp: STRING • network_segment_instance: STRING • pct__network_utilization: INTEGER • total_bytes_received_per_sec: INTEGER • total_bytes_received_per_sec_enum: STRING • total_frames_received_per_sec: INTEGER • total_frames_received_per_sec_enum: STRING • pct__broadcast_frames: INTEGER • broadcast_frames_received_per_sec: INTEGER • broadcast_frames_received_per_sec_enum: STRING • pct__multicast_frames: INTEGER • multicast_frames_received_per_sec: INTEGER •

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
ITM_Gopher_Service	ITM_Gopher_Service event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • files_sent: INTEGER • files_sent_enum: STRING • searches_sent: INTEGER • searches_sent_enum: STRING • directory_listings_sent: INTEGER • directory_listings_sent_enum: STRING • current_connections: INTEGER • current_connections_enum: STRING • maximum_connections: INTEGER • maximum_connections_enum: STRING • connection_attempts: INTEGER • connection_attempts_enum: STRING • connections_in_error: INTEGER • connections_in_error_enum: STRING • aborted_connections: INTEGER • aborted_connections_enum: STRING • current_anonymous_users: INTEGER • current_anonymous_users_enum: STRING • current_nonanonymous_users: INTEGER • current_nonanonymous_users_enum: STRING • maximum_anonymous_users: INTEGER • maximum_anonymous_users_enum: STRING • maximum_nonanonymous_users: INTEGER • maximum_nonanonymous_users_enum: STRING • gopher_plus_requests: INTEGER • gopher_plus_requests_enum:STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
ITM_Gopher_Service (Continued)	• logon_attempts: INTEGER • logon_attempts_enum: STRING • total_anonymous_users: INTEGER • total_anonymous_users_enum: STRING • total_nonanonymous_users: INTEGER • total_nonanonymous_users_enum: STRING
MSMQ_Information_Store	ITM_MSMQ_Information_Store event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • access_to_the_server: INTEGER • access_to_the_server_enum:STRING • errors_returned_to_application: INTEGER • errors_returned_to_application_enum: STRING • replication_requests_received: INTEGER • replication_requests_received_enum: STRING • replication_requests_sent: INTEGER • replication_requests_sent_enum: STRING • sync_replies: INTEGER • sync_replies_enum: STRING • sync_requests: INTEGER • sync_requests_enum: STRING • write_requests_sent: INTEGER • write_requests_sent_enum: STRING
MSMQ_Queue	ITM_MSMQ_Queue event class with these slots: • system_name: STRING • timestamp: STRING • queue_instance: STRING • bytes_in_journal_queue: INTEGER • bytes_in_journal_queue_enum: STRING • bytes_in_queue: INTEGER • bytes_in_queue_enum: STRING • messages_in_journal_queue: INTEGER • messages_in_journal_queue_enum: STRING • messages_in_queue: INTEGER • messages_in_queue_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
MSMQ_Service	ITM_MSMQ_Service event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • incoming_messages_per_sec: INTEGER • outgoing_messages_per_sec: INTEGER • msmq_incoming_messages: INTEGER • msmq_outgoing_messages: INTEGER • total_bytes_in_all_queues: INTEGER • total_messages_in_all_queues: INTEGER • sessions: INTEGER • ip_sessions: INTEGER • ipx_sessions: INTEGER
MSMQ_Sessions	ITM_MSMQ_Sessions event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • session: STRING • incoming_bytes: INTEGER • incoming_bytes_enum: STRING • incoming_bytes_per_sec: INTEGER • incoming_bytes_per_sec_enum: STRING • incoming_messages: INTEGER • incoming_messages_enum: STRING • incoming_messages_per_sec: INTEGER • incoming_messages_per_sec_enum: STRING • outgoing_bytes: INTEGER • outgoing_bytes_enum: STRING • outgoing_bytes_per_sec: INTEGER • outgoing_bytes_per_sec_enum: STRING • outgoing_messages: INTEGER • outgoing_messages_enum: STRING • outgoing_messages_per_sec: INTEGER • outgoing_messages_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
RAS_Port	ITM_RAS_Port event class with these slots: • system_name: STRING • timestamp: STRING • port_instance: STRING • alignment_errors: INTEGER • alignment_errors_enum: STRING • buffer_overrun_errors: INTEGER • buffer_overrun_errors_enum: STRING • bytes_received: INTEGER • bytes_received_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_transmitted: INTEGER • bytes_transmitted_enum: STRING • bytes_transmitted_per_sec: INTEGER • bytes_transmitted_per_sec_enum: STRING • crc_errors: INTEGER • crc_errors_enum: STRING • frames_received: INTEGER • frames_received_enum: STRING • frames_received_per_sec: INTEGER • frames_received_per_sec_enum: STRING • frames_transmitted: INTEGER • frames_transmitted_enum: STRING • frames_transmitted_per_sec: INTEGER • frames_transmitted_per_sec_enum: STRING • percent_compression_in: INTEGER • percent_compression_in_enum: STRING • percent_compression_out: INTEGER • percent_compression_out_enum: STRING • serial_overrun_errors: INTEGER • serial_overrun_errors_enum: STRING • timeout_errors: INTEGER • timeout_errors_enum: STRING • total_errors: INTEGER • total_errors_enum: STRING • total_errors_per_sec: INTEGER • total_errors_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
RAS_Total	ITM_RAS_Total event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • alignment_errors: INTEGER • alignment_errors_enum: STRING • buffer_overrun_errors: INTEGER • buffer_overrun_errors_enum: STRING • bytes_received: INTEGER • bytes_received_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_transmitted: INTEGER • bytes_transmitted_enum: STRING • bytes_transmitted_per_sec: INTEGER • bytes_transmitted_per_sec_enum: STRING • crc_errors: INTEGER • crc_errors_enum: STRING • frames_received: INTEGER • frames_received_enum: STRING • frames_received_per_sec: INTEGER • frames_received_per_sec_enum: STRING • frames_transmitted: INTEGER • frames_transmitted_enum: STRING • frames_transmitted_per_sec: INTEGER • frames_transmitted_per_sec_enum: STRING • percent_compression_in: INTEGER • percent_compression_out: INTEGER • serial_overrun_errors: INTEGER • serial_overrun_errors_enum: STRING • timeout_errors: INTEGER • timeout_errors_enum: STRING • total_connections: INTEGER • total_connections_enum: STRING • total_errors: INTEGER • total_errors_enum: STRING • total_errors_per_sec: INTEGER • total_errors_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Cache	ITM_NT_Cache event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • async_copy_reads_per_sec: INTEGER • async_copy_reads_per_sec_enum: STRING • async_data_maps_per_sec: INTEGER • async_data_maps_per_sec_enum: STRING • async_fast_reads_per_sec: INTEGER • async_fast_reads_per_sec_enum: STRING • async_mdl_reads_per_sec: INTEGER • async_mdl_reads_per_sec_enum: STRING • async_pin_reads_per_sec: INTEGER • async_pin_reads_per_sec_enum: STRING • copy_read_hits_pct: INTEGER • copy_reads_per_sec: INTEGER • copy_reads_per_sec_enum: STRING • data_flush_pages_per_sec: INTEGER • data_flush_pages_per_sec_enum: STRING • data_flushes_per_sec: INTEGER • data_flushes_per_sec_enum: STRING • data_map_hits_pct: INTEGER • data_map_pins_per_sec: INTEGER • data_map_pins_per_sec_enum: STRING • data_maps_per_sec: INTEGER • data_maps_per_sec_enum: STRING • fast_read_not_possibles_per_sec: INTEGER • fast_read_not_possibles_per_sec_enum: STRING • fast_read_resource_misses_per_sec: INTEGER • fast_read_resource_misses_per_sec_enum: STRING • fast_reads_per_sec: INTEGER • fast_reads_per_sec_enum: STRING • lazy_write_flushes_per_sec: INTEGER • lazy_write_flushes_per_sec_enum: STRING • lazy_write_pages_per_sec: INTEGER • lazy_write_pages_per_sec_enum: STRING • mdl_read_hits_pct: INTEGER • mdl_reads_per_sec: INTEGER • mdl_reads_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Cache (Continued)	• pin_read_hits_pct: INTEGER • pin_reads_per_sec: INTEGER • pin_reads_per_sec_enum: STRING • read_aheads_per_sec: INTEGER • read_aheads_per_sec_enum: STRING • sync_copy_reads_per_sec: INTEGER • sync_copy_reads_per_sec_enum: STRING • sync_data_maps_per_sec: INTEGER • sync_data_maps_per_sec_enum: STRING • sync_fast_reads_per_sec: INTEGER • sync_fast_reads_per_sec_enum: STRING • sync_mdl_reads_per_sec: INTEGER • sync_mdl_reads_per_sec_enum: STRING • sync_pin_reads_per_sec: INTEGER • sync_pin_reads_per_sec_enum: STRING • copy_read_hits_dyn_avg: INTEGER • copy_read_hits_dyn_avg_enum: STRING • data_map_hits_dyn_avg: INTEGER • data_map_hits_dyn_avg_enum: STRING • mdl_read_hits_dyn_avg: INTEGER • mdl_read_hits_dyn_avg_enum: STRING • pin_read_hits_dyn_avg: INTEGER • pin_read_hits_dyn_avg_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Printer	ITM_NT_Printer event class with these slots: • system_name: STRING • timestamp: STRING • printer_name: STRING • share_name: STRING • port_name: STRING • driver_name: STRING • comment: STRING • location: STRING • separator_file: STRING • print_processor: STRING • data_type: STRING • parameters: STRING • priority: INTEGER • default_priority: INTEGER • start_time: STRING • until_time: STRING • knt_status: STRING • number_of_jobs: INTEGER • number_of_jobs_enum: STRING • average_ppm: INTEGER • average_ppm_enum: STRING • printer_name_u: STRING • share_name_u: STRING • comment_u: STRING • location_u: STRING • separator_file_u: STRING • average_ppm_64: INTEGER • average_ppm_64_enum: STRING • number_of_jobs_64: INTEGER • number_of_jobs_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Print_Job	ITM_NT_Print_Job event class with these slots: • system_name: STRING • timestamp: STRING • printer_name: STRING • document_name: STRING • user_name: STRING • knt_status: STRING • machine_name: STRING • notify_name: STRING • data_type: STRING • print_processor: STRING • parameters: STRING • driver_name: STRING • priority: INTEGER • position: INTEGER • total_pages: INTEGER • total_pages_enum: STRING • size: INTEGER • size_enum: STRING • time_submitted: STRING • time_elapsed: INTEGER • time_elapsed_enum: STRING • pages_printed: INTEGER • pages_printed_enum: STRING • printer_name_u: STRING • document_name_u: STRING • user_name_u: STRING • notify_name_u: STRING • pages_printed_64: INTEGER • pages_printed_64_enum: STRING • size_64: INTEGER • size_64_enum: STRING • time_elapsed_64: INTEGER • time_elapsed_64_enum: STRING • total_pages_64: INTEGER • total_pages_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Services	ITM_NT_Services event class with these slots: • server_name: STRING • timestamp: STRING • display_name: STRING • current_state: STRING • start_type: STRING • binary_path: STRING • account_id: STRING • load_order_group: STRING • service_name: STRING • display_name_u: STRING • binary_path_u: STRING • account_id_u: STRING • service_name_u: STRING
