Tivoli® Monitoring: i5/OS Agent

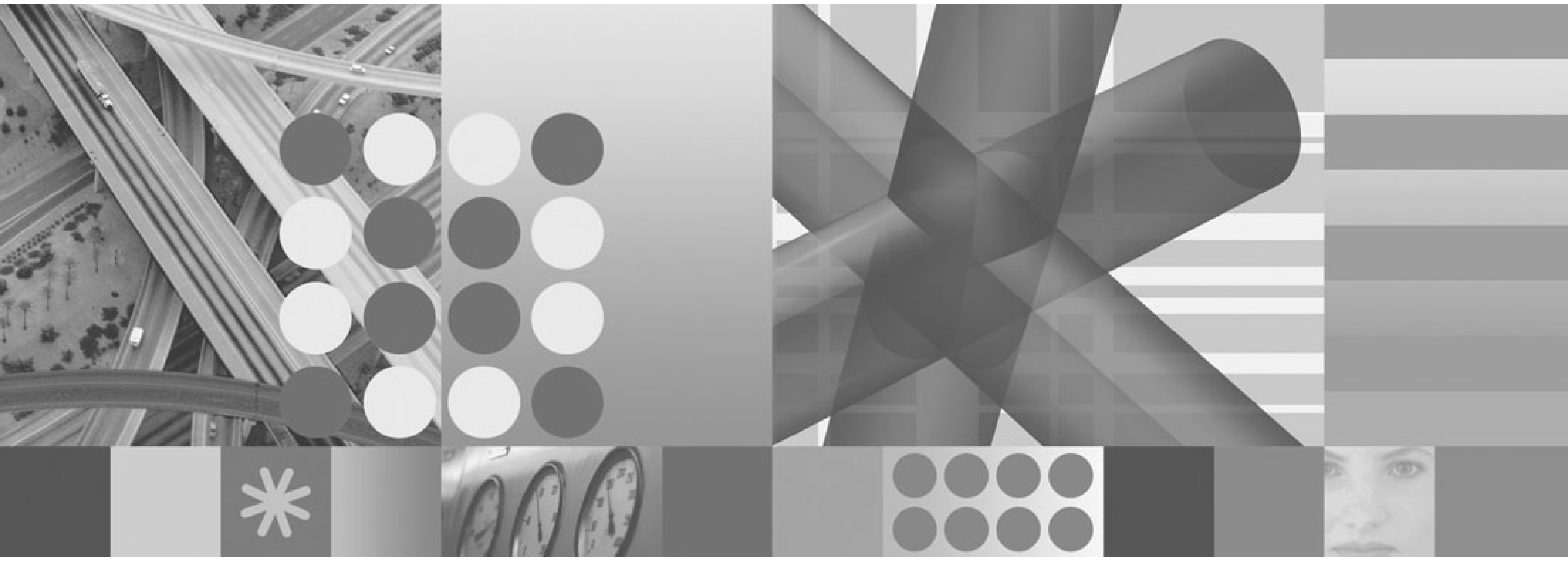
Version 6.2.0

User's Guide

SC32-9448-01

Tivoli® Monitoring: i5/OS Agent

Version 6.2.0



User's Guide

SC32-9448-01

Note

Before using this information and the product it supports, read the information in "Notices" on page 229.

This edition applies to version 6.2.0 of IBM Tivoli Monitoring: i5/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 i5/OS

The Monitoring Agent for i5/OS provides you with the capability to monitor i5/OS resources, and to perform basic actions with i5/OS. This chapter provides a description of the features, components, and interface options for the Monitoring Agent for i5/OS.

IBM Tivoli Monitoring overview

IBM Tivoli Monitoring is the base software for the Monitoring Agent for i5/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 Appendix F, “Documentation library,” on page 225 for complete information about IBM Tivoli Monitoring and the Tivoli Enterprise Portal.

Features of the Monitoring Agent for i5/OS

The Monitoring Agent for i5/OS offers a central point of management for i5/OS systems. It provides a comprehensive means for gathering exactly the information you need to detect problems early and prevent them. Information is standardized across all distributed systems so you can monitor and manage hundreds of servers from a single workstation.

Use the Monitoring Agent for i5/OS to easily collect and analyze i5/OS-specific information, such as:

- Operating system and CPU performance
- i5/OS disk information and performance analysis
- Network performance and information, such as topology and status
- Virtual and physical memory statistics
- Disk and database capacity
- Paging information and swap statistics
- Historical data collection for trend analysis and capacity planning

Table 1 lists the tasks that you can perform using the Monitoring Agent for i5/OS alone, in a network, and in combination with the Tivoli Enterprise Portal.

Table 1. Examples of Monitoring Agent for i5/OS Tasks

Task	Monitoring Agent for i5/OS	User Action	Tivoli Enterprise Portal
Detect library growth	✓		
Detect auxiliary storage pool growth	✓		
Detect security violations	✓		
Detect bad response time	✓		
Send alerts when specified system conditions are detected	✓		
Delete unused files	✓	✓	
Prioritize local jobs	✓	✓	
Limit local use to users temporarily		✓	
Control local job flow	✓	✓	
Take backup on a scheduled basis		✓	
Provide real-time graphical display of resource utilization problems			✓
Distribute situations and policies			✓
View and edit a situation graphically			✓
Specify user action to be taken			✓
Start a situation from the central site	✓		✓
Manage remote jobs	✓	✓	
Check the Monitoring Agent for i5/OS log	✓		
Automate remote configuration changes	✓	✓	
Verify remote fix levels	✓		✓
Centralize monitoring of network conditions	✓		

The Monitoring Agent for i5/OS provides the following benefits:

- Simplifies application and system management by managing applications, platforms and resources across your system.
- Increases profits by providing you with real-time access to reliable, up-to-the-minute data that allows you to make faster, better informed operating decisions.
- Enhances system performance because you can integrate, monitor, and manage your environment, networks, console, and mission-critical applications. The

Monitoring Agent for i5/OS alerts the Tivoli Enterprise Portal when conditions in your environment meet threshold-based conditions. These alerts notify your system administrator to limit and control system traffic. You can view data gathered in reports and charts, informing you of the status of managed resources.

- Enhances efficiency by monitoring diverse platforms and networks. Depending on your Tivoli Enterprise Portal configuration, you can collect and monitor data across platforms. The Monitoring Agent for i5/OS gathers and filters status information at the managed resource rather than at the Hub, eliminating unnecessary data transmission and sending only data that is relevant to changes in status conditions. The Monitoring Agent for i5/OS helps you monitor and gather consistent, accurate, and timely information that you need to effectively perform your job.

New in this release

For version 6.2 of the Monitoring Agent for i5/OS, the following enhancements have been made:

- Changes to supported operating systems as listed in Chapter 2, “Installation and Configuration of the monitoring agent,” on page 7
- Enablement of IBM® Tivoli® License Manager reporting
- New attribute groups
  - Auxiliary Storage Pool
  - Disk
  - Distribution Queue
  - History Log
  - Integrated File System Object
  - Job Log
  - Management Central Events
  - Miscellaneous
  - Network Interface
  - Network Server
  - NetServer™
  - Output Queue
  - System Statistics
  - TCPIP Logical Interface
  - TCPIP Service
- Updated ka4.baroc file to support TEC event mapping
- Updated resource model mapping files
- Migration mapping files to aid in migration from IBM Tivoli Monitoring 5.1 to IBM Tivoli Monitoring 6.2.

Note: These enhancements include ones made for the various IBM Tivoli Monitoring fix packs since the release of IBM Tivoli Monitoring 6.1.

Monitoring Agent for i5/OS components

After you install the Monitoring Agent for i5/OS (product code "ka4" or "a4") as directed in the *IBM Tivoli Monitoring Installation and Setup Guide*, you have an environment that contains the 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, Monitoring Agent for i5/OS, which collects and distributes data to a Tivoli Enterprise Monitoring Server.
- Operating system agents and application agents installed on the systems or subsystems you want to monitor. These agents collect and distribute 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 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® workstation.

i5/OS® non-programmable terminal interface
The non-programmable terminal interface for the Monitoring Agent for i5/OS provides commands, menus, and helps to start, stop, and configure the agent.

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 monitoring services and starting Tivoli services not already designated to start automatically.

Chapter 2. Installation and Configuration of the monitoring agent

This chapter contains information about the following topics and procedures relevant to the installation and configuration of the Monitoring Agent for i5/OS:

- "Requirements for the monitoring agent"
- "Preparing for installation" on page 8
- "Installing the Monitoring Agent for i5/OS" on page 10
- "Starting the monitoring agent" on page 15
- "Stopping the monitoring agent" on page 16
- "Displaying the log" on page 17
- "Deleting the Monitoring Agent for i5/OS" on page 17

Requirements for the monitoring agent

In addition to the requirements described in the *IBM Tivoli Monitoring Installation and Setup Guide*, the Monitoring Agent for i5/OS has the requirements listed in Table 2.

Table 2. System requirements

Operating system	**i5/OS**
Operating system versions	• i5/OS V5R3 • i5/OS V5R4
Disk space	• 100 MB disk space for the monitoring agent • Historical data disk space: see "Disk capacity planning for historical data" on page 143
Other requirements	• TCP/IP Communication Utilities • i5/OS Option 12, Host Servers, and Option 30, QShell must be installed • If you want IBM Tivoli License Manager support on i5/OS V5R3, then you must install a PTF. See the IBM Tivoli License Manager documentation for more information.

Note: For the most current information about the operating systems that are supported, see the following URL:

```
http://www-306.ibm.com/software/sysmgmt/products/support/Tivoli_
Supported_Platforms.html
```

When you get to that site, click **Tivoli platform and database support matrix link** at the bottom of the window.

Running as a non-Administrator user

The Monitoring Agent for i5/OS jobs run under the QAUTOMON user profile that is created during installation. The QAUTOMON profile is created as a system operator class profile (*SYSOPR) and does not have all object authority (*ALLOBJ). So the agent does not run with UNIX® 'root' or Windows 'Administrator' style authorities. The special authorities for the QAUTOMON profile and the object authorities it is given during installation are described in Appendix C, “Object access authority,” on page 195.

This user profile can be configured using the i5/OS Change User Profile (CHGUSRPRF) command.

Preparing for installation

Before installing the Monitoring Agent for i5/OS, complete the following procedures if applicable:

- During installation, you are required to know whether or not the primary language of your iSeries® system is the English language. To determine this, complete the procedure described in “Determining the primary language of your iSeries system.”
- Verify that your TCP/IP network services are configured to return the fully qualified host name of the computer where you will install the monitoring agent as described in “Verifying the TCP/IP configuration.”
- If you have a previous version of a Candle® or IBM Tivoli Monitoring v6.1 monitoring agent installed, delete it as described in “Deleting previous versions of the monitoring agent” on page 9.

Determining the primary language of your iSeries system

Objective: To determine the primary language of your iSeries system.

Background information: During the installation process, you are required to know whether the primary language of your iSeries system is the English language (language ID 2924). The installation procedure includes instructions for systems with and without the primary language set to the English language.

Required authorization role: QSECOFR

Before you begin: Not applicable.

When you finish: Complete the appropriate procedures that are described in “Preparing for installation” and then install the Monitoring Agent for i5/OS as described in “Installing the Monitoring Agent for i5/OS” on page 10.

Procedure:

1. From an i5/OS command line, enter the following command:
   ```
   GO LICPGM
   ```
2. Enter **20** (Display installed secondary languages).
3. Note the primary language and description that is displayed in the upper left corner of the window. For an English language system, the primary language is 2924, and the description is English.

Verifying the TCP/IP configuration

Objective: To ensure that your TCP/IP network services are configured to return the fully qualified host name (for example, myhost.ibm.com).

Background information: The proper TCP/IP configuration is necessary to minimize the risk of inconsistent values being returned for the host name.

Required authorization role: *IOSYSCFG

Before you begin: Not applicable.

When you finish: Complete the appropriate procedures that are described in "Preparing for installation" on page 8 and then install the Monitoring Agent for i5/OS as described in "Installing the Monitoring Agent for i5/OS" on page 10.

Procedure:

1. From an i5/OS command line, enter the following command:
   ```
   CFGTCP
   ```
2. Select **Work with TCP/IP host tables entries**.
3. Confirm that the first entry in the Host Name column is the fully qualified host name that is associated with the IP address of the i5/OS where you plan to install the monitoring agent. If it is not, change the entry to the fully qualified host name.
4. Return to the Configure TCP/IP menu and select **Change TCP/IP domain information**.
5. Confirm that a host name and domain name are provided and that they match the entry you just confirmed in the TCP/IP Host Table.
6. Confirm that the first entry for **Host name search priority** is *LOCAL.

Deleting previous versions of the monitoring agent

Objective: To delete a previous version a previous Candle or IBM Tivoli Monitoring v6.1 monitoring agent if one is installed.

Background information: You must delete the previous Candle monitoring agent if one is installed before you can install the Monitoring Agent for i5/OS.

Required authorization role: QSECOFR or a user with *ALLOBJ special authority

Before you begin: Not applicable.

When you finish: Complete the appropriate procedures that are described in "Preparing for installation" on page 8 and then install the Monitoring Agent for i5/OS as described in "Installing the Monitoring Agent for i5/OS" on page 10.

Procedure:

1. Determine if licensed program 0KA4430, 0KA4440, or 0KA4610 is installed by entering the following command:
   ```
   GO LICPGM
   ```
2. Select **10 Display installed licensed programs**. If licensed program 0KA4430, 0KA4440, or 0KA4610 is installed, continue to the next step. If licensed program 0KA4430, 0KA4440, or 0KA4610 is not installed, no further action is necessary.
3. Enter the following commands to create a save file and save the existing monitoring agent:
   ```
   CRTLIB CCCINST
   CRTSAVF CCCINST/PRE610KA4
   SAVLICPGM LICPGM(0KA4version_number) DEV(*SAVF)
      SAVF (CCCINST/PRE610KA4)
   ```
   where *version_number* is either 430, 440, or 610. You only need to enter the CRTLIB command if the library CCCINST does not exist.
4. Enter the following command to delete the licensed program:

```
DLTLICPGM 0KA4version_number
```

where *version_number* is either 430, 440, or 610.

Installing the Monitoring Agent for i5/OS

Objective

To install the Monitoring Agent for i5/OS.

Background information

This procedure uses the Restore Licensed Program to complete installation of the Monitoring Agent for i5/OS.

You can install the Monitoring Agent for i5/OS from a PC or from an iSeries computer, whichever method is more convenient at your site. This procedure includes instructions for both methods.

Required authorization role

Sign on as QSECOFR or with a profile with an equivalent special authority (SPCAUT):

- *ALLOBJ
- *AUDIT
- *IOSYSCFG
- *JOBCTL
- *SAVSYS
- *SECADM
- *SERVICE
- *SPLCTL

Before you begin

Before beginning this procedure, install IBM Tivoli Monitoring and the Tivoli Enterprise Portal as described in the *IBM Tivoli Monitoring Installation and Setup Guide* and complete the procedures in “Preparing for installation” on page 8 if necessary.

When you finish

Configure the Monitoring Agent for i5/OS as described in “Configuring the Monitoring Agent for i5/OS” on page 12.

Procedure

1. From an i5/OS command line, ensure that the QALWOBJRST system value is set to *ALL. To do this, follow these steps:
   a. Enter the following command:
      ```
      WRKSYSVAL QALWOBJRST
      ```
   b. Select **5** (Display) and verify that the value is set to *ALL.
   c. Press **Enter** to continue.
   d. If the value of QALWOBJRST is set to *ALL, go to step 3 on page 11. If the value of QALWOBJRST is not set to *ALL, make note of the values and go to step 2.
2. If the value of QALWOBJRST is *not* set to *ALL, follow these steps:
   a. On the Work with System Values window, enter **2** to change the values.
   b. On the Change System Value window, change the existing values to *ALL and press **Enter**.

c. Press **F3**.