NT_Service_Dependencies	ITM_NT_Service_Dependencies event class with these slots: • server_name: STRING • timestamp: STRING • service_name: STRING • display_name: STRING • dependency: STRING • display_name_u: STRING
NT_Devices	ITM_NT_Devices event class with these slots: • server_name: STRING • timestamp: STRING • display_name: STRING • current_state: STRING • start_type: STRING • start_type_enum: STRING • binary_path: STRING • driver_object_name: STRING • load_order_group: STRING • device_name: STRING • display_name_u: STRING • binary_path_u: STRING
NT_Device_Dependencies	ITM_NT_Device_Dependencies event class with these slots: • server_name: STRING • timestamp: STRING • device_name: STRING • display_name: STRING • dependency: STRING • display_name_u: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
FTP_Service	ITM_FTP_Service event class with these slots: • system_name: STRING • timestamp: STRING • ftp_site: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • total_files_received: INTEGER • total_files_received_enum: STRING • total_files_sent: INTEGER • total_files_sent_enum: STRING • total_files_transferred: INTEGER • total_files_transferred_enum: STRING • current_anonymous_users: INTEGER • current_anonymous_users_enum: STRING • current_nonanonymous_users: INTEGER • current_nonanonymous_users_enum: STRING • current_connections: INTEGER • current_connections_enum: STRING • total_anonymous_users: INTEGER • total_anonymous_users_enum: STRING • total_nonanonymous_users: INTEGER • total_nonanonymous_users_enum: STRING • total_connection_attempts: INTEGER • total_connection_attempts_enum: STRING • total_logon_attempts: INTEGER • total_logon_attempts_enum: STRING • maximum_anonymous_users: INTEGER • maximum_anonymous_users_enum: STRING • maximum_nonanonymous_users: INTEGER • maximum_nonanonymous_users_enum: STRING • maximum_connections: INTEGER • maximum_connections_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Web_Service	ITM_Web_Service event class with these slots: • system_name: STRING • timestamp: STRING • web_site: STRING • total_connection_attempts: INTEGER • total_connection_attempts_enum: STRING • total_method_requests_per_sec: INTEGER • total_method_requests_per_sec_enum: STRING • current_connections: INTEGER • current_connections_enum: STRING • maximum_connections: INTEGER • maximum_connections_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • total_files_sent: INTEGER • total_files_sent_enum: STRING • total_files_received: INTEGER • total_files_received_enum: STRING • total_files_transferred: INTEGER • total_files_transferred_enum: STRING • total_not_found_errors: INTEGER • total_not_found_errors_enum: STRING • total_cgi_requests: INTEGER • total_cgi_requests_enum: STRING • current_cgi_requests: INTEGER • current_cgi_requests_enum: STRING • maximum_cgi_requests: INTEGER • maximum_cgi_requests_enum: STRING • total_get_requests: INTEGER • total_get_requests_enum: STRING • total_post_requests: INTEGER • total_post_requests_enum: STRING • total_isapi_extension_requests: INTEGER • total_isapi_extension_requests_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Web_Service (Cont.)	• current_isapi_extension_requests: INTEGER • current_isapi_extension_requests_enum: STRING • maximum_isapi_extension_requests: INTEGER • maximum_isapi_extension_requests_enum: STRING • total_head_requests: INTEGER • total_head_requests_enum: STRING • total_other_request_methods: INTEGER • total_other_request_methods_enum: STRING • total_logon_attempts: INTEGER • total_logon_attempts_enum: STRING • current_anonymous_users: INTEGER • current_anonymous_users_enum: STRING • current_nonanonymous_users: INTEGER • current_nonanonymous_users_enum: STRING • total_anonymous_users: INTEGER • total_anonymous_users_enum: STRING • total_nonanonymous_users: INTEGER • total_nonanonymous_users_enum: STRING • maximum_anonymous_users: INTEGER • maximum_anonymous_users_enum: STRING • maximum_nonanonymous_users: INTEGER • maximum_nonanonymous_users_enum: STRING • anonymous_users_per_sec: INTEGER • anonymous_users_per_sec_enum: STRING • cgi_requests_per_sec: INTEGER • cgi_requests_per_sec_enum: STRING • connection_attempts_per_sec: INTEGER • connection_attempts_per_sec_enum: STRING • current_blocked_async_io_requests: INTEGER • current_blocked_async_io_requests_enum: STRING • delete_requests_per_sec: INTEGER • delete_requests_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Web_Service (Cont.)	• files_received_per_sec: INTEGER • files_received_per_sec_enum: STRING • files_sent_per_sec: INTEGER • files_sent_per_sec_enum: STRING • files_per_sec: INTEGER • files_per_sec_enum: STRING • get_requests_per_sec: INTEGER • get_requests_per_sec_enum: STRING • head_requests_per_sec: INTEGER • head_requests_per_sec_enum: STRING • isapi_extension_requests_per_sec: INTEGER • isapi_extension_requests_per_sec_enum: STRING • logon_attempts_per_sec: INTEGER • logon_attempts_per_sec_enum: STRING • measured_async_io_bandwidth_usage: INTEGER • measured_async_io_bandwidth_usage _enum: STRING • nonanonymous_users_per_sec: INTEGER • nonanonymous_users_per_sec_enum: STRING • not_found_errors_per_sec: INTEGER • not_found_errors_per_sec_enum: STRING • other_request_methods_per_sec: INTEGER • other_request_methods_per_sec_enum: STRING • post_requests_per_sec: INTEGER • post_requests_per_sec_enum: STRING • put_requests_per_sec: INTEGER • put_requests_per_sec_enum: STRING • system_code_resident_bytes: INTEGER • system_code_resident_bytes_enum: STRING • total_allowed_async_io_requests: INTEGER • total_allowed_async_io_requests_enum: STRING • total_blocked_async_io_requests: INTEGER • total_blocked_async_io_requests_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Web_Service (Cont.)	• total_delete_requests: INTEGER • total_delete_requests_enum: STRING • total_method_requests: INTEGER • total_method_requests_enum: STRING • total_put_requests: INTEGER • total_put_requests_enum: STRING • total_rejected_async_io_requests: INTEGER • total_rejected_async_io_requests_enum: STRING • total_trace_requests: INTEGER • total_trace_requests_enum: STRING • bytes_received_per_sec_64: INTEGER • bytes_received_per_sec_64_enum: STRING • bytes_sent_per_sec_64: INTEGER • bytes_sent_per_sec_64_enum: STRING • bytes_total_per_sec_64: INTEGER • bytes_total_per_sec_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Indexing_Service	ITM_Indexing_Service event class with these slots: • system_name: STRING • timestamp: STRING • index: STRING • number_of_documents_indexed: INTEGER • number_of_documents_indexed_enum: STRING • deferred_for_indexing: INTEGER • deferred_for_indexing_enum: STRING • files_to_be_indexed: INTEGER • files_to_be_indexed_enum: STRING • index_size_mb: INTEGER • index_size_mb_enum: STRING • merge_progress: INTEGER • running_queries: INTEGER • running_queries_enum: STRING • saved_indexes: INTEGER • saved_indexes_enum: STRING • total_number_of_documents: INTEGER • total_number_of_documents_enum: STRING • total_number_of_queries: INTEGER • total_number_of_queries_enum: STRING • unique_keys: INTEGER • unique_keys_enum: STRING • word_lists: INTEGER • word_lists_enum: STRING • index_u: STRING