3. From an i5/OS command line, enter the following command to create an i5/OS CCCINST library for the Monitoring Agent for i5/OS installation if this library does not already exist:

   ```
   CRTLIB LIB(CCCINST)
   ```

4. Enter the following command to create a save file in the CCCINST library for the Monitoring Agent for i5/OS:

   ```
   CRTSAVF CCCINST/A4520CMA TEXT('ITM 62 i5/OS')
   ```

   Note: When pasting this command to an i5/OS session, the single quote (′) characters that enclose the text string might be missing. If this happens, manually add the single quote (′) characters for the command to work.

5. Transfer the software for the Monitoring Agent for i5/OS to the target i5/OS. Do one of the following:

   - **From a PC, follow these steps:**

     a. Insert the IBM Tivoli Monitoring, V 6.2 product CD into the PC CD-ROM drive.

     b. From a DOS command prompt, enter the following command to start an FTP session:

        ```
        ftp computer_name
        ```

        where *computer_name* is the name of the target i5/OS.

     c. Enter the following command to change to the file type to binary:

        ```
        binary
        ```

     d. Enter the following command to transfer the software for the monitoring agent:

        ```
        put cdrom_drive_letter:\OS400\TMAITM6\A4520CMA.SAV
        CCCINST/A4520CMA (replace
        ```

     e. Enter the following command to end the FTP session:

        ```
        bye
        ```

   - **From an i5/OS system, follow these steps:**

     a. Insert the IBM Tivoli Monitoring, V6.2 product CD into the CD-ROM drive.

     b. Enter the following command to create a work folder:

        ```
        WRKFLR
        ```

     c. Select **1** (Create Folder) and specify the following name for the folder:

        ```
        A4FLR
        ```

     d. Enter the following command:

        ```
        WRKLNK QOPT
        ```

        The Work with Object Links window displays the qopt object link.

     e. Select **5** (Next Level) at the qopt object link to select the next object link, the volume ID of the CD-ROM. Make note of this volume ID for use in the remainder of this procedure.

     f. Continue to select **5** for each link level until the /QOPT/*volume_id*/OS400/TMAITM6 path is displayed, where *volume_id* is the volume ID of the CD-ROM drive from step 5e.

     g. Look for the A4520CMA.SAV file and enter the following command to copy this save file to the QDLS directory:

        ```
        CPY OBJ('/QOPT/volume_id/OS400/TMAITM6/A4520CMA.SAV')
        TODIR('/QDLS/A4FLR')
        ```

        where *volume_id* is the volume ID of the CD-ROM drive from step 5e.

h. Enter the following command to start an FTP session:

```
ftp computer_name
```

where *computer_name* is the name of the target i5/OS system.

i. Enter the following command to change to the file type to binary:

```
binary
```

j. Enter the following command:

```
NAMEFMT 1
```

k. Enter the following command to transfer the software for the monitoring agent:

```
put /QDLS/A4FLR/A4520CMA.SAV /QSYS.LIB/CCCINST.LIB/A4520CMA.SAVF
```

l. Enter **F3** and select **1** to end the FTP session.

6. From an i5/OS command line, install the software for the Monitoring Agent for i5/OS. Do one of the following:
   - If you are installing the monitoring agent on a system that is set to the English language (language ID 2924), enter the following command:

     ```
     RSTLICPGM LICPGM(5724C04) DEV(*SAVF) SAVF(CCCINST/A4520CMA)
     ```

   - If you are installing the monitoring agent on a system that is not set to language ID 2924, enter the following two commands:

     ```
     RSTLICPGM LICPGM(5724C04) DEV(*SAVF) RSTOBJ(*PGM)
     SAVF(CCCINST/A4520CMA)

     RSTLICPGM LICPGM(5724C04) DEV(*SAVF) RSTOBJ(*LNG) LNG(2924)
     SAVF(CCCINST/A4520CMA) LNGLIB(QKA4LNG)
     ```

7. The Software Agreement display is shown. Use the function keys described along the bottom of the screen to select the appropriate language version of the agreement to display, and to accept or decline the agreement. The agreement must be accepted before the agent installation can continue.
8. If you plan to install other monitoring agents, leave the value of QALWOBJRST set to *ALL until you are finished. If you do not plan to install other monitoring agents, change the value of QALWOBJRST to the values you recorded in 1d on page 10.
9. Optional: Enter the following command to delete the installation library, which is no longer needed:

   ```
   DLTLIB CCCINST
   ```

10. **Optional:** Delete the A4520CMA.SAV file from your folder. Follow these steps:

    a. Enter the following command:

    ```
    WRKDOC FLR(A4FLR)
    ```

    b. Enter **4** for the A4520CMA.SAV file.

    c. Press **Enter** to return to the command line.

    d. Enter the following command to delete the installation folder:

    ```
    WRKFLR
    ```

    e. Enter **4** for the A4FLR folder.

    f. Press **F3** to return to the command line.

Configuring the Monitoring Agent for i5/OS

Objective

To configure or reconfigure the network connections between the Monitoring Agent for i5/OS and the Tivoli Enterprise Monitoring Server (monitoring server).

Background information

You must use the i5/OS non-programmable terminal interface to configure, start, and stop the Monitoring Agent for i5/OS. Also use this interface to view the Monitoring Agent for i5/OS message log.

For more information about using the non-programmable interface, refer to the online help. For more information about command and menu interfaces and working with message logs, refer to the documentation provided with your i5/OS system.

If your environment includes a firewall between any IBM Tivoli Monitoring components, you must specify IP.PIPE as your communications protocol during configuration. For more information about firewall support including requirements for firewall configurations that use address translation, refer to the following sections in the *IBM Tivoli Monitoring Installation and Setup Guide*:

- ″Security considerations″ section in the ″Installation and configuration planning″ chapter
- ″Firewall support″ in the ″Advanced UNIX monitoring server configuration″ chapter

Required authorization role

*USER

You need authority to access the agent commands. By default, they all are *PUBLIC *EXCLUDE with some user group profiles given *USE authority as shown in Table 4 on page 15. Use the GRTOBJAUT command to add authorization for other users.

Before you begin

Install the monitoring agent as described in “Installing the Monitoring Agent for i5/OS” on page 10.

When you finish

Start the Monitoring Agent for i5/OS so you can begin using the monitoring agent to monitor your i5/OS resources. For information about how to start the Monitoring Agent for i5/OS, see “Starting the monitoring agent” on page 15.

Procedure

1. From an i5/OS command line, enter the following command:
   ```
   GO OMA
   ```
2. Enter **4** (Configure Tivoli Monitoring: i5/OS Agent).

   The Config i5/OS Monitoring Agent (CFGOMA) window is displayed.
3. Enter your site’s values for the configuration parameters using the guidelines in Table 3.

Table 3. Configuration parameters

Parameter	Description
TEMS TCP/IP address	The TCP/IP address or host name of the computer where the monitoring server resides, such as 127.0.0.1 or RALEIGH. If you use the IP.PIPE or IP.SPIPE parameters, enter `*NONE`. If the correct TCP/IP address or host name was previously defined, enter `*SAME` to retrieve this setting.

Table 3. Configuration parameters (continued)

Parameter	**Description**
TEMS IP.PIPE address	If the monitoring agent must connect to the monitoring server through a firewall, you must use the IP.PIPE communication protocol. Specify the IP.PIPE address or host name of the computer where the monitoring server resides. If you are not using the IP.PIPE communication protocol, enter `*NONE`.
TEMS IP.SPIPE Address	You can change the local Secure Socket Layer (SSL) IP.SPIPE location in an enterprise network that is using SSL IP.SPIPE communications. Configuration on the agent and the Tivoli Enterprise™ Management Server must be completed for SSL communications to function.
Secondary TEMS IP address	The TCP/IP address or host name of the computer where the secondary monitoring server resides. The monitoring agent communicates with the secondary monitoring server if it cannot communicate with the primary monitoring server at startup.
Secondary TEMS IP.PIPE address	The IP.PIPE address or host name of the computer where the secondary monitoring server resides. The monitoring agent communicates with the secondary monitoring server if it cannot communicate with the primary monitoring server at startup.
Partition name	(Required only by sites with firewalls that use address translation.) The name of the partition (up to 32 alphanumeric characters) in which the monitoring agent resides.
Firewall in use	If the monitoring agent must connect to the monitoring server through a firewall, enter `*YES`. If the monitoring agent does not connect through a firewall, keep the default value, `*NO`.
TEMS TCP/IP port address	The listening port for the monitoring server. The default number is 1918. If the correct port was previously defined, enter `*SAME` to retrieve this setting.
TEMS IP.PIPE port address	The listening port for the monitoring server. The default is 1918.
TEMS IP.SPIPE Port Number	The Secure Shell port number.
TCP/IP Server	Specifies whether or not the Tivoli Monitoring: i5/OS Agent is defined as a TCP/IP server. If it is a TCP/IP server then it can be started and stopped using the STRTCPSVR and ENDTCPSVR commands. The agent will also be automatically ended when TCP/IP is ended. If the agent is not defined as a TCP/IP server then you must start it after TCP/IP is started and end it before TCP/IP is ended.
Action user profile	The user authority under which user action must be administered. Keep the default value, QAUTOMON, to grant user system operator authority.

4. **Optional:** Customize the data collection intervals by changing the values of the following configuration variables in the QAUTOTMP/KMSPARM[KBBENV] file, which are listed with their default values:
   - KA4_JOB_DATA_INTERVAL=15
   - KA4_IOP_DATA_INTERVAL=30
   - KA4_DISK_DATA_INTERVAL=30
   - KA4_POOL_DATA_INTERVAL=15
   - KA4_COMM_DATA_INTERVAL=60

Valid values for these configuration variables are 15, 30, 60, 120, and 240. These configuration variables follow the rules of the collection interval parameter of the i5/OS QPMWKCOL API. Keep the following items in mind:

- Disk and IOP-related data require a minimum of 30 seconds between collection intervals.
- Communication-related data requires a minimum of 60 seconds between collection intervals.
- Collect job-related data as infrequently as possible to minimize the impact on system performance.
- The i5/OS collection services performance data collector supports data collection at one-minute intervals, not at two or four-minute intervals. Therefore, when using the API and requesting data at two or four-minute intervals, the data is collected at one-minute intervals but reported back every two or four minutes.

Starting the monitoring agent

Objective

To start the Monitoring Agent for i5/OS.

Background information

When the Monitoring Agent for i5/OS is started, you can use the associated CLI commands. The table shows the group profiles that are authorized to these commands by default when the Monitoring Agent for i5/OS is first installed. A check mark in a column indicates that users associated with that group profile can use the command.

To determine which group profile a user is associated with, use the Display User Profile (DSPUSRPRF) command. The group profile to which the user is associated is listed in the group profile field.

*Table 4. Commands owned by QSYS with *PUBLIC *EXCLUDE*

Command	QSRV	QSRVBAS	QSYSOPR	QPGMR
CFGOMA	✓			
DSPOMALOG	✓	✓	✓	✓
ENDOMA	✓		✓	
STROMA	✓		✓	

Required authorization role

*USER or, in some cases, *JOBCTL special authority if authorities for QAUTOMON were changed after installation

You need authority to access the agent commands. By default, they all are *PUBLIC *EXCLUDE with some user group profiles given *USE authority as shown in Table 4. Use the GRTOBJAUT command to add authorization for other users.

Before you begin

Configure the monitoring agent as described in “Configuring the Monitoring Agent for i5/OS” on page 12.

When you finish

To determine if the monitoring agent is started, check the log file as described in "Displaying the log" on page 17. If the monitoring agent started successfully, the following message is written in the log file:

```
Tivoli Enterprise Monitoring Server located
```

Procedure

1. From an i5/OS, enter the following command:
   ```
   GO OMA
   ```
2. Enter **2** (Start Tivoli Monitoring: i5/OS Agent).

   The greater than character (>) preceding option 2 indicates that the monitoring agent is not started. When the monitoring agent is started the greater than character (>) is not displayed.

Stopping the monitoring agent

Objective

To stop the Monitoring Agent for i5/OS.

Background information

Not applicable.

Required authorization role

*USER

You need authority to access the agent commands. By default, they all are *PUBLIC *EXCLUDE with some user group profiles given *USE authority as shown in Table 4 on page 15. Use the GRTOBJAUT command to add authorization for other users.

Before you begin

Not applicable.

When you finish

Not applicable.

Procedure

1. From an i5/OS, enter the following command:
   ```
   GO OMA
   ```
2. Enter **3** (End Tivoli Monitoring: i5/OS Agent).
3. Specify one of the following options:

   ***IMMED**

   Stops the monitoring agent immediately.

   ***CNTRLD**

   Performs a controlled shutdown. With a controlled shutdown, you can also specify the following options:

   Delay time

   Shutdown is delayed for the time interval (in seconds) that you specify, enabling the monitoring agent to complete operations.

   Allow abnormal end if needed (YES, NO)

   If you enter YES, any jobs that have not ended after 10 minutes are shut down.

Displaying the log

Objective

To display the log for the Monitoring Agent for i5/OS.

Background information

Messages related to the Monitoring Agent for i5/OS while it is running are written in the KMSOMLOG message queue in the QAUTOMON library.

Required authorization role

*USER

You need authority to access the agent commands. By default, they all are *PUBLIC *EXCLUDE with some user group profiles given *USE authority as shown in Table 4 on page 15. Use the GRTOBJAUT command to add authorization for other users.

Before you begin

Not applicable.

When you finish

Not applicable.

Procedure

1. From an i5/OS, enter the following command:

   ```
   GO OMA
   ```
2. Enter **1** (Display Tivoli Monitoring: i5/OS Agent Log).

Deleting the Monitoring Agent for i5/OS

Objective

To delete the Monitoring Agent for i5/OS.

Background information

Not applicable.

Required authorization role

QSECOFR or a user with *ALLOBJ special authority

Before you begin

Ensure that no other users are displaying the 'Tivoli Monitoring: i5/OS Agent' menu, displayed using GO OMA, or displaying any of the associated CLI commands: CFGOMA, DSPOMALOG, ENDOMA, STROMA.

When you finish

Not applicable.

Procedure

1. Stop the Monitoring Agent for i5/OS.
2. From an i5/OS, enter the following command:

   ```
   GO OMA
   ```
3. Enter **3** (End Tivoli Monitoring: i5/OS Agent).
4. Wait until the OMA menu is redisplayed and the agent has stopped.
5. Press **F3** to exit the OMA menu.

6. From an i5/OS command line, enter the following command:

```
DLTLICPGM LICPGM(5724C04)
```

Support for SSL communication with the Monitoring Agent for i5/OS

The Monitoring Agent for i5/OS supports communication with the monitoring server using the SSL communication protocol (Secure Socket Layer).

In IBM Tivoli Monitoring, SSL communication is managed through the use of digital certificates. You have two options for managing certifications:

- iKeyman, a Java-based utility available as part of IBM iSeries Client Encryption licensed program. Key ring files to hold certificates can be created using the iKeyman GUI. Both Server and Client certificates can be created and stored in key ring files.
- Digital Certificate Manager (DCM), a free iSeries feature, to centrally manage certificates for applications. DCM enables managing certificates that are obtained from any Certificate Authority (CA). Also, you can use DCM to create and operate your own local CA to issue private certificates to applications and users in your organization.

Current SSL configuration does not use the key ring files on the Monitoring Agent for i5/OS, unlike other OS monitoring agents. Instead, DCM is used to create a local certificate store, if it does not already exist on the system where i5/OS is installed. Local certificates are created in the certificate store. Certificates obtained from a 3rd party Certificate authority also can be imported to the local certificate store. Steps provided below are for configuring the SSL for the Monitoring Agent for i5/OS using the Application Identifier to associate certificates to the Monitoring Agent for i5/OS application and SSL services provided by iSeries.