Indexing_Service_Filter	ITM_Indexing_Service_Filter event class with these slots: • system_name: STRING • timestamp: STRING • index: STRING • binding_time_msec: INTEGER • binding_time_msec_enum: STRING • indexing_speed_mb_per_hr: INTEGER • indexing_speed_mb_per_hr_enum: STRING • total_indexing_speed_mb_per_hr: INTEGER • total_indexing_speed_mb_per_hr_enum: STRING • index_u: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NNTP_Commands	ITM_NNTP_Commands event class with these slots: • system_name: STRING • timestamp: STRING • nntp_server: STRING • article_commands: INTEGER • article_commands_enum: STRING • article_commands_per_sec: INTEGER • article_commands_per_sec_enum: STRING • check_commands: INTEGER • check_commands_enum: STRING • check_commands_per_sec: INTEGER • check_commands_per_sec_enum: STRING • group_commands: INTEGER • group_commands_enum: STRING • group_commands_per_sec: INTEGER • group_commands_per_sec_enum: STRING • help_commands: INTEGER • help_commands_enum: STRING • help_commands_per_sec: INTEGER • help_commands_per_sec_enum: STRING • ihave_commands: INTEGER • ihave_commands_enum: STRING • ihave_commands_per_sec: INTEGER • ihave_commands_per_sec_enum: STRING • last_commands: INTEGER • last_commands_enum: STRING • last_commands_per_sec: INTEGER • last_commands_per_sec_enum: STRING • list_commands: INTEGER • list_commands_enum: STRING • list_commands_per_sec: INTEGER • list_commands_per_sec_enum: STRING • logon_attempts: INTEGER • logon_attempts_enum: STRING • logon_attempts_per_sec: INTEGER • logon_attempts_per_sec_enum: STRING • logon_failures: INTEGER • logon_failures_enum: STRING • logon_failures_per_sec: INTEGER • logon_failures_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NNTP_Commands (Cont.)	• mode_commands: INTEGER • mode_commands_enum: STRING • mode_commands_per_sec: INTEGER • mode_commands_per_sec_enum: STRING • newgroups_commands: INTEGER • newgroups_commands_enum: STRING • newgroups_commands_per_sec: INTEGER • newgroups_commands_per_sec_enum: STRING • newnews_commands: INTEGER • newnews_commands_enum: STRING • newnews_commands_per_sec: INTEGER • newnews_commands_per_sec_enum: STRING • next_commands: INTEGER • next_commands_enum: STRING • next_commands_per_sec: INTEGER • next_commands_per_sec_enum: STRING • post_commands: INTEGER • post_commands_enum: STRING • post_commands_per_sec: INTEGER • post_commands_per_sec_enum: STRING • quit_commands: INTEGER • quit_commands_enum: STRING • quit_commands_per_sec: INTEGER • quit_commands_per_sec_enum: STRING • search_commands: INTEGER • search_commands_enum: STRING • search_commands_per_sec: INTEGER • search_commands_per_sec_enum: STRING • stat_commands: INTEGER • stat_commands_enum: STRING • stat_commands_per_sec: INTEGER • stat_commands_per_sec_enum: STRING • takethis_commands: INTEGER • takethis_commands_enum: STRING • takethis_commands_per_sec: INTEGER • takethis_commands_per_sec_enum: STRING • xhdr_commands: INTEGER • xhdr_commands_enum: STRING • xhdr_commands_per_sec: INTEGER • xhdr_commands_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NNTP_Commands (Cont.)	• xover_commands: INTEGER • xover_commands_enum: STRING • xover_commands_per_sec: INTEGER • xover_commands_per_sec_enum: STRING • xpat_commands: INTEGER • xpat_commands_enum: STRING • xpat_commands_per_sec: INTEGER • xpat_commands_per_sec_enum: STRING • xreplic_commands: INTEGER • xreplic_commands_enum: STRING • xreplic_commands_per_sec: INTEGER • xreplic_commands_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NNTP_Server	ITM_NNTP_Server event class with these slots: • system_name: STRING • timestamp: STRING • nntp_server: STRING • article_map_entries: INTEGER • article_map_entries_enum: STRING • article_map_entries_per_sec: INTEGER • article_map_entries_per_sec_enum: STRING • articles_deleted: INTEGER • articles_deleted_enum: STRING • articles_deleted_per_sec: INTEGER • articles_deleted_per_sec_enum: STRING • articles_posted: INTEGER • articles_posted_enum:STRING • articles_posted_per_sec: INTEGER • articles_posted_per_sec_enum: STRING • articles_received: INTEGER • articles_received_enum: STRING • articles_received_per_sec: INTEGER • articles_received_per_sec_enum: STRING • articles_sent: INTEGER • articles_sent_enum: STRING • articles_sent_per_sec: INTEGER • articles_sent_per_sec_enum: STRING • articles_total: INTEGER • articles_total_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • control_messages_failed: INTEGER • control_messages_failed_enum: STRING • control_messages_received: INTEGER • control_messages_received_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NNTP_Server (continued)	• current_anonymous_users: INTEGER • current_anonymous_users_enum: STRING • current_connections: INTEGER • current_connections_enum: STRING • current_nonanonymous_users: INTEGER • current_nonanonymous_users_enum: STRING • current_outbound_connections: INTEGER • current_outbound_connections_enum: STRING • failed_outbound_logons: INTEGER • failed_outbound_logons_enum: STRING • history_map_entries: INTEGER • history_map_entries_enum: STRING • history_map_entries_per_sec: INTEGER • history_map_entries_per_sec_enum: STRING • maximum_anonymous_users: INTEGER • maximum_anonymous_users_enum: STRING • maximum_connections: INTEGER • maximum_connections_enum: STRING • maximum_nonanonymous_users: INTEGER • maximum_nonanonymous_users_enum: STRING • moderated_postings_failed: INTEGER • moderated_postings_failed_enum: STRING • moderated_postings_sent: INTEGER • moderated_postings_sent_enum: STRING • sessions_flow_controlled: INTEGER • sessions_flow_controlled_enum: STRING • total_anonymous_users: INTEGER • total_anonymous_users_enum: STRING • total_connections: INTEGER • total_connections_enum: STRING • total_nonanonymous_users: INTEGER • total_nonanonymous_users_enum: STRING • total_outbound_connections: INTEGER • total_outbound_connections_enum: STRING • total_outbound_connections_failed: INTEGER • total_outbound_connections_failed_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NNTP_Server (continued)	• total_passive_feeds: INTEGER • total_passive_feeds_enum: STRING • total_pull_feeds: INTEGER • total_pull_feeds_enum: STRING • total_push_feeds: INTEGER • total_push_feeds_enum: STRING • total_ssl_connections: INTEGER • total_ssl_connections_enum: STRING • xover_entries: INTEGER • xover_entries_enum: STRING • xover_entries_per_sec: INTEGER • xover_entries_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
SMTP_Server	ITM_SMTP_Server event class with these slots: • system_name: STRING • timestamp: STRING • smtp_server: STRING • pct__recipients_local: INTEGER • pct__recipients_remote: INTEGER • avg_recipients_per_msg_received: INTEGER • avg_recipients_per_msg_received_enum: STRING • avg_recipients_per_msg_sent: INTEGER • avg_recipients_per_msg_sent_enum: STRING • avg_retries_per_msg_delivered: INTEGER • avg_retries_per_msg_delivered_enum: STRING • avg_retries_per_msg_sent: INTEGER • avg_retries_per_msg_sent_enum: STRING • kbytes_received_total: INTEGER • kbytes_received_total_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • kbytes_sent_total: INTEGER • kbytes_sent_total_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • kbytes_total: INTEGER • kbytes_total_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • connection_errors_per_sec: INTEGER • connection_errors_per_sec_enum: STRING • directory_drops_total: INTEGER • directory_drops_total_enum: STRING • directory_drops_per_sec: INTEGER • directory_drops_per_sec_enum: STRING • directory_pickup_queue_length: INTEGER • directory_pickup_queue_length_enum: STRING • dns_queries_total: INTEGER • dns_queries_total_enum: STRING • dns_queries_per_sec: INTEGER • dns_queries_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
SMTP_Server (Continued)	• etrn_messages_total: INTEGER • etrn_messages_total_enum: STRING • etrn_messages_per_sec: INTEGER • etrn_messages_per_sec_enum: STRING • inbound_connections_current: INTEGER • inbound_connections_current_enum: STRING • inbound_connections_total: INTEGER • inbound_connections_total_enum: STRING • local_queue_length: INTEGER • local_queue_length_ enum: STRING • local_retry_queue_length: INTEGER • local_retry_queue_length_enum: STRING • message_kbytes_received_total: INTEGER • message_kbytes_received_total_enum: STRING • message_bytes_received_per_sec: INTEGER • message_bytes_received_per_sec_enum: STRING • message_kbytes_sent_total: INTEGER • message_kbytes_sent_total_enum: STRING • message_bytes_sent_per_sec: INTEGER • message_bytes_sent_per_sec_enum: STRING • message_kbytes_total: INTEGER • message_kbytes_total_enum: STRING • message_bytes_total_per_sec: INTEGER • message_bytes_total_per_sec_enum: STRING • message_delivery_retries: INTEGER • message_delivery_retries_enum: STRING • message_received_per_sec: INTEGER • message_received_per_sec_enum: STRING • message_send_retries: INTEGER • message_send_retries_enum: STRING • messages_delivered_total: INTEGER • messages_delivered_total_enum: STRING • messages_delivered_per_sec: INTEGER • messages_delivered_per_sec_enum: STRING • messages_received_total: INTEGER • messages_received_total_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
SMTP_Server (Continued)	• messages_refused_for_address_objects: INTEGER • messages_refused_for_address_objects _enum: STRING • messages_refused_for_mail_objects: INTEGER • messages_refused_for_mail_objects_enum: STRING • messages_refused_for_size: INTEGER • messages_refused_for_size_enum: STRING • messages_retrieved_total: INTEGER • messages_retrieved_total_enum: STRING • messages_retrieved_per_sec: INTEGER • messages_retrieved_per_sec_enum: STRING • messages_sent_total: INTEGER • messages_sent_total_enum: STRING • messages_sent_per_sec: INTEGER • messages_sent_per_sec_enum: STRING • ndrs_generated: INTEGER • ndrs_generated_enum: STRING • number_of_mailfiles_open: INTEGER • number_of_mailfiles_open_enum: INTEGER • number_of_queuefiles_open: INTEGER • number_of_queuefiles_open_enum: STRING • outbound_connections_current: INTEGER • outbound_connections_current_enum: STRING • outbound_connections_refused: INTEGER • outbound_connections_refused_enum: STRING • outbound_connections_total: INTEGER • outbound_connections_total_enum: STRING • remote_queue_length: INTEGER • remote_queue_length_enum: STRING • remote_retry_queue_length: INTEGER • remote_retry_queue_length_enum: STRING • routing_table_lookups_total: INTEGER