The following procedure provides the high-level summary of the steps to configure this support:

1. Install the Monitoring Agent for i5/OS on System i™.
2. Open the Configure Tivoli Monitoring: i5/OS screen by running the **GO OMA** command and selecting Option 4.
3. Set the monitoring server DNS or IP address using the **TEMS IP.SPIPE Address** parameter.
4. Set the port number using the **TEMS IP.SPIPE Port Number** parameter. 3660 is the default port.
5. Configure the Certificate and Application ID using the steps in "Configuring DCM" on page 19.
6. Occasionally, agents might have connection problems on some V5R3 systems. In that case, set the KDEBE_PROTOCOL to SSL_VERSION_3 in QAUTOTMP/KMSPARM(KBBENV) file on System i. This is not necessary if i5/OS PTFs MF40084 and PTF MF39703 are installed.
7. Configure the monitoring server to communicate with the IP.SPIPE protocol on the port set in step 4. You can set this communication protocol in the Monitoring Tivoli Enterprise Monitoring Services utility.
8. Start the monitoring server and the Monitoring Agent for i5/OS.

If there are connection problems, first configure the agent to communicate using the IP.PIPE protocol. If that is successful, then try with the SPIPE protocol.

If the agent does not connect, to troubleshoot the problem, set the agent trace as follows:

1. Add the line KDE_DEBUG=A somewhere in QAUTOTMP/ KMSPARM(KBBENV)
2. Recycle the agent to generate more trace.
3. FTP the file QAUTOTMP/KA4AGENT01 to a PC and send to IBM Software Support.

Prerequisites

The documentation on the SSL and DCM are taken from the iSeries Information Center Web site. Refer to the iSeries documentation for more details on these topics. iSeries documentation can be obtained using the following link: http://publib.boulder.ibm.com/iseries/. After selecting the appropriate i5/OS release, you can search for DCM or SSL to find related information.

The following are prerequisites for the SSL support on i5/OS:

- IBM Digital Certificate Manager (DCM), option 34 of OS/400® (5722-SS1)
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- If you are trying to use the HTTP server to use the DCM, be sure you have the IBM Developer Kit for Java(TM) (5722-JV1) installed, or the HTTP admin server will not start.
- The IBM Cryptographic Access Provider product, 5722-AC3 (128-bit). The bit size for this product indicates the maximum size of the secret material within the symmetric keys that can be used in cryptographic operations. The size allowed for a symmetric key is controlled by the export and import laws of each country. A higher bit size results in a more secure connection.

Optional: You might also want to install cryptographic hardware to use with SSL to speed up the SSL handshake processing. As of release V5R2M0, the following cryptographic hardware options are available to you, for use with your iSeries server:

- 2058 Cryptographic Accelerator (Hardware Feature code 4805)
- 4758 Cryptographic Coprocessor (Hardware Feature codes 4801 or 4802)

If you want to install cryptographic hardware, you must also install Option 35, the Cryptographic Service Provider.

Configuring DCM

The following sections provide the steps to configure DCM.

Starting DCM

Before you can use any of its functions, you need to start Digital Certificate Manager (DCM). Complete these tasks to ensure that you can start DCM successfully:

- Install 5722 SS1 Option 34. This is Digital Certificate Manager (DCM).
- Install 5722 DG1. This is the IBM HTTP Server for iSeries.
- Install 5722 AC3. This is the cryptography product that V5R2 DCM uses to generate a public-private key pair for certificates, to encrypt exported certificate files, and decrypt imported certificate files.

Use the following steps to start DCM:

1. Use the iSeries Navigator to start the HTTP Server *ADMIN instance:
   a. Start iSeries Navigator.
   b. Double-click your iSeries server in the main tree view.
   c. Double-click **Network**.
   d. Double-click **Servers**.
   e. Double-click **TCP/IP**.
   f. Right-click **HTTP Administration** and click **Start**.
2. Start your Web browser and go to the iSeries Tasks page on your system at http://*your_system_name*:2001.
3. Select **Digital Certificate Manager** from the list of products on the iSeries Tasks page to access the DCM feature.

Setting up certificates for the first time

The left frame of Digital Certificate Manager (DCM) is the task navigation frame. You can use this frame to select a wide variety of tasks for managing certificates and the applications that use them. Which tasks are available depends on which certificate store (if any) you have opened and your user profile authority. Most tasks are available only if you have *ALLOBJ and *SECADM special authorities.

When you use Digital Certificate Manager (DCM) for the first time, no certificate stores exist (unless you have migrated from a previous version of DCM). Consequently, the navigation frame displays only these tasks when you have the necessary authorities:

- Manage User Certificates.
- Create New Certificate Store.
- Create a Certificate Authority (CA). (Note: After you use this task to create a private CA, this task no longer appears in the list.)
- Manage CRL Locations.
- Manage PKIX Request Location.

Even if certificate stores already exist on your system (for example, you are migrating from an earlier version of DCM), DCM displays only a limited number of tasks or task categories in the left navigation frame. You must first access the appropriate certificate store before you can begin working with most certificate and application management tasks. To open a specific certificate store, click Select a Certificate Store in the navigation frame.

Certificates can be obtained using either public internet Certificate Authority (CA), such as VeriSign or certificates can issued from the local private Certificate Authority. The steps below primarily applicable to certificates issued using the local CA. iSeries or other documentation need to be considered for the steps to obtain certificates from public CA.

Creating a new certificate store

Perform the steps in this section if *SYSTEM certificate store does not exist already. This section should be skipped if *SYSTEM certificate store already created on the system. "Select Certificate Store" button in the task navigation frame can be used to verify if *SYSTEM certificate store already created or not. "*SYSTEM" will be listed if there is one already.

1. Click **Create New Certificate Store** in the task navigation frame.
2. Select ***SYSTEM** and click **Continue**.

3. Select **No – Do not create a certificate in the certificate store** and click **Continue**.
4. Provide the password and click **Continue**.
5. Click **OK** to complete the step.

Selecting the *SYSTEM certificate store

This step is prerequisite for performing the steps in the sections below.

1. Click **Select a Certificate Store** in the task navigation frame.
2. Choose ***SYSTEM** and click **Continue**.
3. Provide the password and click **Continue**.

A screen will be displayed indicating *SYSTEM as the current certificate store and also showing the **Certificate store path and filename**: `/QIBM/USERDATA/ICSS/CERT/SERVER/DEFAULT.KDB` (if the default certificate store path is chosen).

Authorizing QAUTOMON to use certificate store files

The Monitoring Agent for i5/OS needs to be installed on the System i (iSeries) before completing this step. These steps require that the QAUTOMON user profile is available on the system for authorizing QAUTOMON to the certificate store files.

Authority on '/qibm/userdata/icss/Cert/Server ' directory: On System i 5120 session, run the following command:

```
wrklnk '/qibm/userdata/icss/Cert/Server'
```

If the certificate store files were created in a path other than the default, provide the correct path instead of the default used above.

Type 9 in the **Opt** field next to the directory **Server**. Option 9 is not displayed by default. Use `F23=More options` to display `9=Work with authority`.

In the next screen, type 1 in **Opt** field, `QAUTOMON` in **User** and `*RX` in the **Data Authority** fields. The screen will look like the following. Press Enter.

```
Data     --Object Authorities--
     Opt    User            Authority  Exist  Mgt  Alter  Ref
      1     QAUTOMON        *RX
            *PUBLIC         *EXCLUDE
            QSYS            *RWX         X     X     X     X
```

Perform the above steps for all the directories in the /qibm/userdata/icss/Cert path if *PUBLIC or QAUTOMON does not have *RX authority.

Authority on DEFAULT.KDB & DEFAULT.RDB files: On System i 5120 session, run the following command:

```
wrklnk '/qibm/userdata/icss/Cert/Server'
```

If the certificate store files were created in a path other than the default, provide the correct path instead of the default used above.

Two files DEFAULT.KDB, DEFAULT.RDB are listed. Perform the following steps for both files.

Type 9 in the **Opt** field next to the directory **Server**. Option 9 is not displayed by default. Use `F23=More options` to display `9=Work with authority`.

In the next screen, type 1 in **Opt** field, `QAUTOMON` in **User** and `*RW` in the **Data Authority** fields. The screen will look like the following. Press Enter.

```
Data     --Object Authorities--
      Opt     User             Authority  Exist  Mgt  Alter  Ref
        1     QAUTOMON         *RW
              *PUBLIC          *EXCLUDE
              QSYS             *RW          X     X     X     X
```

This step provides sufficient authority for QAUTOMON to access certificate store files.

Creating the local Certificate Authority

The steps below can be followed if Local Certificate Authority does not exist already. Use the Select Certificate Store task to verify if a local Certificate Authority exists. If one exists, **Local Certificate Authority (CA)** is listed.

1. Click **Create a Certificate Authority** in the task navigation frame.
2. Complete the following fields for the certificate and click **OK**.

Field	Value
Key size	1024
Certificate store password	Type the password for your certificate store. This field is required.
Confirm password	Type the password again.
Certificate Authority (CA) name	LOCAL_CERTIFICATE_AUTHORITY (1). This field is required.
Organization unit	
Organization name	Specify the company name. This field is required.
Locality or city	
State or province	Specify the state. This field is required.
Country or region	Specify the country. This field is required.
Validity period of Certificate Authority (CA) (2-7300)	1095 days

3. The next screen provides the option to install the certificate on your browser. This is an optional step and is not required for i5/OS. To install the certificate on your browser, click **Install Certificate**. Choose to **Open** or **Save** the certificate in local directory. If you choose to save the certificate, click on it after saving to open the certificate. Several screens are displayed to install the certificate.
4. Click **Continue** on the Install Local Certificate screen.
5. Click **Yes** for **Allow creation of user certificates** on the Certificate Authority (CA) Policy Data screen.
6. Click **Continue**.
7. Click **Continue** or **OK** on the next screen to complete the creation of local Certificate Authority.

Creating certificates using the local Certificate Authority

DCM provides a guided task path that can be used for creating a CA and using it to issue certificates to your applications. After clicking the button, a screen will be displayed with the list of Certificate Stores. Make sure *SYSTEM is the current certificate store. Use “Select a Certificate Store” button to select *SYSTEM certificate store.

1. Click **Create Certificate**.

2. Select **Server or Client Certificate**.
3. 3. Select **Local Certificate Authority**.
4. Enter the details for the certificate as listed below:

Certificate type	Server or client
Certificate store	*SYSTEM

5. Complete the form to create the certificate. Use the following values:

Field	**Value**
Key size	1024
Certificate label	IBM_Tivoli_Monitoring_Agent_Certificate
Common name	IBM Tivoli Monitoring Agent Self Signed Certificate
Organization unit	Type the organization name. This field is required.
Locality or city	
State or province	Type the state or province. This field is required.
Country or region	Type the country. This field is required.
IP version 4 address	
Fully qualified domain name (host_name.domain_name)	
E-mail address (user_name@domain_name)	

6. Click **Continue** and **OK** on the next screens. No need to choose any applications at this time.

This will complete the steps to create a Server or Client Certificate. You can view the details of the certification using the **View Certificate** task.

Creating an application ID

To create an application definition, follow these steps:

1. In DCM, click **Select a Certificate Store** and select the appropriate certificate store. (This should be *SYSTEM certificate store for creating SSL application definition for either a server application or client application.)
2. When the Certificate Store and Password page displays, provide the password that you specified for the certificate store when you created it and click **Continue**.
3. In the navigation frame, select **Manage Applications** to display a list of tasks.
4. Select **Add application** from the task list to display a form for defining the application.

   Note: If you are working in the *SYSTEM certificate store, DCM will prompt you to choose whether to add a server application definition or a client application definition. Choose to create Client application definition for this purpose.
5. Complete the form and click **Add**. The information that you can specify for the application definition varies based on the type of application that you are defining.

Below are the current properties for the default Application ID created for IBM Tivoli Monitoring for the Monitoring Agent for i5/OS.

Field	Default value
Application type	Client
Application ID	QIBM_ITM_KA4_AGENT
Exit program	CT_AGENT
Exit program library	QAUTOMON
Threadsafe	Yes
Multithread job action	Run program and send message
Application user profile	QAUTOMON
Define the CA trust list	Yes
Certificate revocation processing	No
Application description	IBM Tivoli Monitoring v6.2: i5/OS Agent

Associating the certificate with the application ID

Use the following steps to associate the certificate with the application ID:

1. Click **Assign Certificate** under Manage Certificates in the task navigation frame.
2. Select the certificate from the list.
3. Click **Assign to Applications**.
4. Select the application definition you want to associate with the certificate and click **Continue**.

Defining the CA Trust list

Use the following steps to define the CA Trust list:

1. Click **Define CA Trust list** under **Manage Applications**.
2. Select **Client - Add or remove a Certificate Authority (CA) certificate from a client application CA trust list**.
3. Select **ITM 6.2 Monitoring Agent for i5/OS Agent** and click **Define CA Trust List**.
4. Click **Trust All** and click **OK**.

Configuring the Monitoring Agent for i5/OS

Four new environment variables have been introduced for SSL configuration on the agent.

- KDEBE_APPLICATIONID
- KDC_PORTSSL
- IP_SPIPE
- KDEBE_PROTOCOL

You can set the KDEBE_OS400_APP_ID and KDEBE_PROTOCOL variables by editing the QAUTOTMP/KMSPARM(KBBENV) file. You can set the IP_PIPE and KDC_PORTSSL variables using the configuration screen provided using **GO OMA**, Option 4.

KDEBE_APPLICATIONID

Required for identifying the Application Identifier used to establish the SSL communication handshake between the Monitoring Agent for i5/OS and the monitoring server. The value for this variable depends on the Application Identifier name that is created using DCM. The default value is QIBM_ITM_KA4_AGENT for the Monitoring Agent for i5/OS. If the default Application Identifier is not used, you must update the KDEBE_APPLICATIONID value in the KBBENV configuration file with the correct Application ID.

IP_SPIPE

Used to store the monitoring server's SPIPE Address. This can be either the DNS name or IP address. This value can be set using the configuration screen available from the main menu (**GO OMA** Option 4). You do not need to edit the KBBENV environment variable file for this variable.

KDC_PORTSSL

Used to store the monitoring server's SPIPE port number. This value can be set using the configuration screen available from the main menu (**GO OMA** Option 4). You do not need to edit the KBBENV environment variable file for this variable.

KDEBE_PROTOCOL

Used to set the SSL Version protocol that the agent computer uses to connect to the monitoring server computer. If a monitoring agent on a V5R3 computer fails to connect to the monitoring server, set the **KDEBE_PROTOCOL=SSL_VERSION_3** variable to circumvent connection problems using SPIPE configuration.

KDEBE_PROTOCOL has the following characteristics:

- KDEBE_PROTOCOL=SSL_VERSION_3 (SSL 3 only). This causes an override of the available cipher suites to preclude the use of AES and to circumvent the i5/OS defects of AES not tolerated in cipher suite. This circumvents the connection problems on V5R3 systems.

  System i PTFs for SSL Layer (PTF MF40084, PTF MF39703), available in August of 2006, will fix these defects. These PTFs are installed on the V5R3 system, KDEBE_PROTOCOL can be set to SSL_VERSION_CURRENT to take advantage of all the ciphers supported.
- KDEBE_PROTOCOL=SSL_VERSION_CURRENT (TLS with SSL 3 and 2 compatibility)
- KDEBE_PROTOCOL=SSL_VERSION_2 (SSL 2, not recommended, weak)
  KDEBE_PROTOCOL=TLSV1_SSLV3 (TLS with SSL 3 compatibility)

Setting the Coded Character Set Identifier (CCSID)

When the Coded Character Set on the agent system is not the same as that on the Tivoli Enterprise Portal Server the text displayed for messages and other attribute fields might not be displayed correctly. To correct this situation you can change the CCSID defined for the QAUTOMON user profile on the Monitoring Agent for i5/OS. Use the Change User Profile (CHGUSRPRF) command on the Monitoring Agent for i5/OS system to set the CCSID to be compatible with the server. For example, the following command changes the CCSID to 5035 for Japanese, combined SBCS/DBCS:

```
CHGUSRPRF USRPRF(QAUTOMON) CCSID(5035)
```

To ensure that this change is maintained with new installations of the agent, you can add a property to the QAUTOTMP/KMSPARM.KBBENV agent properties file. Add property KA4_QAUTOMON_CCSID followed by an equal sign and the desired CCSID number. For example, adding the following line to the properties file sets the CCSID for the QAUTOMON profile to 5035:

```
KA4_QAUTOMON_CCSID=5035
```

You must stop and restart the agent after using the CHGUSRPRF command or adding the KA4_QAUTOMON_CCSID line to the properties file for the change to take affect.

Chapter 3. How to use a monitoring agent

After you have installed and configured a Tivoli Enterprise Monitoring Agent and the agent is running, you can begin using this agent to monitor your resources. The following sources of information are relevant to installation and configuration:

- *IBM Tivoli Monitoring Installation and Setup Guide*
- *IBM Tivoli Monitoring Command Reference*
- Chapter 2, “Installation and Configuration of the monitoring agent” in the user’s guide for the agent that you are installing and configuring

This chapter provides information about how to use a monitoring agent to perform the following tasks:

- “View real-time data that the agent collects”
- “Investigate an event” on page 28
- “Recover the operation of a resource” on page 28
- “Customize your monitoring environment” on page 29
- “Monitor with custom situations that meet your requirements” on page 30
- “Collect and view historical data” on page 31

For each of these tasks, there is a list of procedures that you perform to complete the task. For the tasks, there is a cross-reference to where you can find information about performing that procedure. Information about the procedures is located in subsequent chapters of this user’s guide and in the following publications:

- *IBM Tivoli Monitoring User’s Guide*
- *IBM Tivoli Monitoring Administrator’s Guide*

View real-time data that the agent collects

After you install, configure, and start the Tivoli Enterprise Monitoring Agent, the agent begins monitoring.

Table 5 contains a list of the procedures for viewing the real-time data that the monitoring agent collects through the predefined situations. The table also contains a cross-reference to where you can find information about each procedure.

Table 5. View real-time data

Procedure	**Where to find information**
View the hierarchy of your monitored resources from a system point of view (Navigator view organized by operating system type, monitoring agents, and workspaces).	*IBM Tivoli Monitoring User’s Guide:* ″Navigating through workspaces″ (in ″Monitoring: real-time and event-based″ chapter)
View the indicators of real or potential problems with the monitored resources (Navigator view).	

Table 5. View real-time data (continued)

Procedure	Where to find information
View changes in the status of the resources that are being monitored (Enterprise Message Log view).	*IBM Tivoli Monitoring User’s Guide:* ″Using workspaces″ (in ″Monitoring: real-time and event-based″ chapter) Chapter 4, “Workspaces reference,” on page 33 in this guide
View the number of times an event has been opened for a situation during the past 24 hours (Open Situations Account view).	*IBM Tivoli Monitoring User’s Guide:* ″Using workspaces″ (in ″Monitoring: real-time and event-based″ chapter) Chapter 4, “Workspaces reference,” on page 33 in this guide Chapter 6, “Situations reference,” on page 147 in this guide
Manipulate the views in a workspace.	*IBM Tivoli Monitoring User’s Guide:* ″Using views″ (in ″Monitoring: real-time and event-based″ chapter)

Investigate an event

When the conditions of a situation have been met, an event indicator is displayed in the Navigator. When an event occurs, you want to obtain information about that event so you can correct the conditions and keep your enterprise running smoothly.

Table 6 contains a list of the procedures for investigating an event and a cross-reference to where you can find information about each procedure.

Table 6. Investigating an event

Procedure	Where to find information
Determine which situation raised the event and identify the attributes that have values that are contributing to the alert.	*IBM Tivoli Monitoring User’s Guide:* ″Opening the situation event workspace″ (in ″Monitoring: real-time and event-based″ chapter, ″Responding to alerts″ section) Chapter 4, “Workspaces reference,” on page 33 in this guide
Review available advice.	
Notify other users that you have taken ownership of the problem related to an event and are working on it.	*IBM Tivoli Monitoring User’s Guide:* ″Acknowledging a situation event″ (in ″Monitoring: real-time and event-based″ chapter, ″Responding to alerts″ section)
Remove the event from the Navigator.	*IBM Tivoli Monitoring User’s Guide:* ″Closing the situation event workspace″ (in ″Monitoring: real-time and event-based″ chapter, ″Responding to alerts″ section)

Recover the operation of a resource

When you find out that a resource is not operating as desired, you can control it manually or automatically using Take Action commands.

Table 7 contains a list of the procedures for recovering the operation of a resource and a cross-reference to where you can find information about each procedure.

Table 7. Recover the operation of a resource

Procedure	**Where to find information**
Take an action on a resource manually.	*IBM Tivoli Monitoring User's Guide:* • ″Other views″ (in ″Custom workspaces″ chapter, ″Workspace views″ section) • ″Take action: Reflex automation″ (in Situations for event-based monitoring″ chapter, ″Event-based monitoring overview″ section) • "Take action" (in "Designing customized responses" chapter) Chapter 7, “Take Action commands reference,” on page 155 in this guide
Take an action on a system condition automatically by setting up a situation to run a Take Action command.	*IBM Tivoli Monitoring User's Guide:* ″Situations for event-based monitoring″ chapter • ″Customize a situation″ • ″Create a situation″ • ″Specify an action to take″ • ″Distribute the situation″ Chapter 7, “Take Action commands reference,” on page 155 in this guide
Take multiple actions on system conditions automatically using a policy.	*IBM Tivoli Monitoring User's Guide:* ″Policies for automation″ chapter • ″Creating a policy″ • ″Maintaining policies″ • ″Workflows window″ Chapter 8, “Policies reference,” on page 157 in this guide
Take actions across systems, agents, or computers using a policy.	

Customize your monitoring environment

You can change how your monitoring environment looks by creating new workspaces with one or more views in it.

Table 8 contains a list of the procedures for customizing your monitoring environment and a cross-reference to where you can find information about each procedure.

Table 8. Customizing your monitoring environment

Procedure	**Where to find information**
Display data in tables or charts (views) in the Tivoli Enterprise Portal.	*IBM Tivoli Monitoring User's Guide:* • ″Custom workspaces″ • ″Table and chart views″

Table 8. Customizing your monitoring environment (continued)

Procedure	Where to find information
Display an overview of changes in the status of situations for your monitored resources (Message Log View).	*IBM Tivoli Monitoring User's Guide:* ″Message log view″ (in ″Situation event views: message log, situation event console and graphic″ chapter)
Specify which attributes to retrieve for a table or chart so you can retrieve only the data you want by creating custom queries.	*IBM Tivoli Monitoring User's Guide:* ″Creating custom queries″ (in ″Table and chart views″ chapter) Chapter 5, "Attributes reference," on page 41 in this guide
Build links from one workspace to another.	*IBM Tivoli Monitoring User's Guide:* • ″Link from a workspace″ (in ″Custom workspaces″ chapter) • ″Link from a table or chart″ (in ″Table and chart views″ chapter)
Identify which predefined situations started running automatically when you started the Tivoli Enterprise Monitoring Server.	*IBM Tivoli Monitoring User's Guide:* ″What the enterprise workspace shows″ (in ″Monitoring: real-time and event-based″ chapter, ″Using workspaces″ section) Chapter 6, "Situations reference," on page 147 in this guide
Determine whether to run situations as defined, modify the values in situations, or create new situations to detect possible problems.	Chapter 6, "Situations reference," on page 147 in this guide

Monitor with custom situations that meet your requirements

When your environment requires situations with values that are different from those in the existing situations, or when you need to monitor conditions not defined by the existing situations, you can create custom situations to detect problems with resources by creating an entirely new situation.

You can specify the following information for a situation:

- Name
- Attribute group and attributes
- Qualification to evaluate multiple rows when a situation has a multiple-row attribute group (display item)
- Formula
- Take Action commands
- Run at startup
- Sampling interval
- Persistence
- Manual or automatic start
- Severity
- Clearing conditions
- Expert Advice
- When a true situation closes

- Available Managed Systems
- Whether to send a Tivoli Enterprise Console event
- Event severity

Table 9 contains a list of the procedures for monitoring your resources with custom situations that meet your requirements and a cross-reference to where you can find information about each procedure.

Table 9. Monitor with custom situations

Procedure	Where to find information
Create an entirely new situation.	*IBM Tivoli Monitoring User's Guide:* ″Creating a new situation″ (in ″Situations for event-based monitoring″ chapter, ″Creating a situation″ section) Chapter 5, "Attributes reference," on page 41 in this guide
Run a situation on a managed system.	*IBM Tivoli Monitoring User's Guide:* ″Situations for event-based monitoring″ chapter • ″Associating situations with navigator items″ • ″Distribute the situation″ (in ″Customizing a situation″ section) • ″Starting, stopping or deleting a situation″

Collect and view historical data

When you collect historical data, you specify the following configuration requirements:

- Attribute groups for which to collect data
- Collection interval
- Summarization and pruning of attribute groups
- Roll-off interval to a data warehouse, if any
- Where to store the collected data (at the agent or the Tivoli Enterprise Management Server)

Table 10 on page 32 contains a list of the procedures for collecting and viewing historical data and a cross-reference to where you can find information about each procedure.

Table 10. Collect and view historical data

Procedure	**Where to find information**
Configure and start collecting short-term data (24 hours).	*IBM Tivoli Monitoring User′s Guide:* ″Historical reporting″ (in ″Table and chart views″ chapter) *IBM Tivoli Monitoring Administrator′s Guide* “Disk capacity planning for historical data” on page 143 in this guide
Configure and start collecting longer-term data (more than 24 hours).	
View historical data in the Tivoli Enterprise Portal.	
Create reports from historical data using third-party reporting tools.	
Filter out unwanted data to see specific areas of interest.	

Chapter 4. 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. Every workspace has a set of properties associated with it.

This monitoring agent provides predefined workspaces. You cannot modify 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.

Predefined workspaces

The following predefined workspaces are provided with IBM Tivoli Monitoring: i5/OS Agent:

- "APPN Topology workspace" on page 34
- "Asynchronous workspace" on page 34
- "Binary Synchronous workspace" on page 34
- "Communications workspace" on page 35
- "Configuration, 2 workspace" on page 35
- "Database and Objects workspace" on page 35
- "Database Files workspace" on page 35
- "File Members workspace" on page 36
- "Disk and I/O, i5 workspace" on page 35
- "Distribution Queue workspace" on page 36
- "Ethernet workspace" on page 36
- "History Log workspace" on page 36
- "i5/OS workspace" on page 36
- "Integrated File System workspace" on page 37
- "Integrated File System Object workspace" on page 37
- "Job Log workspace" on page 37

- “Job Resource Details workspace” on page 37
- “Jobs and Queues, 2 workspace” on page 38
- “Managed Systems for i5/OS Logs workspace” on page 38
- “Messages and Spool, 2 workspace” on page 38
- “NetServer workspace” on page 38
- “Network workspace” on page 38
- “Object Library Details workspace” on page 39
- “SDLC workspace” on page 39
- “Subsystem Information workspace” on page 39
- “System Status, i5 workspace” on page 39
- “System Values workspace” on page 39
- “Token Ring workspace” on page 40
- “X.25 workspace” on page 40

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.

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

APPN Topology workspace

Use the APPN Topology predefined workspace to access information about the communications connections for the system. The predefined workspace includes the following views:

- An APPN Topology table view that displays information about APPN transmissions (such as type of APPN node that was used, timestamps, and Network ID for that node)
- A Take Action view that you can use to create and run Take Action commands

Asynchronous workspace

Use the Asynchronous predefined workspace to see information about the configuration and performance of asynchronous communications for the system. The workspace includes the following views:

- An Asynchronous table view that lists the line descriptions for the lines and displays details about the lines (such as information about the IOP and the utilization percent)
- A Take Action view that you can use to create and run Take Action commands

Binary Synchronous workspace

Use the Binary Synchronous predefined workspace to see information about the configuration and performance of the binary synchronous communications for the system. The predefined workspace includes the following views:

- A Binary Synchronous table view that lists the line descriptions for the lines and displays details about the lines (such as information about the IOP and the utilization percent)
- A Take Action view that you can use to create and run Take Action commands

Communications workspace

Use the Communications predefined workspace to see information for the configuration and status of the TCP/IP and APPN communications for the system. The predefined workspace includes the following views:

- An APPN Topology table view that displays information about APPN transmissions (such as the timestamps for the transmissions, the type of APPN node used, and the network ID for that node)
- A TCP/IP Logical Interface table view that displays information about the TCP/IP version 4 and version 6 interfaces (such as address, line used, status, and type)
- A TCP/IP Service table view that displays information about the TCP/IP services defined (such as name, the port and protocol used, and status)
- A Take Action view that you can use to create and run Take Action commands

Configuration, 2 workspace

Use the Configuration, 2 predefined workspace to access information about the system communications for the system (such as line description, controller description, and network attributes). The predefined workspace includes the following table views:

- Controller Description
- Device Description
- Line Description
- Network Attribute

The workspace is useful for pinpointing inactive communication sessions and quickly summarizing the network configuration for the system.

Database and Objects workspace

Use the Database and Objects predefined workspace to access a list of the libraries on the system. The predefined workspace includes the following views:

- A Database/Objects Library table view that you can use to display information about the libraries (such as the name of the library)
- A Take Action view that you can use to create and run Take Action commands

Database Files workspace

Use the Database Files predefined workspace to see the names of the files in the selected library. This workspace is selected as a link from the Database and Objects workspace. The predefined workspace includes the following views:

- A Database Files table view that you can use to display detailed information about the file
- A Take Action view that you can use to create and run Take Action commands

Disk and I/O, i5 workspace

Use the Disk and I/O, i5 predefined workspace to access information about the storage devices and I/O processors for the system. The predefined workspace includes the following views:

- A Disk Units table view that lists information and status for the disk units accessible by the system (such as the drive capacity, percentage of the disk that is being used, and protection type and status)

- A Controller Description table view that lists name of the controller descriptions and displays details about each of the controllers (such as the category and status)
- A Storage Pools table view that lists details and performance information for the system and user defined storage pools (such as the pool size, number of page faults, and transition counts)
- A Take Action view that you can use to create and run Take Action commands

In some cases, a column is blank. If a column is blank, the column does not apply to the type of hardware that you are using.

Distribution Queue workspace

Use the Distribution Queue predefined workspace to display information about configuration and status of the distribution queues that are defined for the system. The predefined workspace contains the following views:

- A Distribution Queue table view that displays information about the defined distribution queues (such as name, status, and send depths)
- A Take Action view that you can use to create and run Take Action commands

Ethernet workspace

Use the Ethernet predefined workspace to see information about the configuration and performance of the Ethernet communications for the system. The predefined workspace includes the following views:

- A Ethernet table view that lists the line descriptions for the lines and displays details about the lines (such as information about the IOP and the utilization percent)
- A Take Action view that you can use to create and run Take Action commands

File Members workspace

Use the File Members predefined workspace to see detailed information about the members in a selected file. This workspace is selected as a link from the Database Files workspace. The predefined workspace includes the following views:

- A Members for File table view that lists the name of the member and details for the member (such as the type of file and the percentages of space used for the file)
- A Take Action view that you can use to create and run Take Action commands

History Log workspace

Use the History Log predefined workspace to display information about messages in the system history log. The predefined workspace contains the following views:

- A History Log table view that displays information about the messages in the log (such as message ID, text, and severity)
- A Take Action view that you can use to create and run Take Action commands

i5/OS workspace

Use the i5/OS predefined workspace to see an overview for the system. The predefined workspace includes the following views:

- Three bar chart views that display System Status information about system CPU performance, auxiliary storage usage, and job counts

- An Operator Messages table view that lists the dates and times of the messages and displays details for the message (such as the type of message and the severity)

The Operator Messages table view has these advantages. You can:

- Reduce the number of times you have to access the message log.
- Quickly access information about messages to see if there are any messages that require urgent action.

Integrated File System workspace

Use the Integrated File System predefined workspace to display information about objects in the Integrated File System. The initial display lists information for objects found in the /root file system, which includes files, directories, and other file systems. You can use the initial display links to drill down to subdirectories, other objects, and other file system structures. The predefined workspace contains the following views:

- An Integrated File System table view that displays information about the objects in the /root file system (such as name, path, and object type and size)
- A Take Action view that you can use to create and run Take Action commands

Integrated File System Object workspace

Use the Integrated File System Object predefined workspace to display information about objects in the Integrated File System. If the object is a directory or library, you can see the objects it contains and use links to drill down to any subdirectories. For other objects, you can see information about the object. This workspace is selected as a link from the Integrated File System workspace. The predefined workspace contains the following views:

- A Integrated File System Object table view that displays information about the object (such as name and size) if the object is not a directory nor a library, or lists the objects in the directory or library along with their information (such as name and owner).
- A Take Action view that you can use to create and run Take Action commands

Job Log workspace

Use the Job Log predefined workspace to display information about messages in a job log. This workspace is selected as a link from the Jobs and Queues workspace.