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
SMTP_Server (Continued)	• routing_table_lookups_total_enum: STRING • routing_table_lookups_per_sec: INTEGER • routing_table_lookups_per_sec_enum: STRING • total_connection_errors: INTEGER • total_connection_errors_enum: STRING
Job_Object	ITM_Job_Object event class with these slots: • system_name: STRING • timestamp: STRING • name: STRING • current_pct__kernel_mode_time: INTEGER • current_pct__processor_time: INTEGER • current_pct__user_mode_time: INTEGER • pages_per_sec: INTEGER • pages_per_sec_enum: STRING • process_count_active: INTEGER • process_count_active_enum: STRING • process_count_terminated: INTEGER • process_count_terminated_enum: STRING • process_count_total: INTEGER • process_count_total_enum: STRING • this_period_msec_kernel_mode: INTEGER • this_period_msec_kernel_mode_enum: STRING • this_period_msec_processor: INTEGER • this_period_msec_processor_enum: STRING • this_period_msec_user_mode: INTEGER • this_period_msec_user_mode_enum: STRING • total_msec_kernel_mode: INTEGER • total_msec_kernel_mode_enum: STRING • total_msec_processor: INTEGER • total_msec_processor_enum: STRING • total_msec_user_mode: INTEGER • total_msec_user_mode_enum: STRING • name_u: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Job_Object (Continued)	• this_period_msec_kernel_mode_64: INTEGER • this_period_msec_kernel_mode_64_enum: STRING • this_period_msec_processor_64: INTEGER • this_period_msec_processor_64_enum: STRING • this_period_msec_user_mode_64: INTEGER • this_period_msec_user_mode_64_enum: STRING • total_msec_kernel_mode_64: INTEGER • total_msec_kernel_mode_64_enum: STRING • total_msec_processor_64: INTEGER • total_msec_user_mode_64: INTEGER • total_msec_user_mode_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Job_Object_Details	ITM_NT_Job_Object_Details event class with these slots: • server_name: STRING • timestamp: STRING • process: STRING • pct__privileged_time: INTEGER • pct__processor_time: INTEGER • pct__user_time: INTEGER • creating_process_id: INTEGER • creating_process_id_enum: STRING • elapsed_time: INTEGER • elapsed_time_enum: STRING • handle_count: INTEGER • handle_count_enum: STRING • id_process: INTEGER • id_process_enum: STRING • io_data_bytes_per_sec: INTEGER • io_data_bytes_per_sec_enum: STRING • io_data_operations_per_sec: INTEGER • io_data_operations_per_sec_enum: STRING • io_other_bytes_per_sec: INTEGER • io_other_bytes_per_sec_enum: STRING • io_other_operations_per_sec: INTEGER • io_other_operations_per_sec_enum: STRING • io_read_bytes_per_sec: INTEGER • io_read_bytes_per_sec_enum: STRING • io_read_operations_per_sec: INTEGER • io_read_operations_per_sec_enum: STRING • io_write_bytes_per_sec: INTEGER • io_write_bytes_per_sec_enum: STRING • io_write_operations_per_sec: INTEGER • io_write_operations_per_sec_enum: STRING • page_faults_per_sec: INTEGER • page_faults_per_sec_enum: STRING • page_file_bytes: INTEGER • page_file_bytes_enum: STRING • page_file_bytes_peak: INTEGER • page_file_bytes_peak_enum: STRING • page_file_kbytes: INTEGER • page_file_kbytes_enum: STRING • page_file_kbytes_peak: INTEGER • page_file_kbytes_peak_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Job_Object_Details (Continued)	• pool_nonpaged_bytes: INTEGER • pool_nonpaged_bytes_enum: STRING • pool_paged_bytes: INTEGER • pool_paged_bytes_enum: STRING • priority_base: INTEGER • priority_base_enum: STRING • private_bytes: INTEGER • private_bytes_enum: STRING • private_kbytes: INTEGER • private_kbytes_enum: STRING • thread_count: INTEGER • thread_count_enum: STRING • virtual_bytes: INTEGER • virtual_bytes_enum: STRING • virtual_bytes_peak: INTEGER • virtual_bytes_peak_enum: STRING • virtual_kbytes: INTEGER • virtual_kbytes_enum: STRING • virtual_kbytes_peak: INTEGER • virtual_kbytes_peak_enum: STRING • working_set: INTEGER • working_set_enum: STRING • working_set_peak: INTEGER • working_set_peak_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Job_Object_Details	ITM_Job_Object_Details event class with these slots: • server_name: STRING • timestamp: STRING • process: STRING • pct__privileged_time: INTEGER • pct__processor_time: INTEGER • pct__user_time: INTEGER • creating_process_id: INTEGER • creating_process_id_enum: STRING • elapsed_time: INTEGER • elapsed_time_enum: STRING • handle_count: INTEGER • handle_count_enum: STRING • id_process: INTEGER • id_process_enum: STRING • io_data_bytes_per_sec: INTEGER • io_data_bytes_per_sec_enum: STRING • io_data_operations_per_sec: INTEGER • io_data_operations_per_sec_enum: STRING • io_other_bytes_per_sec: INTEGER • io_other_bytes_per_sec_enum: STRING • io_other_operations_per_sec: INTEGER • io_other_operations_per_sec_enum: STRING • io_read_bytes_per_sec: INTEGER • io_read_bytes_per_sec_enum: STRING • io_read_operations_per_sec: INTEGER • io_read_operations_per_sec_enum: STRING • io_write_bytes_per_sec: INTEGER • io_write_bytes_per_sec_enum: STRING • io_write_operations_per_sec: INTEGER • io_write_operations_per_sec_enum: STRING • page_faults_per_sec: INTEGER • page_faults_per_sec_enum: STRING • page_file_bytes: INTEGER • page_file_bytes_enum: STRING • page_file_bytes_peak: INTEGER • page_file_bytes_peak_enum: STRING • pool_nonpaged_bytes: INTEGER • pool_nonpaged_bytes_enum: STRING • pool_paged_bytes: INTEGER • pool_paged_bytes_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Job_Object_Details (Continued)	• priority_base: INTEGER • private_bytes: INTEGER • private_bytes_enum: STRING • thread_count: INTEGER • thread_count_enum: STRING • virtual_bytes: INTEGER • virtual_bytes_enum: STRING • virtual_bytes_peak: INTEGER • virtual_bytes_peak_enum: STRING • working_set: INTEGER • working_set_enum: STRING • working_set_peak: INTEGER • working_set_peak_enum: STRING • page_file_kbytes: INTEGER • page_file_kbytes_enum: STRING • page_file_kbytes_peak: INTEGER • page_file_kbytes_peak_enum: STRING • private_kbytes: INTEGER • private_kbytes_enum: STRING • virtual_kbytes: INTEGER • virtual_kbytes_enum: STRING • virtual_kbytes_peak: INTEGER • virtual_kbytes_peak_enum: STRING • process_u: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DHCP_Server	ITM_DHCP_Server event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • acks_per_sec: INTEGER • acks_per_sec_enum: STRING • active_queue_length: INTEGER • active_queue_length_enum: STRING • conflict_check_queue_length: INTEGER • conflict_check_queue_length_enum: STRING • declines_per_sec: INTEGER • declines_per_sec_enum: STRING • discovers_per_sec: INTEGER • discovers_per_sec_enum: STRING • duplicates_dropped_per_sec: INTEGER • duplicates_dropped_per_sec_enum: STRING • informs_per_sec: INTEGER • informs_per_sec_enum: STRING • milliseconds_per_packet_average: INTEGER • milliseconds_per_packet_average_enum: STRING • nacks_per_sec: INTEGER • nacks_per_sec_enum: STRING • offers_per_sec: INTEGER • offers_per_sec_enum: STRING • packets_expired_per_sec: INTEGER • packets_expired_per_sec_enum: STRING • packets_received_per_sec: INTEGER • packets_received_per_sec_enum: STRING • releases_per_sec: INTEGER • releases_per_sec_enum: STRING • requests_per_sec: INTEGER • requests_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DNS_Memory	ITM_DNS_Memory event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • caching_memory: INTEGER • caching_memory_enum: STRING • database_node_memory: INTEGER • database_node_memory_enum: STRING • nbstat_memory: INTEGER • nbstat_memory_enum: STRING • record_flow_memory: INTEGER • record_flow_memory_enum: STRING • tcp_message_memory: INTEGER • tcp_message_memory_enum: STRING • udp_message_memory: INTEGER • udp_message_memory_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DNS_Zone_Transfer	ITM_DNS_Zone_Transfer event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • axfr_request_received: INTEGER • axfr_request_received_enum: STRING • axfr_request_sent: INTEGER • axfr_request_sent_enum: STRING • axfr_response_received: INTEGER • axfr_response_received_enum: STRING • axfr_success_received: INTEGER • axfr_success_received_enum: STRING • axfr_success_sent: INTEGER • axfr_success_sent_enum: STRING • ixfr_request_received: INTEGER • ixfr_request_received_enum: STRING • ixfr_request_sent: INTEGER • ixfr_request_sent_enum: STRING • ixfr_response_received: INTEGER • ixfr_response_received_enum: STRING • ixfr_success_received: INTEGER • ixfr_success_received_enum: STRING • ixfr_success_sent: INTEGER • ixfr_success_sent_enum: STRING • ixfr_tcp_success_received: INTEGER • ixfr_tcp_success_received_enum: STRING • ixfr_udp_success_received: INTEGER • ixfr_udp_success_received_enum: STRING • notify_received: INTEGER • notify_received_enum: STRING • notify_sent: INTEGER • notify_sent_enum: STRING • zone_transfer_failure: INTEGER • zone_transfer_failure_enum: STRING • zone_transfer_request_received: INTEGER • zone_transfer_request_received_enum: STRING • zone_transfer_soa_request_sent: INTEGER • zone_transfer_soa_request_sent_enum: STRING • zone_transfer_success: INTEGER • zone_transfer_success_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DNS_Dynamic_Update	ITM_DNS_Dynamic_Update event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • dynamic_update_nooperation: INTEGER • dynamic_update_nooperation_enum: STRING • dynamic_update_nooperation_per_sec: INTEGER • dynamic_update_nooperation_per_sec _enum: STRING • dynamic_update_queued: INTEGER • dynamic_update_queued_enum: STRING • dynamic_update_received: INTEGER • dynamic_update_received_enum: STRING • dynamic_update_received_per_sec: INTEGER • dynamic_update_received_per_sec_enum: STRING • dynamic_update_rejected: INTEGER • dynamic_update_rejected_enum: STRING • dynamic_update_timeouts: INTEGER • dynamic_update_timeouts_enum: STRING • dynamic_update_written_to_database: INTEGER • dynamic_update_written_to_database _enum: STRING • dynamic_update_written_to_database_ per_sec: INTEGER • dynamic_update_written_to_database_ per_sec_enum: STRING • secure_update_failure: INTEGER • secure_update_failure_enum: STRING • secure_update_received: INTEGER • secure_update_received_enum: STRING • secure_update_received_per_sec: INTEGER • secure_update_received_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DNS_Query	ITM_DNS_Query event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • recursive_queries: INTEGER • recursive_queries_enum: STRING • recursive_queries_per_sec: INTEGER • recursive_queries_per_sec_enum: STRING • recursive_query_failure: INTEGER • recursive_query_failure_enum: STRING • recursive_query_failure_per_sec: INTEGER • recursive_query_failure_per_sec_enum: STRING • recursive_send_timeouts: INTEGER • recursive_send_timeouts_enum: STRING • recursive_timeout_per_sec: INTEGER • recursive_timeout_per_sec_enum: STRING • tcp_query_received: INTEGER • tcp_query_received_enum: STRING • tcp_query_received_per_sec: INTEGER • tcp_query_received_per_sec_enum: STRING • tcp_response_sent: INTEGER • tcp_response_sent_enum: STRING • tcp_response_sent_per_sec: INTEGER • tcp_response_sent_per_sec_enum: STRING • total_query_received: INTEGER • total_query_received_enum: STRING • total_query_received_per_sec: INTEGER • total_query_received_per_sec_enum: STRING • total_response_sent: INTEGER • total_response_sent_enum: STRING • total_response_sent_per_sec: INTEGER • total_response_sent_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
DNS_Query (Continued)	• udp_query_received: INTEGER • udp_query_received_enum: STRING • udp_query_received_per_sec: INTEGER • udp_query_received_per_sec_enum: STRING • udp_response_sent: INTEGER • udp_response_sent_enum: STRING • udp_response_sent_per_sec: INTEGER • udp_response_sent_per_sec_enum: STRING
DNS_WINS	ITM_DNS_WINS event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • wins_lookup_received: INTEGER • wins_lookup_received_enum: STRING • wins_lookup_received_per_sec: INTEGER • wins_lookup_received_per_sec_enum: STRING • wins_response_sent: INTEGER • wins_response_sent_enum: STRING • wins_response_sent_per_sec: INTEGER • wins_response_sent_per_sec_enum: STRING • wins_reverse_lookup_received: INTEGER • wins_reverse_lookup_received_enum: STRING • wins_reverse_lookup_received_per_sec: INTEGER • wins_reverse_lookup_received_per_sec _enum: STRING • wins_reverse_response_sent: INTEGER • wins_reverse_response_sent_enum: STRING • wins_reverse_response_sent_per_sec: INTEGER • wins_reverse_response_sent_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Print_Queue	ITM_Print_Queue event class with these slots: • system_name: STRING • timestamp: STRING • name: STRING • add_network_printer_calls: INTEGER • add_network_printer_calls_enum: STRING • bytes_printed_per_sec: INTEGER • bytes_printed_per_sec_enum: STRING • enumerate_network_printer_calls: INTEGER • enumerate_network_printer_calls_enum: STRING • job_errors: INTEGER • job_errors_enum: STRING • jobs: INTEGER • jobs_enum: STRING • jobs_spooling: INTEGER • jobs_spooling_enum: STRING • max_jobs_spooling: INTEGER • max_jobs_spooling_enum: STRING • max_references: INTEGER • max_references_enum: STRING • not_ready_errors: INTEGER • not_ready_errors_enum: STRING • out_of_paper_errors: INTEGER • out_of_paper_errors_enum: STRING • references: INTEGER • references_enum: STRING • total_jobs_printed: INTEGER • total_jobs_printed_enum: STRING • total_pages_printed: INTEGER • total_pages_printed_enum: STRING • name_u: STRING • average_job_errors_per_day: INTEGER • average_job_errors_per_day_enum: STRING • average_not_ready_errors_per_day: INTEGER • average_not_ready_errors_per_day_enum: STRING • average_out_of_paper_errors_per_day: INTEGER • average_out_of_paper_errors_per_day _enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
Print_Queue (Continued)	• bytes_printed_per_sec_64: INTEGER • bytes_printed_per_sec_64_enum: STRING • total_jobs_printed_64: INTEGER • total_jobs_printed_64_enum: STRING • total_pages_printed_64: INTEGER • total_pages_printed_64_enum: STRING
NT_Thread	ITM_NT_Thread event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • thread_instance: STRING • id_process: INTEGER • id_thread: INTEGER • pct__privileged_time: INTEGER • pct__processor_time: INTEGER • pct__user_time: INTEGER • context_switches_per_sec: INTEGER • context_switches_per_sec_enum: STRING • elapsed_time: INTEGER • elapsed_time_enum: STRING • priority_base: INTEGER • priority_base_enum: STRING • priority_current: INTEGER • priority_current_enum: STRING • start_address: INTEGER • thread_state: INTEGER • thread_wait_reason: INTEGER