The predefined workspace contains the following views:

- A Job Log table view that displays information about the messages in the job log (such as ID, text, and severity)
- A Take Action view that you can use to create and run Take Action commands

Job Resource Details workspace

Use the Job Resource Details predefined workspace to see detailed information about the selected job. This workspace is selected as a link from the Jobs and Queues workspace. The predefined workspace includes the following views:

- A Job Detail for *Job Name* table view that lists the start date and time for the job and displays details about running the job (such as the percentage of CPU that the job used)
- A Take Action view that you can use to create and run Take Action commands

Jobs and Queues, 2 workspace

Use the Jobs and Queues, 2 predefined workspace to access information about the jobs and job queues. The predefined workspace includes the following views:

- A Job Queue table view that lists the names of the job queue and displays details about the queues (such as the subsystem that retrieves jobs and the number of jobs in the queue)
- A Subsystem Information table view that lists the names of the subsystems and displays details about the subsystems (such as the subsystem status, pool name, and number of active jobs)
- A Job Resource Information table view that lists the active jobs and displays details about the jobs (such as the job name, job number, job user, and job type)
- A Take Action view that you can use to create and run Take Action commands

Managed Systems for i5/OS Logs workspace

Use the Managed Systems for i5/OS Logs predefined workspace to see messages from the QAUTOMON/QKMSOMLOG message queue. The predefined workspace includes the following views:

- A Managed Systems for OS/400 Logs table view that lists details for messages on the QAUTOMON/QKMSOMLOG message queue (such as the ID, data, severity, and send data and time).
- A Take Action view that you can use to create and run Take Action commands.

Messages and Spool, 2 workspace

Use the Messages and Spool, 2 predefined workspace to access information about the operator messages and output queues. The predefined workspace includes the following views:

- An Operator Messages table view that lists the dates and times of the messages and displays details for the message (such as the type of message and the severity). This view can help you reduce the number of times you have to access the message log, and you can quickly access information about messages to see if any messages require urgent action.
- An Output Queue table view that displays information such as name, status, and number of spool files for the defined output queues
- The Take Action view that you can use to create and run Take Action commands

NetServer workspace

Use the NetServer predefined workspace to display information about the support for Windows Network Neighborhood. The predefined workspace includes the following views:

- A NetServer table view that displays statistical information for supporting Windows Network Neighborhood (for example, file opens, session starts, and password violations)
- A Take Action view that you can use to create and run Take Action commands

Network workspace

Use the Network predefined workspace to see information for the configuration and status of the network interfaces and servers defined for the system. The predefined workspace includes the following views:

- A Network Interface table view that displays information about the network interface descriptions (such as name, category, and status)

- A Network Server table view that displays information about the network server descriptions (such as name, category, and status)
- A Take Action view that you can use to create and run Take Action commands

Object Library Details workspace

Use the Object Library Details predefined workspace to display the objects in the library. This workspace is selected as a link from the Database and Objects workspace.

The predefined workspace includes the following views:

- Object Library details for *Object Name* table view that displays information for the library objects (such as name, type, and owner)
- A Take Action view that you can use to create and run Take Action commands

SDLC workspace

Use the SDLC predefined workspace to see information about the configuration and performance of the SDLC communications for the system. The predefined workspace includes the following views:

- A SDLC table view that lists the line descriptions for the lines and displays details about the line (such as information about the IOP and the utilization percent)
- A Take Action view that you can use to create and run Take Action commands

Subsystem Information workspace

Use the Subsystem Information predefined workspace to access subsystem information and status. The predefined workspace includes the following views:

- A Subsystem Information table view that lists the names of the subsystems and displays details about the subsystems (such as the status, the number of jobs, and the number of pools)
- A Take Action view that you can use to create and run Take Action commands

System Status, i5 workspace

Use the System Status, i5 predefined workspace to access values for specific areas. The predefined workspace includes the following views:

- A System Status table view that displays an overview of system performance (such as basic, interactive, and database CPU usage, shared processor usage, upcapped CPU usage, and total amount of auxiliary storage usage)
- A System Statistics table view that displays information about batch jobs and users
- An Auxiliary Storage Pools table view that displays information and status for basic and independent auxiliary storage pools
- A CPU% chart view that displays overall CPU utilization percent
- A System Address and Aux Storage Pool% chart view that displays percentages for system ASP, permanent address, and temporary address usage

System Values workspace

Use the System Values predefined workspace to access the current settings for many of the i5/OS system values. The predefined workspace includes the following views:

- Activity System Values

- Device System Values
- General System Values (such as the serial number, level of security, interval to be used for expiring passwords, and whether an IPL is performed automatically after a power failure)
- IPL System Values
- Performance System Values
- Problem System Values
- User System Values

Token Ring workspace

Use the Token Ring predefined workspace to see information about the configuration and performance of the token ring communications for the system. The predefined workspace includes the following views:

- A Token Ring table view that lists the line descriptions for the lines and displays details about the line (such as information about the IOP and the utilization and response time percentages)
- A Take Action view that you can use to create and run Take Action commands

X.25 workspace

Use the X.25 predefined workspace to see information about the configuration and performance of the X.25 communications for the system. The predefined workspace includes the following views:

- A X.25 table view that lists the line descriptions for the lines and displays details about the line (such as information about the IOP, sent error percentage, and receive error percentages)
- A Take Action view that you can use to create and run Take Action commands

Chapter 5. Attributes reference

This chapter contains information about the following topics:

- Overview of attributes
- References for detailed information about attributes
- Descriptions of the attributes for each attribute group included in this monitoring agent
- Disk space requirements for historical data

About attributes

Attributes are the application properties being measured and reported by the Monitoring Agent for i5/OS, such as the amount of memory usage or the message ID.

Attributes are organized into 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 the Monitoring Agent for i5/OS and registers an *event* if the condition is met. You are alerted to events by indicator icons that appear 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*.

For a list of the attributes groups, a list of the attributes in each attribute group, and descriptions of the attributes for this monitoring agent, refer to the Attribute groups and attributes section in this chapter.

Attribute groups and attributes for the Monitoring Agent for i5/OS

You can use the following attribute groups with this agent:

- "Acct Journal attributes" on page 43
- "Alert attributes" on page 45
- "APPN Topology attributes" on page 47

- “Auxiliary Storage Pool attributes” on page 48
- “Comm Async attributes” on page 50
- “Comm Bisync attributes” on page 51
- “Comm Ethernet attributes” on page 51
- “Comm SDLC attributes” on page 52
- “Comm Token Ring attributes” on page 53
- “Comm X25 attributes” on page 54
- “Controller Description attributes” on page 55
- “Database Member attributes” on page 57
- “Device Description attributes” on page 59
- “Disk Unit attributes” on page 62
- “Distribution Queue attributes” on page 63
- “History Log attributes” on page 64
- “i5 Disk attributes” on page 66
- “I/O Processor attributes” on page 68
- “Integrated File System Object attributes” on page 69
- “Job attributes” on page 71
- “Job Log attributes” on page 79
- “Job Queue attributes” on page 80
- “Line attributes” on page 81
- “Management Central Events attributes” on page 83
- “Messages attributes” on page 86
- “Miscellaneous attributes” on page 89
- “NetServer attributes” on page 90
- “Network attributes” on page 91
- “Network Interface attributes” on page 94
- “Network Server attributes” on page 96
- “Object attributes” on page 98
- “Output Queue attributes” on page 103
- “Security Jrn AuditJrn attributes” on page 105
- “Security Jrn AuthFail attributes” on page 106
- “Security Jrn ChgAuth attributes” on page 110
- “Security Jrn ChgOwner attributes” on page 112
- “Security Jrn ChgUserProf attributes” on page 113
- “Security Jrn JobDesc attributes” on page 115
- “Security Jrn Network attributes” on page 116
- “Security Jrn Password attributes” on page 117
- “Security Jrn ProfSwap attributes” on page 118
- “Security Jrn ProgAdopt attributes” on page 119
- “Security Jrn RestoreJob attributes” on page 120
- “Security Jrn RestoreProg attributes” on page 120
- “Security Jrn SYSVAL attributes” on page 121
- “Storage Pool attributes” on page 122
- “Subsystem attributes” on page 123
- “System Statistics attributes” on page 124

- “System Status attributes” on page 125
- “System Values Acct attributes” on page 127
- “System Values attributes” on page 130
- “System Values Device attributes” on page 132
- “System Values IPL attributes” on page 133
- “System Values Perf attributes” on page 134
- “System Values Prob attributes” on page 136
- “System Values User attributes” on page 137
- “TCP/IP Logical Interface attributes” on page 139
- “TCP/IP Service attributes” on page 142

The following sections contain descriptions of these attribute groups, which are listed alphabetically. Each description contains a list of attributes in the attribute group.

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.

Acct Journal attributes

The Acct Journal attribute group includes attributes that you can use to monitor work management. The attributes can only be used if the accounting level system value (QACGLVL) is set to *JOB. When you start monitoring for a situation using the attributes, the accounting journal receiver is locked. (While the journal receiver is locked, you cannot detach it from the journal, save it, or delete it.) Coding specific compare values for Job Name and User attributes reduces the amount of data IBM Tivoli Monitoring for i5/OS has to handle, improving performance. Under certain circumstances (especially on large systems), failing to specify one or more of these attributes might overload IBM Tivoli Monitoring for i5/OS and cause the situation to be unevaluated.

If you use the OS400 Acct Journal attributes, the i5/OS Accounting Journal, QACGJRN, must exist in library QSYS. In addition, you must have created some journal receivers and attached them to the Accounting journal. Refer to the IBM documentation of accounting journal management. Changing the system value QDATE and QTIME affects exactly when OS400 Acct Journal attributes are picked up.

For example, if you change the system values to a future date or time, such as the year 2010, any journal entries that occur are marked with this future date. When you change the system values back to the current date, any subsequent journal entries are correctly marked with the current date. Modifying the system value in this way marks older journal entries with a more recent date.

If you start a journal situation, all journal entries that have a date and time equal to or greater than the current date are returned. If an older entry that is predated with the year 2000 date is found, the situation returns all entries following the year 2000 entry. Some of these entries occurred before the situation was started. If a large number of these journal entries exist, they can cause the situation to time out. To avoid this problem, remove the current journal receiver or receivers from the JRN and create and attach a new one.

Acct Code The accounting code assigned to the job by the system. As the job is processed, the system uses the accounting code to collect statistics on the system resources used by the job. The valid value is an alphanumeric string with a maximum of 15 characters.

Completion Code The two-digit code that indicates how the job ended. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions. The following values are valid:

00	Normal completion
10	Normal completion during controlled end or controlled subsystem end
20	Job exceeded end severity
30	Job ended abnormally
40	Job ended before becoming active
50	Job ended while active
60	Subsystem ended abnormally while job was active
70	System ended abnormally while job was active
80	Job completed in the time limit
90	Job forced to complete after the time limit has ended
99	CHGACGCDE command caused an accounting entry.

CPU Time The processing time used by the job (in seconds). The valid value is a decimal number from 0.000 - 2147483647.000

Database I/O Operations The total number of database read, write, update, delete, FEOD, release, commit, and rollback operations. The valid value is an integer from 0 - 2147483647.

Date The date when the job entered the system. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Date and Time The date and time when the job entered the system. For batch jobs, this is the date and time the job was placed in a job queue. The valid value is a date and time in the format CYYMMDDHHmmSSmmm (For example, 0961002103000000 indicates a century bit of 0, a date of October 2, 1996, and a time of 10:30:00:000.)

Job Name The name of the job. The valid value is an alphanumeric string with a maximum of 10 characters.

Job Number The number the system assigned to the job. The valid value is an alphanumeric string with a maximum of 6 characters.

Job Type Indicates the type of job. The following values are valid:

A	Autostart job
B	Batch job (includes communications and MRT)
I	Interactive job
M	Subsystem monitor
R	Spooling reader

W	Spooling writer

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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 Date The date when the job started. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Start Date and Time The date and time when the job started. For batch jobs, this is the date and time the job left a job queue and started running. The valid value is a date and time in the format CYYMMDDHHmmSSmmm. For example, 0961002103000000 indicates a century bit of 0, date of October 2, 1996, and time of 10:30:00:000.

Start Time The time when the job started. For batch jobs, this is the time the job left a job queue and started running. The valid value is a time in the format HHMMSS (For example, 103000 is a time of 10:30:00 a.m.)

Time The time when the job entered the system. For batch jobs, this is the time the job was placed on the job queue. The valid value is a time in the format HHMMSS (For example, 103000 indicates a time of 10:30:00 a.m.)

Transaction Number The number of transactions run by the job. The valid value is an integer from 0 - 2147483647.

Transaction Time Total transaction time (in seconds). The valid value is an integer from 1 - 2147483647.

User The user of the job. The valid value is an alphanumeric string with a maximum of 10 characters.

Alert attributes

The Alert attributes are notification attributes in the operational areas of problem analysis and work management. These attributes can be used only if the i5/OS network attributes are set to enable alerts.

Use the i5/OS Display Network Attributes (DSPNETA) command to view the network attributes.

Analysis Available Specifies whether problem analysis is available for a message. The following values are valid:

*YES	Problem analysis is available for this problem or the alert is for a problem analysis message.
*NO	The message is not for problem analysis.

Delayed Specifies whether an alert has been delayed. The following values are valid:

*YES	The alert was delayed.
*NO	The alert has never been delayed.

Description The description of the alert. The text is found in the QALRMSG message file in the QSYS library. The prefix for the message ID is ALD, and the suffix is the value of this field. The valid value is an alphanumeric string with a maximum of 4 characters.

Description (Unicode) The description of the alert. The text is found in the QALRMSG message file in the QSYS library. The prefix for the message ID is ALD, and the suffix is the value of this field. The valid value is a string with a maximum of 12 bytes.

First Cause The most probable cause for the alert. The valid value is an alphanumeric string with a maximum of 4 characters.

First Cause (Unicode) The most probable cause for the alert. The valid value is a string with a maximum of 12 bytes.

Held Specifies whether an alert has been held. The following values are valid:

*YES	The alert was held for the purpose of sending to the focal point.
*NO	The alert has never been held.

ID Identifier assigned to the alert. The valid value is an alphanumeric string with a maximum of 4 characters.

Local Specifies whether the alert has been locally generated or received by another system. The following values are valid:

*YES	The alert is a locally generated alert.
*NO	The alert is a received alert.

Message ID The ID of the message causing an alert. The valid value is an alphanumeric string with a maximum of 7 characters.

Message Severity The severity of the message causing the alert. The higher the number, the severe the error. The valid value is an integer from 0 - 99.

Operator Generated Specifies whether the alert was generated by an operator. The following values are valid:

*YES	The alert was generated by an operator.
*NO	The alert was not generated by an operator.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Origin System The system where the associated problem entry occurred. The valid value is an alphanumeric string with a maximum of 20 characters. If the field is blank, there is no problem log entry associated with the alert.

Problem ID The ID of the problem associated with the alert. If no problem log entry is associated with the alert, this field is blank. The valid value is an alphanumeric string with a maximum of 10 characters. I

Resource The name of the resource that detected the error condition. The valid value is an alphanumeric string with a maximum of 10 characters.

Resource Type The type of resource that detected the error condition. The failing resource is the lowest resource in the resource hierarchy. The valid value is an alphanumeric string with a maximum of 3 characters.

Type The type of alert. The text for the code point is found in the QALRMSG message file in the QSYS library. The prefix for the message ID is ALT, and the suffix is the value of this field followed by 00. The valid value is an alphanumeric string with a maximum of 2 characters.

APPN Topology attributes

The APPN Topology attribute group includes attributes that you can use to monitor APPN nodes.

CPNAME The control point name for the node. The valid value is an alphanumeric string with a maximum of 8 characters.

Date The date that the attributes were reported.

Date and Time The date and time that the attributes were reported. The valid value is a date and time in the format CYYMMDDHHmmSSmmm (For example, 0961002103000000 indicates a century bit of 0, a date of October 2, 1996, and a time of 10:30:00:000.)

NETID The network ID for the node. The valid value is an alphanumeric string with a maximum of 8 characters.

Node Congestion Indicates whether there is congestion for a node (indicates excessive traffic or excessive usage). The following values are valid:

*YES	There is congestion for the node.
*NO	The node is not congested.

Node Type The type of APPN node. The following values are valid:

*EN	Node is low entry networking or and APPN end node.
*NN	Node is an APPN networking node.
*VN	Node is an APPN virtual node.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

TransGroup Controller Name The name of the controller description object for the transmission group. The valid value is an alphanumeric string with a maximum of 8 characters. If the field is blank, the transmission group is not associated with the local node.

TransGroup DestNode CPNAME The APPN transmission group control point name for the destination node. The valid value is an alphanumeric string with a maximum of 8 characters.

TransGroup DestNode NETID The APPN transmission group network ID for the destination node. The valid value is an alphanumeric string with a maximum of 8 characters.

TransGroup Number The APPN transmission group number that is used to identify a unique logical link between 2 nodes. The valid value is an integer from 0 - 2147483647.

TransGroup Operational The APPN transmission group status between two nodes. The following values are valid:

*YES	Operational status between 2 nodes is yes.
*NO	Operational status between 2 nodes is no.

Time The time that the attributes were reported. The valid value is a time in the format HHMMSS (For example, 103000 indicates a time of 10:30:00 a.m.)

Update Type Controls how the topology information is collected. The following values are valid:

CURRENT	Topology existed at the time the situation is first evaluated. Topology data is returned on the first evaluation only.
UPDATED	A node or transmission group record was updated.
DELETED	A node or transmission group was deleted. This situation raises only after the node has been deleted for at least 21 days.
INSERTED	A new node or transmission group was added.

Auxiliary Storage Pool attributes

Use the Auxiliary Storage Pool (ASP) attributes to monitor the status and details for the basic and independent ASPs. The attributes are returned for active and inactive independent ASPs. Auxiliary Storage Pool attributes are sampled attributes in the storage and configuration operations.

Capacity Specifies the total space, in megabytes, on the storage media that is allocated to the ASP. A varied-off independent ASP can contain a zero in this field if the system cannot determine which disk units are assigned to the ASP.

Name The name of the independent auxiliary storage pool, or blank for basic ASPs. The name is an alphanumeric string with up to 10 characters.

Number The unique number that identifies the auxiliary storage pool. The ASP number can have a value from 1 - 255. A value of 1 indicates the system ASP. A value of 2 - 32 indicates a basic user ASP. Independent user ASPs have a value of 33 - 255.

Number of Disk Units The number of disk units assigned, which is the number of configured, non-mirrored units plus the number of mirrored pairs allocated to the ASP.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Overflow Storage Indicates the number of bytes, in megabytes, of auxiliary storage that overflowed from a basic ASP into the system ASP. This number is one or greater if any bytes have overflowed.

Protected Capacity Specifies the total number of bytes, in megabytes, of auxiliary storage that is protected by mirroring or device parity in the ASP. A varied-off independent ASP can have zero in this field if the system cannot determine the disk units that are assigned to the ASP.

Protected Used Percent The percentage of protected capacity that is currently used for objects or internal computer functions. If the protected capacity is zero, the used percent value is also zero.

Status The status of the ASP. Basic ASPs are always in the VARIED_ON status. The following values are valid:

- VARIED_OFF specifies that the independent ASP is not active. (0)
- VARIED_ON specifies that the basic or independent ASP is active. (1)

System Storage™ Percent Specifies the percent of capacity that is currently allocated to system storage.

Type The type of ASP. The following values are valid:

- Basic specifies a basic user ASP or the system ASP. (0)
- Independent specifies an independent ASP. (1)
- Independent_Primary specifies an independent ASP that is the primary ASP in an ASP group. (2)
- Independent_Secondary specifies an independent ASP that is a secondary ASP in an ASP group. (3)

- Independent_UDFS specifies an independent, UDFS (User-defined File System) ASP. (4)

Unprotected Capacity Specifies the total number of bytes, in megabytes, of auxiliary storage that is not protected by mirroring or device parity in the ASP. A varied-off independent ASP can have zero in this field if the system cannot determine which disk units are assigned to the ASP.

Unprotected Used Percent The percentage of unprotected capacity that is currently used for objects or internal computer functions. If the unprotected capacity is zero, the used percent value is also zero.

Utilization Percent The percentage of total capacity that is currently used for objects or internal computer functions. If the capacity is zero, the used percent value is also zero.

Comm Async attributes

The Comm Async attribute group includes attributes that you can use to monitor the asynchronous communications for your system.

Error Percent The percent of protocol data units received with errors during the last monitor interval. This value can indicate congestion on the communications line or that the quality of the communications line is poor. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

IOP Bus Address The IOP bus address. The valid value is an integer from 0 - 31. A value of -1 indicates NA.

IOP Bus Number The IOP bus number. The valid value is an integer from 0 - 255. A value of -1 indicates NA.

IOP Name The system resource name associated with the IOP that controls the disk unit. The valid value is an alphanumeric string with a maximum of 10 characters.

Line Description The name of the description for this line. The valid value is an alphanumeric with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Utilization Percent The percent of the capacity of the line that was used during the last interval (measured in bits or bytes per second). The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Comm Bisync attributes

The Comm Bisync attribute group includes attributes that you can use to monitor the bisynchronous communications for your system.

IOP Bus Address The IOP bus address. The valid values are 0 - 31. A value of -1 indicates NA.

IOP Bus Number The IOP bus number. The valid values are 0 - 255. A value of -1 indicates NA.

IOP Name The system resource name associated with the IOP on which this protocol runs. The valid value is an alphanumeric string with a maximum of 10 characters.

Line Description The name of the line description for this line. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Receive Error Percent The percent of data characters received that contained errors. This value can indicate congestion on the communication line or that the quality of the communications line is poor. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Send Error Percent The percent of data characters transmitted that had to be retransmitted. This value can indicate congestion on the communications line or that the quality of the communications line is poor. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Utilization Percent The percent of the capacity of the line that was used during the last interval (measured in bits or bytes). The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Comm Ethernet attributes

The Comm Ethernet attribute group includes attributes that you can use to monitor the Ethernet communications for your system.

IOP Bus Address The IOP bus address. The valid value is an integer from 0 - 31. A value of -1 indicates NA.

IOP Bus Number The IOP bus number. The valid value is an integer from 0 - 255. A value of -1 indicates NA.

IOP Name The system resource name associated with the IOP that controls the disk unit. The valid value is an alphanumeric string with a maximum of 10 characters.

Local RNR Percent The percent of information (I) frames received that resulted in a receive-not-ready (RNR) frame being transmitted from the local system to the remote controller or system. This transmission often indicates congestion at the local system. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Line Description The name of the line description for this line. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Remote RNR Percent The percent of information (I) frames transmitted that resulted in a receive-not-ready (RNR) frame being returned by the remote controller or system. This transmission often indicates congestion at the remote system or controller. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Response Time Percent The percent of total frames transmitted that resulted in a time out of the response (TI) timer of the local area network. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Utilization Percent The percent of the capacity of the line that was used during the last interval (measured in bits or bytes per second). The valid value is an integer from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Comm SDLC attributes

The Comm SDLC attribute group includes attributes that you can use to monitor SDLC communications for your system.

Controller Poll Percent The percentage of the active line that is spent by the line polling inoperative controllers during the sample interval. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

IOP Bus Address The IOP bus address. The valid value is an integer from 0 - 31. A value of -1 indicates NA.

IOP Bus Number The IOP bus number. The valid value is an integer from 0 - 255. A value of -1 indicates NA.

IOP Name The system resource name associated with this IOP. The valid value is an alphanumeric string with a maximum of 10 characters.

Local RNR Percent The percent of information (I) frames received that caused a receive-not-ready (RNR) frame to be transmitted from the local system to the remote controller or system. This value often indicates congestion at the local system. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Line Description The name of the line description for this line. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Receive Error Percent The percent of received data characters that contained errors. This value can indicate congestion on the communication line or that the quality of the communication line is poor. The valid value is an integer from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Remote RNR Percent The percent of transmitted information (I) frames that caused a receive-not-ready (RNR) frame to be returned by the remote controller or system. This value often indicates congestion at the remote system or controller. The valid value is an integer from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Send Error Percent The percent of data characters transmitted that had to be retransmitted. This value can indicate congestion on the communications line or that the quality of the communications line is poor. The valid value is an integer from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Utilization Percent The percent of the capacity of the line that was used during the last interval (measured in bits or bytes per second). The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Comm Token Ring attributes

The Comm Token Ring attribute group includes attributes that you can use to monitor the performance of token ring communications.

IOP Bus Address The IOP bus address. The valid value is an integer from 0 - 31. A value of -1 indicates NA.

IOP Bus Number The IOP bus number. The valid value is an integer from 0 - 255. A value of -1 indicates NA.

IOP Name The system resource name that is associated with the IOP that controls the disk unit. The valid value is an alphanumeric string with a maximum of 10 characters.

Line Description The name of the line description for this line. The valid value is an alphanumeric string with a maximum of 10 characters.

Local RNR Percent The percent of information (I) frames received that caused a receive-not ready (RNR) frame to be transmitted from the local system to the remote controller or system. This value often indicates congestion at the local system. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Remote RNR Percent The percent of information (I) frames transmitted that resulted in a receive-not-ready (RNR) frame being returned by the remote controller or system. This transmission often indicates congestion at the remote system or controller. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Response Time Percent The percentage of the total frames transmitted that resulted in a time out of the response (TI) timer of the local area network. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Utilization Percent The percentage of the capacity of the line that was used during the last interval (measured in bits or bytes). The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Comm X25 attributes

The Comm X25 attribute group includes attributes that you can use to monitor X.25 communications for your system.

Average Utilization Percent Average of the attributes Send Utilization Percent and Receive Utilization Percent. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions. The valid value is an integer from 0 - 100 or one of these values.

- *GUIDELINE
- *THRESHOLD

IOP Bus Address The IOP bus address. The valid value is an integer from 0 - 31. A value of -1 indicates NA.

IOP Bus Number The IOP bus number. The valid value is an integer from 0 - 255. A value of -1 indicates NA.

IOP Name The system resource name associated with the IOP that controls the disk unit. The valid value is an alphanumeric string with a maximum of 10 characters.

Line Description The name of the line description for this line. The valid value is an alphanumeric string with a maximum of 10 characters.

Local RNR Percent The percent of information (I) frames received that resulted in a receive-not-ready (RNR) frame being transmitted from the local system to the remote controller or system. This transmission often indicates congestion at the local system. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Receive Error Percent The percent of data characters received that contained errors. This value can indicate congestion on the communication line or that the quality of the communications line is poor. The valid value is an integer from 0 - 100.

Receive Utilization Percent The percentage of the capacity of the line to receive that was used during the last monitor interval. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Remote RNR Percent The percent of information (I) frames transmitted that resulted in a receive-not-ready (RNR) frame being returned by the remote controller or system. This transmission often indicates congestion at the remote system or controller. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Send Error Percent The percent of data characters transmitted that had to be retransmitted. This value can indicate congestion on the communications line or that the quality of the communications line is poor. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Send Utilization Percent The percentage of the capacity of the line to send that was used during the last monitor interval. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Controller Description attributes

The Controller Description attribute group includes attributes that provide information such as category, name and status about the controller.

Category The category for the controller description. The following values are valid:

- An alphanumeric string with a maximum of 10 characters
- APPC
- ASYNC
- BSC
- FNC

- HOST
- LWS
- NET
- RTL
- RWS
- TAP
- VWS

Name A name for the controller. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Status Indicates the state or condition (status) of a controller. The following values are valid:

00	VARIED_OFF
01	OPERATIONAL
02	AS/36_DISABLED
05	DEALLOCATED
06	UNPROTECTED
07	ALLOCATED
08	STAND-ALONE
10	VARY_OFF_PENDING
20	VARY_ON_PENDING
21	VARY_ON_PENDING/DETACHED
22	VARY_ON_PENDING/ALLOCATE
30	VARIED_ON
31	VARIED_ON/ALLOCATE
32	VARY_ON_or_CNN_PENDING
33	AS/36_ENABLED
40	CONNECT_PENDING
50	SIGNON_DISPLAY
51	ACTIVE_or_CNN_PENDING
60	ACTIVE
61	ACTIVE/DETACHED
62	ACTIVE/SOURCE
63	ACTIVE READER
64	ACTIVE/TARGET
65	ACTIVE/ALLOCATE

66	ACTIVE WRITER
67	AVAILABLE
70	HELD
71	HELD/DETACHED
72	HELD/SOURCE
73	HELD/TARGET
74	HELD/ALLOCATE
75	POWERED_OFF
80	RCYPND
81	RCYPND/DETACHED
82	RCYPND/SOURCE
83	RCYPND/TARGET
84	RCYPND/ALLOCATE
90	RCYCNL
91	RCYCNL/DETACHED
92	RCYCNL/SOURCE
93	RCYCNL/TARGET
94	RCYCNL/ALLOCATE
95	SYSTEM_REQUEST
96	REBUILD
100	FAILED
101	FAILED/DETACHED
102	FAILED/SOURCE
103	FAILED READER
104	FAILED/TARGET
105	FAILED/ALLOCATE
106	FAILED WRITER
107	SHUTDOWN
110	DIAGNOSTIC MODE
111	DAMAGED
112	LOCKED
113	UNKNOWN
114	DEGRADED
200	INVALID_STATUS

Database Member attributes

The Database Member attribute group includes attributes that you can use to monitor storage and work management.

Coding specific compare values for Member, File, and Library reduces the amount of data that the product has to handle. This reduction improves system performance. Failing to specify one or more of these attributes can overload the product. Such situations and queries are not evaluated.

Note that you cannot use the OR function between any of the predicates when building situations using this group of attributes.

File The name of the file from which the member list was retrieved. The valid value is an alphanumeric string with a maximum of 10 characters.

File Attribute The type of file found. The following values are valid:

PF	Physical file
LF	Logical file
DDMF	Distributed Data Management file

Increments Left The remaining number of increments that can be automatically added to the member size. This value applies only to physical files The value for logical files is 0. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Library The name of the library that includes the object. The valid value is an alphanumeric string with a maximum of 10 characters.

Member The name of the member whose description is being retrieved. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Percent Delete Records The percentage of the current number of records that have been deleted. This value applies to data files only. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Percent Used The percentage of the capacity of the member that is currently being used. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Records Unused The number of records that are not being used. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Records Used The number of records used. The valid value is an integer and can be -1 if the member is suspended, or -2 if the number is greater than 2,147,483,647 or from zero to 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Source File Flag Indicates whether the file is a source file or a data file. The following values are valid:

*DATA	File is a data file.

*SOURCE	File is a source file.

Source Member Type If this is a source file, this is the type of source member. The valid value is an alphanumeric string with a maximum of 10 characters.

SQL Type The type of Structured Query Language (SQL) file. The following values are valid:

Blank	The file is not an SQL file.
TABLE	The file is a non-keyed physical file that contains field characteristics.
VIEW	The file is a logical file over one or more tables or views. This SQL file type provides a subset of data in a particular table or a combination of data from more than one table or view.
INDEX	The file is keyed logical file over one table. The keyed logical file is used whenever access to records in a certain order is requested frequently.

Device Description attributes

The Device Description attribute group includes attributes that you can use to monitor the performance and configuration of communication devices.

Category The category of the device description. The category is an alphanumeric string with a maximum of 10 characters. The following values are valid:

Note: On queries, if you do not specify a category using the Category attribute, it defaults to *CMN.