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Server	ITM_NT_Server event class with these slots: • server_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • blocking_requests_rejected: INTEGER • blocking_requests_rejected_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • bytes_transmitted_per_sec: INTEGER • bytes_transmitted_per_sec_enum: STRING • context_blocks_queued_per_sec: INTEGER • context_blocks_queued_per_sec_enum: STRING • errors_access_permissions: INTEGER • errors_access_permissions_enum: STRING • errors_granted_access: INTEGER • errors_granted_access_enum: STRING • errors_logon: INTEGER • errors_logon_enum: STRING • errors_system: INTEGER • errors_system_enum: STRING • file_directory_searches: INTEGER • file_directory_searches_enum: STRING • files_open: INTEGER • files_open_enum: STRING • files_opened_total: INTEGER • files_opened_total_enum: STRING • logon_total: INTEGER • logon_total_enum: STRING • logon_per_sec: INTEGER • logon_per_sec_enum: STRING • pool_nonpaged_bytes: INTEGER • pool_nonpaged_bytes_enum: STRING • pool_nonpaged_failures: INTEGER • pool_nonpaged_failures_enum: STRING • pool_nonpaged_peak: INTEGER • pool_nonpaged_peak_enum: STRING • pool_paged_bytes: INTEGER • pool_paged_bytes_enum: STRING • pool_paged_failures: INTEGER • pool_paged_failures_enum: STRING • pool_paged_peak: INTEGER • pool_paged_peak_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Server (Continued)	• server_sessions: INTEGER • server_sessions_enum: STRING • sessions_errored_out: INTEGER • sessions_errored_out_enum: STRING • sessions_forced_off: INTEGER • sessions_forced_off_enum: STRING • sessions_logged_off: INTEGER • sessions_logged_off_enum: STRING • sessions_timed_out: INTEGER • sessions_timed_out_enum: STRING • work_item_shortages: INTEGER • work_item_shortages_enum: STRING • total_ended_sessions: INTEGER • total_ended_sessions_enum: STRING • error_session_percent: INTEGER • high_pct__bytes_per_sec: INTEGER • high_pct__bytes_per_sec_enum: STRING • bytes_received_per_sec_64: INTEGER • bytes_received_per_sec_64_enum: STRING • bytes_total_per_sec_64: INTEGER • bytes_total_per_sec_64_enum: STRING • bytes_transmitted_per_sec_64: INTEGER • bytes_transmitted_per_sec_64_enum: STRING • total_ended_sessions_64: INTEGER • total_ended_sessions_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Server_Work_Queues_64	ITM_NT_Server_Work_Queues_64 event class with these slots: • server_name: STRING • timestamp: STRING • work_queue_name: STRING • active_threads: INTEGER • active_threads_enum: STRING • available_threads: INTEGER • available_threads_enum: STRING • available_work_items: INTEGER • available_work_items_enum: STRING • borrowed_work_items: INTEGER • borrowed_work_items_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • bytes_transferred_per_sec: INTEGER • bytes_transferred_per_sec_enum: STRING • context_blocks_queued_per_sec: INTEGER • context_blocks_queued_per_sec_enum: STRING • current_clients: INTEGER • current_clients_enum: STRING • queue_length: INTEGER • queue_length_enum: STRING • read_bytes_per_sec: INTEGER • read_bytes_per_sec_enum: STRING • read_operations_per_sec: INTEGER • read_operations_per_sec_enum: STRING • total_bytes_per_sec: INTEGER • total_bytes_per_sec_enum: STRING • total_operations_per_sec: INTEGER • total_operations_per_sec_enum: STRING • work_item_shortages: INTEGER • write_bytes_per_sec: INTEGER • write_bytes_per_sec_enum: STRING • write_operations_per_sec: INTEGER • write_operations_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Server_Work_Queues	ITM_NT_Server_Work_Queues event class with these slots: • server_name: STRING • timestamp: STRING • work_queue_name: STRING • active_threads: INTEGER • active_threads_enum: STRING • available_threads: INTEGER • available_threads_enum: STRING • available_work_items: INTEGER • available_work_items_enum: STRING • borrowed_work_items: INTEGER • borrowed_work_items_enum: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_sent_per_sec: INTEGER • bytes_sent_per_sec_enum: STRING • bytes_transferred_per_sec: INTEGER • bytes_transferred_per_sec_enum: STRING • context_blocks_queued_per_sec: INTEGER • context_blocks_queued_per_sec_enum: STRING • current_clients: INTEGER • current_clients_enum: STRING • queue_length: INTEGER • queue_length_enum: STRING • read_bytes_per_sec: INTEGER • read_bytes_per_sec_enum: STRING • read_operations_per_sec: INTEGER • read_operations_per_sec_enum: STRING • total_bytes_per_sec: INTEGER • total_bytes_per_sec_enum: STRING • total_operations_per_sec: INTEGER • total_operations_per_sec_enum: STRING • work_item_shortages: INTEGER • work_item_shortages_enum: STRING • write_bytes_per_sec: INTEGER • write_bytes_per_sec_enum: STRING • write_operations_per_sec: INTEGER • write_operations_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Registry	ITM_NT_Registry event class with these slots: • server_name: STRING • timestamp: STRING • root_key_name: INTEGER • root_key_name_enum: STRING • path_name: STRING • type: INTEGER • type_enum: STRING • string_value: STRING • numeric_value: INTEGER
Process_IO	ITM_Process_IO event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • process_name: STRING • id_process: INTEGER • io_data_bytes_per_sec: INTEGER • io_data_bytes_per_sec_enum: STRING • io_data_operations_per_sec: INTEGER • io_data_operations_per_sec_enum: STRING • io_other_bytes_per_sec: INTEGER • io_other_bytes_per_sec_enum: STRING • io_other_operations_per_sec: INTEGER • io_other_operations_per_sec_enum: STRING • io_read_bytes_per_sec: INTEGER • io_read_bytes_per_sec_enum: STRING • io_read_operations_per_sec: INTEGER • io_read_operations_per_sec_enum: STRING • io_write_bytes_per_sec: INTEGER • io_write_bytes_per_sec_enum: STRING • io_write_operations_per_sec: INTEGER • io_write_operations_per_sec_enum: STRING • binary_path: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Redirector	ITM_NT_Redirector event class with these slots: • system_name: STRING • timestamp: STRING • parameter: STRING • knt_value: STRING • bytes_received_per_sec: INTEGER • bytes_received_per_sec_enum: STRING • bytes_total_per_sec: INTEGER • bytes_total_per_sec_enum: STRING • bytes_transmitted_per_sec: INTEGER • bytes_transmitted_per_sec_enum: STRING • connects_core: INTEGER • connects_core_enum: STRING • connects_lan_manager_20: INTEGER • connects_lan_manager_20_enum: STRING • connects_lan_manager_21: INTEGER • connects_lan_manager_21_enum: STRING • connects_windows_nt: INTEGER • connects_windows_nt_enum: STRING • current_commands: INTEGER • current_commands_enum: STRING • file_data_operations_per_sec: INTEGER • file_data_operations_per_sec_enum: STRING • file_read_operations_per_sec: INTEGER • file_read_operations_per_sec_enum: STRING • file_write_operations_per_sec: INTEGER • file_write_operations_per_sec_enum: STRING • network_errors_per_sec: INTEGER • network_errors_per_sec_enum: STRING • packets_received_per_sec: INTEGER • packets_received_per_sec_enum: STRING • packets_transmitted_per_sec: INTEGER • packets_transmitted_per_sec_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Redirector (continued)	• packets_per_sec: INTEGER • packets_per_sec_enum: STRING • read_bytes_cache_per_sec: INTEGER • read_bytes_cache_per_sec_enum: STRING • read_bytes_network_per_sec: INTEGER • read_bytes_network_per_sec_enum: STRING • read_bytes_non-paging_per_sec: INTEGER • read_bytes_non-paging_per_sec_enum: STRING • read_bytes_paging_per_sec: INTEGER • read_bytes_paging_per_sec_enum: STRING • read_operations_random_per_sec: INTEGER • read_operations_random_per_sec_enum: STRING • read_packets_small_per_sec: INTEGER • read_packets_small_per_sec_enum: STRING • read_packets_per_sec: INTEGER • read_packets_per_sec_enum: STRING • reads_denied_per_sec: INTEGER • reads_denied_per_sec_enum: STRING • reads_large_per_sec: INTEGER • reads_large_per_sec_enum: STRING • server_disconnects: INTEGER • server_disconnects_enum: STRING • server_reconnects: INTEGER • server_reconnects_enum: STRING • server_sessions: INTEGER • server_sessions_enum: STRING • server_sessions_hung: INTEGER • server_sessions_hung_enum: STRING • write_bytes_cache_per_sec: INTEGER • write_bytes_cache_per_sec_enum: STRING • write_bytes_network_per_sec: INTEGER • write_bytes_network_per_sec_enum: STRING • write_bytes_non-paging_per_sec: INTEGER • write_bytes_non-paging_per_sec_enum: STRING • write_bytes_paging_per_sec: INTEGER • write_bytes_paging_per_sec_enum:STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Redirector (continued)	• write_operations_random_per_sec: INTEGER • write_operations_random_per_sec_enum: STRING • write_packets_small_per_sec: INTEGER • write_packets_small_per_sec_enum: STRING • write_packets_per_sec: INTEGER • write_packets_per_sec_enum: STRING • writes_denied_per_sec: INTEGER • writes_denied_per_sec_enum: STRING • writes_large_per_sec: INTEGER • writes_large_per_sec_enum: STRING • high_pct__bytes_per_sec: INTEGER • high_pct__bytes_per_sec_enum: STRING • high_current_mod: INTEGER • high_current_mod_enum: STRING • bytes_received_per_sec_64: INTEGER • bytes_received_per_sec_64_enum: STRING • bytes_total_per_sec_64: INTEGER • bytes_total_per_sec_64_enum: STRING • bytes_transmitted_per_sec_64: INTEGER • bytes_transmitted_per_sec_64_enum: STRING • packets_per_sec_64: INTEGER • packets_per_sec_64_enum: STRING • packets_received_per_sec_64: INTEGER • packets_received_per_sec_64_enum: STRING • packets_transmitted_per_sec_64: INTEGER • packets_transmitted_per_sec_64_enum: STRING • read_bytes_cache_per_sec_64: INTEGER • read_bytes_cache_per_sec_64_enum: STRING • read_bytes_network_per_sec_64: INTEGER • read_bytes_network_per_sec_64_enum: STRING • read_bytes_non-paging_per_sec_64: INTEGER • read_bytes_non-paging_per_sec_64_enum: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Redirector (continued)	• read_bytes_paging_per_sec_64: INTEGER • read_bytes_paging_per_sec_64_enum: STRING • write_bytes_cache_per_sec_64: INTEGER • write_bytes_cache_per_sec_64_enum: STRING • write_bytes_network_per_sec_64: INTEGER • write_bytes_network_per_sec_64_enum: STRING • write_bytes_non-paging_per_sec_64: INTEGER • write_bytes_non-paging_per_sec_64_enum: STRING • write_bytes_paging_per_sec_64: INTEGER • write_bytes_paging_per_sec_64_enum: STRING
NT_Network_Port	ITM_NT_Network_Port event class with these slots: • system_name: STRING • timestamp: STRING • protocol: STRING • local_port: INTEGER • remote_port: INTEGER • remote_port_enum: STRING • local_port_name: STRING • state: INTEGER • state_enum: STRING • local_host_ip_address: STRING • local_host_name: STRING • remote_host_ip_address: STRING • remote_host_name: STRING;