- *APPC
- *ASP
- *ASYNC
- *BSC
- *CMN
- *CRP
- *DKT
- *DSP
- *FNC
- *HOST
- *INTRA
- *MLB
- *NET
- *OPT
- *OPTMLB
- *PRT
- *RTL
- *SNPT
- *SNUF
- *TAP
- *TAPMLB
- *VRTDSP

- *VRTPRT

Job Name The name of the job associated with an active device (if applicable). The valid value is an alphanumeric string with a maximum of 10 characters. Do not use * values.

Job Number The job number portion of a full qualified job name. The valid value is an alphanumeric string with a maximum of 6 characters. Do not use * values.

Job User The user name portion of a full qualified job name. The valid value is an alphanumeric string with a maximum of 10 characters. Do not use * values.

Name A name or identifier describing a device. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Passthru Device The name of an upstream device used to complete a pass-through session (if applicable). The valid value is an alphanumeric string with a maximum of 10 characters. Do not use * values.

Status The status returned that indicates the state or condition of a device (such as printers, modems, and tapes). The following values are valid:

00	VARIED OFF
01	OPERATIONAL
02	AS/36_DISABLED
05	DEALLOCATED
06	UNPROTECTED
07	ALLOCATED
08	STAND-ALONE
10	VARY OFF PENDING
20	VARY ON PENDING
21	VARY_ON_PENDING/DETACHED
22	VARY_ON_PENDING/ALLOCATE
30	VARIED ON
31	VARIED_ON/ALLOCATE
32	VARY_ON_or_CNN_PENDING
33	AS/36_ENABLED
40	CONNECT PENDING
50	SIGNON DISPLAY
51	ACTIVE_or_CNN_PENDING
60	ACTIVE

61	ACTIVE/DETACHED
62	ACTIVE/SOURCE
63	ACTIVE READER
64	ACTIVE/TARGET
65	ACTIVE/ALLOCATE
66	ACTIVE WRITER
67	AVAILABLE
70	HELD
71	HELD/DETACHED
72	HELD/SOURCE
73	HELD/TARGET
74	HELD/ALLOCATE
75	POWERED OFF
80	RCYPND
81	RCYPND/DETACHED
82	RCYPND/SOURCE
83	RCYPND/TARGET
84	RCYPND/ALLOCATE
90	RCYCNL
91	RCYCNL/DETACHED
92	RCYCNL/SOURCE
93	RCYCNL/TARGET
94	RCYCNL/ALLOCATE
95	SYSTEM_REQUEST
96	REBUILD
100	FAILED
101	FAILED/DETACHED
102	FAILED/SOURCE
103	FAILED READER
104	FAILED/TARGET
105	FAILED/ALLOCATE
106	FAILED WRITER
107	SHUTDOWN
110	DIAGNOSTIC MODE
111	DAMAGED
112	LOCKED
113	UNKNOWN
114	DEGRADED
200	INVALID_STATUS

Type The type of the device (either its basic category or a specific device type identifier). Valid values are 10 alphanumeric characters long, and are one of the **Category** attribute values, or a device type such as 3179.

Disk Unit attributes

The Disk Unit attribute group contains attributes that you can use to monitor the performance of storage. You can collect data that is based on the cumulative value of disk unit counters. The Disk Unit attribute group is similar to the i5 Disk group, and includes several of the same attributes. However, the i5 Disk group includes disk protection information and uses system interfaces that are faster, using fewer resources than this Disk Unit group. You can still use this Disk Unit group if you require its performance attributes, but use the i5 Disk attribute group when possible.

Arm Number The unique identifier for the disk unit. The valid value is an alphanumeric string maximum of 4 characters.

Aux Storage Pool Number The auxiliary storage pool (ASP) to which the disk unit is currently allocated. The following values are valid:

0	The disk unit is not allocated.
1	The disk unit is allocated to the system ASP.
2 - 32	The disk unit is allocated to a basic user ASP.
33 - 255	The disk unit is allocated to an independent user ASP.

Average Queue Length The sum of the number of I/O operations awaiting service (including any operation in progress) at the end of each collection interval, divided by the number of collections taken during the last monitor interval. The valid value is an integer from 0 - 2147483647.

Average Service Time The average service time (in seconds) during the last monitor interval. The program calculates the number by dividing the percentage of samples where the disk arm is busy by the sum of read data commands and write data commands. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Checksum Number Specifies the checksum set to which this unit is currently allocated. The following values are valid:

0	The number is not currently assigned to a checksum value.
1 - 16	Checksum is set.

Drive Capacity The capacity of the drive in Kilobytes. The total number of bytes of auxiliary storage provided on the unit for the storage of objects and internal computer functions when the auxiliary storage pool (ASP) containing it is not under checksum protection. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Drive Type The type of disk drive. The valid value is an alphanumeric string with a maximum of 4 characters.

IOP Bus Address The IOP bus address. The valid value is an integer from 0 - 31. A value of -1 indicates NA.

IOP Bus Number The IOP bus number. The valid value is an integer from 0 - 255. A value of -1 indicates NA.

IOP Name The system resource name associated with the IOP that controls this disk unit. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Percent Busy The percentage of time that the actuator for the disk unit is busy during the last monitor interval. An actuator moves the read and write heads within an auxiliary storage device. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Percent Permanent Used The percent of permanent disk capacity used (checksum case). The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Percent Used The percentage of the capacity of the member that is currently being used. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Distribution Queue attributes

Use the Distribution Queue attribute group to monitor the queue status and the distributions for queue types. The following types are available:

- *DLS (Document library services)
- *RPDS (VM/MVS bridge function and SNADS extended bridge function, which includes the X.400 message handling services and the Simple Mail Transfer Protocol (SMTP))
- *SNADS (SNA distribution services)
- *SVDS (SystemView® distribution services)

This attribute group can be used in historical collections but is not collected by default. The Distribution Queue attributes are sample attributes in the operational area of communications.

Depth high The number of distributions currently on the queue for high service levels. Valid entries are numeric values in the range 0 to 2147483647.

Depth normal The number of distributions that are currently on the queue for data low service levels. Valid entries are numeric values in the range 0 to 2147483647.

Force time high The specific time of the day (24-hour clock HHMM format) when distributions in the high service level queue are sent regardless of send depth. Valid entries are simple alphanumeric text strings with a maximum length of 4 characters.

Force time normal The specific time of the day (24-hour clock HHMM format) when distributions in the data low service level queue are sent, regardless of send depth. Valid entries are simple alphanumeric text strings with a maximum length of 4 characters.

From time high The start of the transmission time (24-hour clock HHMM format) for the high service level queue, if no other controlling considerations exist. Valid entries are simple alphanumeric text strings with a maximum length of 4 characters.

From time normal The start of the transmission time (24-hour clock HHMM format) for the data low service level queue, if no other controlling considerations exist. Valid entries are simple alphanumeric text strings with a maximum length of 4 characters.

Name The name of the distribution queue. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Send depth high The number of distributions that you require on the high service level queue before sending can begin, or zero if they are not sent automatically. Valid entries are numeric values in the range 0 to 2147483647.

Send depth normal The number of distributions that you require on the data low service level queue before sending can begin, or zero if they are not sent automatically. Valid entries are numeric values in the range 0 to 2147483647.

Status high The status of the high service level distributions. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Status normal The status of the data low service level distributions. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

To time high The end of the transmission time (24-hour clock HHMM format) for the high service level queue. Valid entries are simple alphanumeric text strings with a maximum length of 4 characters.

To time normal The end of the transmission time (24-hour clock HHMM format) for the data low service level queue. Valid entries are simple alphanumeric text strings with a maximum length of 4 characters.

History Log attributes

The History Log attribute group can be used in historical collections, but the group is not collected by default. You can use these sampled attributes in the operational areas of problem analysis and work management to monitor the messages in the system history log.

Date and time The date and time that the message arrived in the history log. The format is MM/DD/YY HH:mm:SS, where: MM = Month; DD = Day; YY = Year; HH = Hour; mm = Minute; SS = Second.

Library The name of the message file library, or blank if this message is immediate. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Message file The name of the message file that contains the message, or blank if this message is immediate. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Message ID The message identification code, or blank if this message is immediate. Valid entries are alphanumeric strings with a maximum of seven characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Send job name The name of the job that sent the message. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Send job number The number of the job that sent the message. Valid entries are alphanumeric strings with a maximum length of 6 characters.

Send job user The user name of the job that sent the message. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Severity The severity level of the message. Valid entries are integers in the range 0 to 99.

Text (Unicode) The message text with included substitution data. Valid entries are strings with a maximum of 396 characters. This attribute supports UTF-8 characters.

Type The type of message. Valid entries are simple numeric text strings with a maximum length of two characters. The following table lists the available types and their associated codes:

01	Completion
02	Diagnostic
04	Informational
05	Inquiry
06	Sender copy
08	Request
10	Request with prompting
14	Notify, exception already handled

15	Escape, exception already handled
16	Notify, exception not handled
17	Escape, exception not handled
21	Reply, not checked for validity
22	Reply, checked for validity
23	Reply, message default used
24	Reply, system default used
25	Reply, from system reply list
26	Reply, from exit program

i5 Disk attributes

Use the i5 Disk attributes to monitor the status and details for disk units, including the type and status of protection in use for the disk units. i5 Disk attributes are sampled attributes in the operational areas of configuration and operations.

The i5 Disk attribute group is similar to the OS/400 Disk Unit attribute group and includes several of the same attributes. The differences are that the i5 Disk attributes are gathered using a faster mechanism, and they contain disk protection and status information added over the past few i5/OS releases. The OS/400 Disk Unit attributes can still be used for their detailed performance numbers, but they continue to use the performance collection function of i5/OS. The performance collection function requires several fifteen second or longer intervals to gather data, and uses more i5/OS resources than the mechanism used for the i5 Disk attributes.

ASP number The number of the Auxiliary Storage Pool to which this unit is currently allocated. A value of 0 indicates that this unit is currently unallocated. A value of 1 specifies the system ASP. A value of 2 - 32 indicates a basic user ASP. Independent user ASPs have a value of 33 - 255.

Capacity The space, in number of megabytes, on the non-mirrored unit or mirrored pair. This attribute is the capacity of the unit prior to any formatting or allocation of space by the system. For a mirrored pair, this space is the number of bytes of auxiliary storage on either one of the mirrored units. Unit capacity is also known as “logical capacity”. For compressed drives the logical capacity is dynamic and changes depending on how well the data is compressed. This value is zero for non-configured units.

Compressed Indicates that the unit uses compression. The logical capacity of the unit might be greater than its physical capacity in bytes, depending on how well the data can be compressed. The following values are valid:

- No (0)- unit does not use compression
- Yes (1)- unit uses compression

Mirror status The status of the mirrored unit. The following values are valid:

N/A (0)	The disk unit is not mirrored.
Active (1)	This mirrored unit of a mirrored pair is active (that is, on-line with current data).
Synchronizing (2)	The mirrored unit is being synchronized.
Suspended (3)	This mirrored unit is suspended.

Last_Known_Active (41)	The unit has not reported in this IMPL. Its last known state was Active.
Last_Known_Synchronizing (42)	The unit has not reported in this IMPL. Its last known state was Synchronizing.
Last_Known_Suspended (43)	The unit has not reported in this IMPL. Its last known state was Suspended.

Multipath Indicates that the system has multipath connections to the disk unit. The following values are valid:

- No (0)- The system has only one connection to the disk unit.
- Yes (1)- The system has multipath connections to the disk unit.
- Unknown (-1)- An operating system level does not report multipath status unit.

Name The unique ten-character name for the unit that is assigned by the system.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Parity Indicates whether this unit is device parity protected. The following values are valid:

- No (0)- unit is not device parity protected
- Yes (1)- unit is device parity protected

Percent_Busy The approximate percentage of time that the disk unit is busy. Set to NA (-1) if the disk is not configured or its use cannot be determined. Valid values range from 0-100.

Percent_Used The percent of the capacity that is currently used. If the capacity is zero, this value is zero. Valid values range from 0-100.

Percent_Reserved The percent of the capacity that is reserved for use by the computer. This storage is not available for storing objects, redundancy data, and other internal computer data. This value is zero for non-configured units. Valid values range from 0-100.

Raid_Type The current type of RAID (device parity) array that this unit belongs to. The following values are valid:

- NA (0)- the unit is not in a parity set
- 5 - the unit belongs to a RAID 5 parity set
- 6 - the unit belongs to a RAID 6 parity set

Serial number The serial number of the device containing this auxiliary storage unit. This ten-character serial number field identifies the vital product data for the disk device.

Status The current status of the disk unit. The following values are valid:

-1	Not_configured	The disk is not in use by the system.
0	Unknown	The current status cannot be determined.
4096	Active	The array subsystem is active.
2048	Failed	This unit in an array subsystem has failed. Data protection for the subsystem is no longer in effect.
1024	Other_unit_failed.	This unit is operational, but another unit in the array subsystem has failed. Data protection for this subsystem is no longer in effect.
512	Degraded	The array subsystem is operational and data protection for this subsystem is in effect, but a failure that might affect performance has occurred. It must be fixed.
256	Hardware_failure	The array subsystem is operational and data protection for this subsystem is in effect, but hardware failure has occurred. It must be fixed.
128	Parity_rebuilt	The device parity protection for this device is being rebuilt following a repair action.
64	Not_ready	The unit is not ready for I/O operation.
32	Write_protected	The write operation is not allowed on the unit.
16	Busy	The unit is busy.
8	Not_operational	The unit being addressed is not operational. The status of the device is not known.
4	Unknown	The unit being addressed has an unexpected status. The unit is operational, but its status returned to Storage Management from the IOP is not one of those previously described.
2	Status_not_available	The computer is not able to communicate with I/O processor. The status of the device is not known.
1	Read-write_protected	The unit is in a read/write protected state. An array might be in the read/write protected state when there is a problem, such as a cache problem, configuration problem, or some other array problems that can create a data integrity exposure.

Unit model This four-byte character field from the vital product data for the disk device identifies the model of the drive.

Unit number System assigned number for the disk unit (units of a mirrored pair have the same unit number, while non-configured units have a unit number of zero).

Unit type This four-byte character field from the vital product data for the disk device identifies the type of drive.

I/O Processor attributes

The I/O Processor attribute group includes attributes that you can use to monitor how I/O is being used by the system, storage, and communications.

Comm Percent The percentage of the total IOP processor time that was used by communications tasks during the last monitor interval. This field only applies to communications and multifunction IOPs. Otherwise, it is set to 0. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Disk Percent The percentage of the total IOP processor time that was used by disk tasks during the last monitor interval. This percentage applies only to multifunction IOPs. Otherwise, it is set to 0. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

IOP Bus Address The IOP bus address. The valid value is an integer from 0 - 31. A value of -1 indicates NA.

IOP Bus Number The IOP bus number. The valid value is an integer from 0 - 255. A value of -1 indicates NA.

Name The system resource name associated with this IOP that controls the disk unit. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Type The type of IOP. The following values are valid:

*COMM	IOP is a communications IOP.
*DISK	IOP is a disk IOP.
*WKSTN	IOP is a local workstation IOP.
*MLTFUN	IOP is a multifunction IOP.

Utilization Percent The percentage of the total IOP processor time that the IOP was busy and not idle during the last monitor interval. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Integrated File System Object attributes

Use the i5/OS Integrated File System (IFS) Objects attributes to monitor the status of directories, files, and other objects in the Integrated File System. This attribute group can be used in historical collections, but is not collected by default.

Note: The i5/OS programming interfaces used to give these attributes only permit access to the IFS objects that the QAUTOMON user profile has authority to access. For example, if a root file system directory has PUBLIC *EXCLUDE access authority, then the directory's contents cannot be accessed. To remedy this situation give at least the *USE authority to the QAUTOMON user profile for IFS directories and objects, or add *ALLOBJ authority to the QAUTOMON user profile.