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Processor_Summary	ITM_NT_Processor_Summary event class with these slots: • server_name: STRING • timestamp: STRING • high_processor: STRING • high_pct__processor_time: INTEGER • high_pct__privileged_time: INTEGER • high_pct__user_time: INTEGER • high_pct__interrupt_time: INTEGER • high_interrupts_per_sec: INTEGER • high_interrupts_per_sec_enum: STRING • low_processor: STRING • low_pct__processor_time: INTEGER • low_pct__privileged_time: INTEGER • low_pct__user_time: INTEGER • low_pct__interrupt_time: INTEGER • low_interrupts_per_sec: INTEGER • low_interrupts_per_sec_enum: STRING • processor_utilization_difference: INTEGER • processor_utilization_difference_enum: STRING • processor_privileged_difference: INTEGER • processor_privileged_difference_enum: STRING • processor_user_difference: INTEGER • processor_user_difference_enum: STRING • processor_interrupt_difference: INTEGER • processor_interrupt_difference_enum: STRING • high_process_name: STRING • high_process_id: INTEGER • high_process_utilization: INTEGER • high_process_utilization_enum: STRING • high_process_avg_utilization: INTEGER •

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_Processor_Information	ITM_NT_Processor_Information event class with these slots: • system_name: STRING • timestamp: STRING • processor_device_id: STRING • processor_address_width: STRING • processor_data_width: STRING • current_clock_speed: STRING • maximum_clock_speed: STRING • l2_cache_size: STRING • load_percentage: STRING • socket_designation: STRING • processor_name: STRING • processor_manufacturer: STRING • processor_description: STRING • power_management_support: STRING • processor_id: STRING • processor_version: STRING
NT_BIOS_Information	ITM_NT_BIOS_Information event class with these slots: • system_name: STRING • timestamp: STRING • bios_version: STRING • bios_description: STRING • bios_manufacturer: STRING • bios_release_date: STRING • bios_serial_number: STRING
NT_Computer_Information	ITM_NT_Computer_Information event class with these slots: • system_name: STRING • timestamp: STRING • computer_system_description: STRING • computer_id_number: STRING • computer_name: STRING • computer_uuid_number: STRING • computer_vendor: STRING • computer_version: STRING • computer_hostname: STRING • computer_domain_name: STRING

Table 22. Overview of attribute groups to event classes and slots (continued)

Attribute group	event class and slots
NT_IP_Address	ITM_NT_IP_Address event class with these slots: • system_name: STRING • timestamp: STRING • network_interface_name: STRING • network_interface_name_enum: STRING • ip_address: STRING • dns_name: STRING • dns_name_enum: STRING
NT_Mount_Points	ITM_NT_Mount_Points event class with these slots: • system_name: STRING • timestamp: STRING • drive_name: STRING • mounted_volume_name: STRING • mount_point: STRING • mount_point_state: STRING • mount_point_state_enum: STRING;

Appendix D. Monitoring Agent for Windows data collection

The Monitoring Agent for Windows gathers data when requested to satisfy a workspace refresh, situation sampling of attributes, or historical data collection. All attributes in the attribute groups that make up a workspace or situation are gathered at that time. The default refresh/sampling intervals were chosen so that the agent does not put a significant load on the system as it gathers the data.

Most of the attributes gathered by the Monitoring Agent for Windows come from Performance Monitors (Perfmon). A few Application Programming Interfaces (API) and Windows Management Instrumentations (WMI) are used.

The following table shows each attribute group and the mechanism used to gather the attributes:

Table 23. Mechanisms used to gather attributes

Attribute group	Collection methods	Perfmon/API name
Active Server Pages	Perfmon	Active Server Pages
Agent Availability Management Status	API	Proxy Agent Services API
Agent Active Runtime Status	API	Windows Service Control Manager, NtQueryInformationProcess APIs
Alerts Table	API	Proxy Agent Services API
BIOS Information	WMI	Win32_BIOS
Cache	Perfmon	Cache
Computer Information	WMI	Win32_ ComputerSystemProduct
Configuration Information	API	eXpat parser API, Proxy Agent Services API
Device Dependencies	API	Windows Service Control Manager APIs
DHCP Server	Perfmon	DHCP Server
DNS Dynamic Update	Perfmon	DNS
DNS Memory	Perfmon	DNS
DNS Query	Perfmon	DNS
DNS WINS	Perfmon	DNS
DNS Zone Transfer	Perfmon	DNS
Devices	API	Windows SCM APIs
Event Log	API	Windows File System and Event Log APIs
File Change	API	Windows File System APIs
File Trend	API	Windows file system APIs
FTP Server Statistics	Perfmon	FTP Server
FTP Service	Perfmon	FTP Service

Table 23. Mechanisms used to gather attributes (continued)

Attribute group	Collection methods	Perfmon/API name
Gopher Service	Perfmon	Gopher Service
HTTP Content Index	Perfmon	HTTP Content Index
HTTP Service	Perfmon	HTTP Service
ICMP Statistics	Perfmon	ICMP
IIS Statistics	Perfmon	Internet Information Services Global
Indexing Service	Perfmon	Indexing Service
Indexing Service Filter	Perfmon	Indexing Service Filter
IP Address	API	GetAdaptersAddresses **Note:** Not supported on Windows 2000.
IP Statistics	Perfmon	IP
Job Object	Perfmon	Job Object
Job Object Details	Perfmon	Job Object Details
Job Object Details (64-bit version)	Perfmon	Job Object Details
Logical Disk	Perfmon	Logical Disk
Memory	Perfmon	Memory
Memory (64-bit version)	Perfmon	Memory
Monitored Logs	API	Windows file system and Event Log APIs
Mount Point	API	GetVolumeNameForVolume MountPoint
MSMQ Information Store	Perfmon	MSMQ IS
MSMQ Queue	Perfmon	MSMQ Queue
MSMQService	Perfmon	MSMQ Service
MSMQ Sessions	Perfmon	MSMQ Sessions
Network Interface	Perfmon	Network Interface
Network Interface (64-bit version)	Perfmon	Network Interface
Network Port	API	GetTcpTable(), GetUcpTable()
Network Segment	Perfmon	Network Segment
NNTP Commands	Perfmon	Network Commands
NNTP Server	Perfmon	NNTP Server
Objects	Perfmon	Objects
Paging File	Perfmon	Paging File
Physical Disk	Perfmon	Physical Disk
Print Job	API	Windows Printer APIs
Printer	API	Windows Printer APIs
Print Queue	Perfmon	Print Queue
Process	Perfmon/API	Process, Windows APIs
Process (64-bit version)	Perfmon	Process

Table 23. Mechanisms used to gather attributes (continued)

Attribute group	Collection methods	Perfmon/API name
Process IO	Perfmon	Process
Processor	Perfmon	Processor
Processor Information	WMI	Win32_Processor
Processor Summary	Perfmon	Processor, Process
RAS Port	Perfmon	RAS Port
RAS Total	Perfmon	RAS Total
Redirector	Perfmon	Redirector
Registry	API	Windows Registry APIs
Server	Perfmon	Server
Server Work Queues	Perfmon	Server Work Queues
Server Work Queues (64-bit version)	Perfmon	Server Work Queues
Service Dependencies	API	Windows SCM APIs
Services	API	Windows APIs
SMTP Server	Perfmon	SMTP Server
System	Perfmon/API	Process, System, Windows APIs
TCP Statistics	Perfmon	TCP
Thread	Perfmon	Thread
UDP Statistics	Perfmon	UDP
Web Service	Perfmon	Web Service

Appendix E. Discovery Library Adapter for the monitoring agent

This chapter contains information about the Discovery Library Adapter (DLA) for the Monitoring Agent for Windows.

About the DLA

The Tivoli Management Services DLA discovers resources and relationships and creates a Discovery Library Book file. The Book follows the Discovery Library IdML schema version 2.9.2 and is used to populate the Configuration Management Database (CMDB) and Tivoli Business System Management products. The Tivoli Management Services DLA discovers Windows resources. For all Windows systems that are active and online at the Tivoli Enterprise Portal Server, information is included in the discovery book for those resources. The Tivoli Management Services DLA discovers active resources. It is run on-demand and can be run periodically to discover resources that were not active during previous discoveries.

The DLA discovers Windows components.

Note: Because the Monitoring Agent for Windows is not able to discover IP addresses for Windows 2000 systems, the Tivoli Management Services DLA cannot create the IP address elements that are required for the discovery book. Therefore, only the TMSAgent CDM object is created in the book for Windows 2000 systems.

More information about DLAs

The following sources contain additional information about using the DLA program with all monitoring agents:

- The *IBM Tivoli Monitoring Administrator's Guide* contains information about using the Tivoli Management Services Discovery Library Adapter.
- For information about using a DLA with Tivoli Application Dependency Discovery Manager (TADDM), see the information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v10r1/topic/com.ibm.taddm.doc_7.1/cmdb_welcome.html

Windows data model class types represented in CDM

This section contains information about how the various source application data objects map to classes in the Common Data Model (CDM) for the Monitoring Agent for Windows.

The following information is provided for each class where appropriate:

Relationships
CDM relationships (hierarchical) between currently identified model objects

CDM attributes, agent attributes, descriptions, and examples
CDM and agent attributes that are required to create an instance of a resource, descriptions of the attributes, and examples of the attributes

WindowsOperatingSystem class

The following information describes the WindowsOperatingSystem class.

CDM class name

sys.windows.WindowsOperatingSystem

Relationships

- installedOn
- runsOn

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: ManagedSystemName
  Agent attribute: none
  Description: Managed System Name
- CDM attribute: OSVersion
  Agent attribute: VERSION/WTSYSTEM
  Description: OS VERSION
- CDM attribute: Name
  Agent attribute: none
  Description: "Windows"
- CDM attribute: OSName
  Agent attribute: OSTYPE/WTSYSTEM
  Description: Windows type
- CDM attribute: FQDN
  Agent attribute: DNSNAME/NTIPADDR
  Description: Fully Qualified Domain Name

ComputerSystem class

The following information describes the ComputerSystem class.

CDM class name

sys.ComputerSystem

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: ManagedSystemName
  Agent attribute: none
  Description: Managed System Name
- CDM attribute: Name
  Agent attribute: none
  Description: Fully Qualified Host Name
- CDM attribute: Signature
  Agent attribute: IPADDRESS/NTIPADDR and MACADDRESS/NTIPADDR
  Description: Lowest IP Address (MAC Address)
- CDM attribute: PrimaryMACAddress
  Agent attribute: MACADDRESS/NTIPADDR
  Description: MAC Address of the network interface with the lowest IP Address (alpha order)
- CDM attribute: Type
  Agent attribute: none
  Description: "ComputerSystem"
- CDM attribute: Fqdn
  Agent attribute: DNSNAME/NTIPADDR
  Description: Fully Qualified Domain Name

- CDM attribute: SystemBoardUUID
  Agent attribute: COMPUUID/NTCOMPINFO
  Description: System Board UUID
- CDM attribute: SerialNumber
  Agent attribute: COMPUUID/NTCOMPINFO
  Description: Serial number
- CDM attribute: Model
  Agent attribute: COMPNAME/NTCOMPINFO
  Description: Model
- CDM attribute: Manufacturer
  Agent attribute: COMPVEND/NTCOMPINFO
  Description: Manufacturer
- CDM attribute: Label
  Agent attribute: none
  Description: Fully Qualified Host Name

IpInterface class

The following information describes the IpInterface class.

CDM class name
net.IpInterface

Relationships

- contains

CDM attributes, agent attributes, descriptions, and examples
none

IpV4Address class

The following information describes the IpV4Address class.

CDM class name
net.IpV4Address

Relationships

- bindsTo

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: DotNotation
  Agent attribute: IPADDRESS/NTIPADDR
  Description: IP Address of the network interface
- CDM attribute: Label
  Description: IP Address of the network interface

IpV6Address class

The following information describes the IpV6Address class.

CDM class name
net.IpV6Address

Relationships
bindsTo

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: StringNotation
  Agent attribute: IPADDRESS/NTIPADDR
  Description: IP Address of the network interface

- CDM attribute: Label
  Description: IP Address of the network interface

Fqdn class

The following information describes the Fqdn class.

CDM class name
net.Fqdn

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: Fqdn
  Agent attribute: DNSNAME/NTIPADDR
  Description: Fully Qualified Domain Name for the network interface

TMSAgent class

The following information describes the TMSAgent class.

CDM class name
app.TMSAgent

Relationships

- installedOn
- monitors

CDM attributes, agent attributes, descriptions, and examples

- CDM attribute: ManagedSystemName
  Agent attribute: none
  Description: Managed System Name
- CDM attribute: ManagedObjectName
  Description: "p@" Managed System Name
- CDM attribute: SoftwareVersion
  Description: OS Agent ITM version
- CDM attribute: ProductCode
  Description: OS Agent Product Code (NT)
- CDM attribute: Affinity
  Description: OS Agent affinity
- CDM attribute: Label
  Description: Managed System Name "- Windows OS"

Appendix F. Documentation library

This appendix contains information about the publications related to IBM Tivoli Monitoring and to the commonly shared components of Tivoli Management Services. These publications are listed in the following categories:

- IBM Tivoli Monitoring library
- Related publications

See *IBM Tivoli Monitoring and OMEGAMON XE Products: Documentation Guide*, SC23-8816, for information about accessing and using the publications. You can find the *Documentation Guide* in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/. To open the *Documentation Guide* in the information center, select **Using the publications** in the **Contents** pane.

To find a list of new and changed publications, click **What's new** on the Welcome page of the IBM Tivoli Monitoring and OMEGAMON XE Information Center. To find publications from the previous version of a product, click **Previous versions** under the name of the product in the **Contents** pane.

IBM Tivoli Monitoring library

The following publications provide information about IBM Tivoli Monitoring and about the commonly shared components of Tivoli Management Services:

- *Quick Start Guide*

  Introduces the components of IBM Tivoli Monitoring.
- *Installation and Setup Guide*, GC32-9407

  Provides instructions for installing and configuring IBM Tivoli Monitoring components on Windows, Linux, and UNIX systems.
- *Program Directory for IBM Tivoli Management Services on z/OS*, GI11-4105

  Gives instructions for the SMP/E installation of the Tivoli Management Services components on z/OS®.
- *Configuring the Tivoli Enterprise Monitoring Server on z/OS*, SC27-2313

  Provides instructions for preparing, configuring, and customizing your monitoring servers on z/OS. This guide complements the *IBM Tivoli OMEGAMON XE and IBM Tivoli Management Services on z/OS Common Planning and Configuration Guide* and the *IBM Tivoli Monitoring Installation and Setup Guide*.
- *Administrator's Guide*, SC32-9408

  Describes the support tasks and functions required for the Tivoli Enterprise Portal Server and clients, including Tivoli Enterprise Portal user administration.

- *High-Availability Guide for Distributed Systems*, SC23-9768

  Gives instructions for several methods of ensuring the availability of the IBM Tivoli Monitoring components.
- Tivoli Enterprise Portal online help

  Provides context-sensitive reference information about all features and customization options of the Tivoli Enterprise Portal. Also gives instructions for using and administering the Tivoli Enterprise Portal.
- *Tivoli Enterprise Portal User's Guide*, SC32-9409

  Complements the Tivoli Enterprise Portal online help. The guide provides hands-on lessons and detailed instructions for all Tivoli Enterprise Portal features.
- *Command Reference*, SC32-6045

  Provides detailed syntax and parameter information, as well as examples, for the commands you can use in IBM Tivoli Monitoring.
- *Troubleshooting Guide*, GC32-9458

  Provides information to help you troubleshoot problems with the software.
- *Messages*, SC23-7969

  Lists and explains messages generated by all IBM Tivoli Monitoring components and by z/OS-based Tivoli Management Services components (such as Tivoli Enterprise Monitoring Server on z/OS and TMS:Engine).
- *IBM Tivoli Universal Agent User's Guide*, SC32-9459

  Introduces you to the IBM Tivoli Universal Agent, an agent of IBM Tivoli Monitoring. The IBM Tivoli Universal Agent enables you to use the monitoring and automation capabilities of IBM Tivoli Monitoring to monitor any type of data you collect.
- *IBM Tivoli Universal Agent API and Command Programming Reference Guide*, SC32-9461

  Explains the procedures for implementing the IBM Tivoli Universal Agent APIs and provides descriptions, syntax, and return status codes for the API calls and command-line interface commands.
- *Agent Builder User's Guide*, SC32-1921

  Explains how to use the Agent Builder for creating monitoring agents and their installation packages, and for adding functions to existing agents.
- *Performance Analyzer User's Guide*, SC27-4004

  Explains how to use the Performance Analyzer to understand resource consumption trends, identify problems, resolve problems more quickly, and predict and avoid future problems.

Documentation for the base agents

If you purchased IBM Tivoli Monitoring as a product, you received a set of *base* monitoring agents as part of the product. If you purchased a monitoring agent product (for example, an OMEGAMON XE product) that includes the commonly shared components of Tivoli Management Services, you did not receive the base agents.

The following publications provide information about using the base agents.

- Operating system agents:
  - *Windows OS Agent User's Guide*, SC32-9445
  - *UNIX OS Agent User's Guide*, SC32-9446
  - *Linux OS Agent User's Guide*, SC32-9447
  - *i5/OS® Agent User's Guide*, SC32-9448
  - *UNIX Log Agent User's Guide*, SC32-9471
- Agentless operating system monitors:
  - *Agentless Monitoring for Windows Operating Systems User's Guide*, SC23-9765
  - *Agentless Monitoring for AIX Operating Systems User's Guide*, SC23-9761
  - *Agentless Monitoring for HP-UX Operating Systems User's Guide*, SC23-9763
  - *Agentless Monitoring for Solaris Operating Systems User's Guide*, SC23-9764
  - *Agentless Monitoring for Linux Operating Systems User's Guide*, SC23-9762
- Warehouse agents:
  - *Warehouse Summarization and Pruning Agent User's Guide*, SC23-9767
  - *Warehouse Proxy Agent User's Guide*, SC23-9766
- System P agents:
  - *AIX Premium Agent User's Guide*, SA23-2237
  - *CEC Base Agent User's Guide*, SC23-5239
  - *HMC Base Agent User's Guide*, SA23-2239
  - *VIOS Premium Agent User's Guide*, SA23-2238
- Other base agents:
  - *Systems Director base Agent User's Guide*, SC27-2872
  - *Tivoli Log File Agent User's Guide*, SC14-7484
  - *Monitoring Agent for IBM Tivoli Monitoring 5.x Endpoint User's Guide*, SC32-9490

Related publications

You can find useful information about related products in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/.

Other sources of documentation

You can also obtain technical documentation about IBM Tivoli Monitoring and related products from the following sources:

- IBM Integrated Service Management Library

  http://www-01.ibm.com/software/brandcatalog/ismlibrary/

  IBM Integrated Service Management Library is an online catalog that contains integration documentation and other downloadable product extensions.
- Redbooks

  http://www.redbooks.ibm.com/

  IBM Redbooks® and Redpapers include information about products from platform and solution perspectives.

- Technotes

  Technotes provide the latest information about known product limitations and workarounds. You can find Technotes through the IBM Software Support Web site at http://www.ibm.com/software/support.
- Tivoli wikis on the IBM developerWorks Web site

  Tivoli Wiki Central at http://www.ibm.com/developerworks/wikis/display/tivoli/Home is the home for interactive wikis that offer best practices and scenarios for using Tivoli products. The wikis contain white papers contributed by IBM employees, and content created by customers and business partners.

  Two of these wikis are of particular relevance to IBM Tivoli Monitoring:

  – Tivoli Distributed Monitoring and Application Management Wiki at http://www.ibm.com/developerworks/wikis/display/tivolimonitoring/Home provides information about IBM Tivoli Monitoring and related distributed products, including IBM Tivoli Composite Application Management products.
  – Tivoli System z Monitoring and Application Management Wiki at http://www.ibm.com/developerworks/wikis/display/tivoliomegamon/Home provides information about the OMEGAMON XE products, NetView for z/OS, Tivoli Monitoring Agent for z/TPF, and other System z monitoring and application management products.

Appendix G. Accessibility

Accessibility features help users with physical disabilities, such as restricted mobility or limited vision, to use software products successfully. The major accessibility features in this product enable users to do the following:

- Use assistive technologies, such as screen-reader software and digital speech synthesizer, to hear what is displayed on the screen. Consult the product documentation of the assistive technology for details on using those technologies with this product.
- Operate specific or equivalent features using only the keyboard.
- Magnify what is displayed on the screen.

In addition, the product documentation was modified to include the following features to aid accessibility:

- All documentation is available in both HTML and convertible PDF formats to give the maximum opportunity for users to apply screen-reader software.
- All images in the documentation are provided with alternative text so that users with vision impairments can understand the contents of the images.

Navigating the interface using the keyboard

Standard shortcut and accelerator keys are used by the product and are documented by the operating system. Refer to the documentation provided by your operating system for more information.

Magnifying what is displayed on the screen

You can enlarge information on the product windows using facilities provided by the operating systems on which the product is run. For example, in a Microsoft Windows environment, you can lower the resolution of the screen to enlarge the font sizes of the text on the screen. Refer to the documentation provided by your operating system for more information.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Cell Broadband Engine and Cell/B.E. are trademarks of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index

T

U

W

Printed in USA

SC32-9445-05