The group can monitor all file systems, other than QSYS.LIB, that support the IFS APIs and are thread-safe, including the following systems:

- ″Root″ (/)
- Open system (QpenSys)
- User-defined (UDFS)
- Optical (QOPT)
- NetClient (QNTC)
- i5/OS file server (QFileSvr.400)
- Network (NFS)

The following systems are not supported because they are not thread-safe and the IFS APIs do not allow program access to them:

- Document library services (QDLS)
- NetWare (QNetWare)

The QSYS.LIB file system is not supported by this attribute group since monitoring for those objects is provided in other attribute groups. For QSYS.LIB object monitoring use the Object and Database Member attribute groups.

T

Access An octal value that indicates the access permissions and privileges of the file. This attribute defines a four-digit octal number representing the access rights. Each digit is the decimal equivalent of a binary three-bit string. Valid entries are numbers in the range 0000 to 7777 (leading zeroes are not displayed). From left to right, each digit has the following meaning:

- 1st digit Determines whether, upon execution, the file takes on the ID of the user or group that owns the file. This permission assignment applies to users who neither own the file they are trying to run nor belong to the group that owns the file.
- 2nd digit Determines the access permissions of the user that owns the file.
- 3rd digit Determines the access permissions of the group that owns the file.
- 4th digit Determines the access permissions for other users.

From left to right, the bits for the first digit have the following meanings:

- 1st bit Set user ID on execution
- 2nd bit Set group ID on execution
- 3rd bit Restricted rename and unlink

From left to right, the bits for the second, third and fourth digits have the following meanings (a value of one means that access level is permitted):

- 1st bit Read access
- 2nd bit Write access
- 3rd bit Execute and search access

Allocated percent The percent of the allocated size of the objects that is used. Valid entries are numeric values with one decimal point in the range 0 to 100.

Group The object group. Valid entries are simple alphanumeric text strings with a maximum length 10 characters.

Last access The date and time that the object was last accessed.

Last change The date and time that the object was last changed.

Link name The name of the file for which this file is a symbolic link, or blank if the file is not a link (up to 768 bytes of the Unicode characters in the name). Valid entries are simple text strings, with a maximum length of 768 bytes. This attribute supports UTF-8 characters.

Links The number of links to the object, or 2,147,483,647 if the number is that size or greater. Valid entries are numeric values in the range 0 to 2,147,483,647.

Name The name of the object (up to 768 bytes of the Unicode characters in the name).

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Owner The object owner. Valid entries are simple alphanumeric text strings with a maximum length 10 characters.

Path The path for the object (up to 1536 bytes of the Unicode characters in the path). Valid entries are text strings with a maximum length of 768 bytes. This attribute supports UTF-8 characters.

Size The size of the object in bytes, or 2,147,483,647 if the file size is that size or greater.

Size (MB) The size of the object in Megabytes. Valid entries are numeric values with one decimal point in the range 0 to 214748364.7.

Type The i5/OS object type. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Job attributes

The Job attribute group includes attributes that you can use to monitor work management. You can collect performance data about started jobs, running jobs, and jobs that end during the monitor interval.

Note: Note that only active system request jobs, group jobs and disconnected jobs are monitored.

Acct Code The identifier assigned to the job by the system to collect resource use information for the job when job accounting is active. This attribute monitors in the operational areas of performance and work management. The valid value is an alphanumeric string with a maximum of 15 characters.

Acct Status The status of the job. A job displays only 1 status and the attribute can be used to monitor in the operational area of performance. The following values are valid:

Blank	A blank status field represents a job that is in transition or is not active.

BSCA	The job is waiting in a pool activity level for the completion of an I/O operation to a binary synchronous device.
BSCW	The job is waiting for the completion of an I/O operation to a binary synchronous device.
CMNA	The job is waiting in a pool activity level for the completion of an I/O operation to a communications device.
CMNW	The job is waiting for the completion of an I/O operation to a communications device.
CMTW	The job is waiting for the completion of save-while-active checkpoint processing in another job.
CPCW	The job is waiting for the completion of a CPI communications call.
DEQA	The job is waiting in the pool activity level for completion of a dequeue operation.
DEQW	The job is waiting for completion of a dequeue operation. For example, QSYSARB and subsystem monitors generally wait for work by waiting for a dequeue operation.
DKTA	The job is waiting in a pool activity level for the completion of an I/O operation to a diskette unit.
DKTW	The job is waiting for the completion of an I/O operation to a diskette unit.
DLYW	The job is delayed. The Delay Job (DLYJOB) command delays the job for a time interval to end, or for a specific delay end time. The function field shows either the number of seconds the job is to delay (999999), or the specific time when the job is to start running again.
DSC	The job is disconnected from a workstation display.
DSPA	The job is waiting in a pool activity level for input from a workstation display.
DSPW	Waiting for input from a workstation display.
END	The job has been ended with the *IMMED option, or its delay time has ended with the *CNTRLD option.
EOFA	Waiting in the activity level to try a read operation again on a database file after the end-of-file has been reached.
EOFW	Waiting to try a read operation again on a database file after the end-of-file has been reached.
EOJ	Ending for a reason other than running the End Job (ENDJOB) or End Subsystem (ENDSBS) command, such as SIGNOFF, End Group Job (ENDGRPJOB), or an exception that is not handled.
EVTW	Waiting for an event. For example, QLUS and SCPF generally wait for work by waiting for an event.
GRP	The job is suspended by a Transfer Group Job (TFRGRPJOB) command.
HLD	The job is held.
ICFA	The job is waiting in a pool activity level for the completion of an I/O operation to an intersystem communications function file.
ICFW	The job is waiting for the completion of an I/O operation to an intersystem communications function file.
INEL	The job is ineligible and not currently in the pool activity level.
LCKW	The job is waiting for a lock.
MLTA	The job is waiting in a pool activity level for the completion of an I/O operation to multiple files.

MLTW	The job is waiting for the completion of an I/O operation to multiple files.
MSGW	The job is waiting for a message from a message queue.
MXDW	The job is waiting for the completion of an I/O operation to a mixed device file.
OS/W	The job is waiting for the completion of an OSI Communications Subsystem/400 OSLISN, OSRACS, OSRACA, OSRCV, or OSRCVA operation.
PRTA	The job is waiting in a pool activity level for output to a printer to complete.
PRTW	The job is waiting for output to a printer to be completed.
PSRW	A prestart job waiting for a program start request.
RUN	The job is currently running in the pool activity level.
SRQ	The job is the suspended half of a system request job pair.
SVFA	The job is waiting in a pool activity level for completion of a save file operation.
SVFW	The job is waiting for completion of a save file operation.
TAPA	The job is waiting in a pool activity level for completion of an I/O operation to a tape unit.
TAPW	The job is waiting for completion of an I/O operation to a tape unit.
TIMA	The job is waiting in a pool activity level for a time interval to end.
TIMW	The job is waiting for a time interval to end.

Async I/O The rate of physical asynchronous database and nondatabase read and write operations per second during the last monitor interval. The valid value is an integer from 0 - 1000000. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

CPU Percent The percentage of the processing unit used by this job during the last monitor interval. This attribute monitors in the operational area of performance. The valid value is a decimal number from 0.0 - 100.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

CPU Time The processing time used by the job (in seconds). This attribute monitors in the operational area of performance. The valid value is a decimal number from 0.000 - 2147483647.000. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

CPU Time Overall The total processing unit time used by the job (in seconds), the total since the job started. This attribute monitors in the operational area of performance. The valid value is a decimal number from 0.000 - 2147483647.000. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

End Status Indicates whether the system issued a controlled cancellation. The attribute monitors in the operational area of work management. The following values are valid:

*ACTIVE	The system, subsystem, or job is not canceled.
*ENDING	The system, the subsystem in which the job is running, or the job itself is cancelled.
*INACTIVE	The job is not running.

Function Name The name of the function and additional information (as described in the function type field) about the function the job is currently performing. The program updates the information only when a command is processed. The valid value is an alphanumeric string with a maximum of 10 characters.

Function Type Indicates the type of function and whether the job is performing a high-level function. The following values are valid:

Blank	The system is not doing a logged function.
A - C	The command is running interactively, it is a batch stream, or it was rerequested from a system menu. Commands in CL programs or REXX™ procedures are not logged.
D	The job is processing a delay job command.
G	The Transfer Group Job (TRFGRPJOB) command suspended the job.
I	The job is rebuilding an index (access path). The Function Name field includes the group job name for the field.
L	The system logs history information in a database file. The Function Name filed includes the name of the file. QHST is the only log currently supported.
M	The job is a multiple requester terminal (MRT) job with the job type of BATCH and the subtype is MRT, or it is an interactive job attached to an MRT job if the job type is interactive.
N	The job is currently at a system menu. The Function Name field includes the name of the menu.
O	The job is a subsystem monitor that is performing I/O operations to a workstation. The Function Name field includes the name of the workstation device to which the subsystem is performing an I/O operation.
P	The job is running a program. The Function Name filed includes the name of the program.
R	The job is running a procedure. The Function Name field includes the name of the procedure.
*	This value does a special function. For this value, the Function Name field includes one of these values. • ADLACTJOB (Auxiliary storage is being allocated for the number of active jobs specified in the QADLACTJ system value, indicating that the system value for the initial number of active jobs is too low.) • ADLTOTJOB (Auxiliary storage is being allocated for the number of jobs specified in the QADLTOTJ system value.) • CMDENT (The command Entry display is being used.) • DIRSHD (Directory shadowing is occurring.) • DLTSPLF (The system is deleting a spooled file.) • DUMP (A dump is in process.) • JOBLOG (The system is producing a job log.) • Passthru (The job is a pass-through job.) • RCLSPLSTG (The empty spooled database members are being deleted.) • SPLCLNUP (The spool cleanup is in process.)

Job Queue The name of the job queue that the job is currently in, or that the job was in when it became active. The attribute monitors in the operational area of work management. The following values are valid:

- For jobs with a status of *JOBQ or *ACTIVE, an alphanumeric string with a maximum of 10 characters.
- For *OUTQ, the field is blank.

Job Queue Library The name of the library where the job queue is located. The attribute monitors in the operational area of work management. The valid value is an alphanumeric string with a maximum of 10 characters.

Job Queue Priority The scheduling priority of the job in the job queue. The attribute monitors in the operational area of work management. The following values are valid:

- For jobs with a status of *JOBQ or *ACTIVE, 0-9. (0 is the highest and 9 is the lowest.)
- For *OUTQ, the field is blank.

Message Queue The name of the message queue where the system sends a completion message when a batch job ends. This attribute monitors in the operational area of work management. The following values are valid:

- If the job has a submitter, an alphanumeric string with a maximum of 10 characters.
- If the job has no submitter, the field is blank.

Message Queue Library The name of the library that includes the message queue. The default is QSYS. The attribute monitors in the operational area of work management. The valid value is an alphanumeric string with a maximum of 10 characters.

Mode The mode name of the advanced program-to-program communications (APPC) device that started the job. The attribute monitors in the operational are of performance. The valid value is an alphanumeric string with a maximum of 8 characters.

Multiple Request Terminal Job The multiple requester terminal (MRT) active job flag. The attribute monitors in the operational area of performance. The following values are valid:

*YES	The active job is an MRT job.
*NO	The active job is not an MRT job.

Name The name of the job. The attribute monitors in the operational areas of performance and work management. The valid value is an alphanumeric string with a maximum of 10 characters.

- For interactive jobs, the system assigns the job the name of the workstation where the job started.
- For batch jobs, you specify the name in the command when you submit the job.

Number The system assigned to the job. The attribute monitors in the operational areas of performance and work management. The valid value is an alphanumeric string with a maximum of 6 characters.

If you substitute Number (OS400 Job) into a CL command that requires an alphanumeric or character parameter, enclose the job number in apostrophes. For example, use 000123 so that the CL command uses it as a character parameter.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Pool Indicates the pool in which the job ran or is running. The attribute monitors in the operational area of performance. The valid value is an alphanumeric string with a maximum of 2 characters.

Priority Indicates the run priority over other jobs. The attribute monitors in the operational area of performance. The valid value is an integer from 1 (highest priority) through 9 (lowest priority).

Response Time The average transaction time (or average response time of the job) during the last monitor interval. The attribute monitors in the operational area of performance. The valid value is a decimal number from 0.0 - 2147483647.0. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Response Time Overall The average response time (in seconds) for interactive jobs. The program calculates the value by dividing Transaction Time Overall by Transaction Count Overall. The attribute monitors in the operational area of performance. The valid value is an integer from 0.0 - 214748364.7. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Signed On User Indicates whether the job is to be treated like a user signed on to the system. The attribute monitors in the operational area of performance. The following values are valid:

*YES	The job must be treated like a signed-on user.
*NO	The job must not be treated like a signed-on user.

Start Date The date the job started. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Submit Date The date the job entered the system. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Submit Date and Time The date and time the job entered the system. The attribute monitors in the operational area of work management. The following values are valid:

- If the job was not in the job queue, this field is blank.
- If the job was in the job queue, a date and time in the format CYYMMDDHHmmSSmmm (For example, 0961002103000000 indicates a century bit of 0, date of October 2, 1996 and a time of 10:30:00:000.)

Submit Time The time the job entered the system. This attribute monitors in the operational area of work management. The valid value include:

- If the job was in the job queue, a time in the format HHMMSS (For example, 103000 is a time of 10:30:00 a.m.)
- If the job was not in the job queue, the field is blank.

Subsystem The name of the subsystem that can retrieve the job from the queue. The attribute monitors in the operational areas of work management and performance. The following values are valid:

- For a job with a status of *ACTIVE, an alphanumeric string with a maximum of 10 characters.
- For a job with a status of *OUTQ or *JOBQ, the field is blank.

Start Date and Time The date and time the job started. For batch jobs, this is the date and time the job left the queue and started running. This attribute monitors in the operational area of performance. The following values are valid:

- If the job became active, the date and time is in the format CYYMMDDHHmmSSmmm. (For example, 9610021030000000 indicates a century bit of 0, date of October 2, 1996 and time of 10:30:00:000.)
- If the job did not become active, the field is blank.

Start Time The time the job started. The attribute monitors in the operational area of performance. The following values are valid:

- If the job became active, the time is in the format HHMMSS. (For example, 10:30:00:000 indicates a time of 10:30:00:000.)
- If the job did not become active, the field is blank.

Subtype Indicates the subtype of the job. This attribute monitors in the operational area of performance. The following values are valid:

Blank	No special subtype.
*BCI	Immediate
*EVK	Evoke job
*PJ	Prestart job
*PDJ	Print driver job
*MRT	Multiple requester terminal (MRT) job
*ALTSPLUSR	Alternate spool user

Synch I/O The rate of physical synchronous database and nondatabase read and write operations per second during the last monitor interval. This attribute monitors in the operational area of performance. The valid value is an integer from 0 - 1000000. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

S36 Environment Indicates whether the job is a System/36™ environment job. This attribute monitors in the operational area of performance. The following values are valid:

*YES	The job is a System/36 environment job.
*NO	The job is not a System/36 environment job.

Time Active The amount of time (in seconds) that the job has been active, or zero if the job is not currently active. Valid entries are integers in the range 0-2147483647.

Time in System The amount of time (in seconds) that the job has been in the system. Valid entries are integers in the range 0-2147483647.

Timeslice The job time slice value (in seconds). This attribute monitors in the operational area of performance. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Transaction Count The number of transactions performed by the job during the last monitor interval. This attribute monitors in the operational area of performance. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Transaction Count Overall The total number of interactive transactions performed by the job since the start of the job. This attribute monitors in the operational area of performance. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Transaction Time The transaction time (in seconds) accrued during the last monitor interval. The attribute monitors in the operational area of performance. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Transaction Time Overall The total interactive job transaction time since the start of the job (in seconds). This attribute monitors in the operational area of performance. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Type Indicates the type of job or task. This attribute monitors in the operational areas of performance and work management. The following values are valid:

*ASJ	Autostart job
*BATCH	Batch job
Blank	No special type
*HLIC	Horizontal Licensed Internal Code (HLIC) (tasks only)
*INT	Interactive job
*SBS	Subsystem monitor job
*RDR	Spooled reader job
*SYSTEM	System job
*VLIC	Vertical Licensed Internal Code (VLIC) (tasks only)
*WRITER	Spooled writer job
*SCPF	Start-control-program-function (SCPF) system job

User The user of the job. The user name is the same as the user profile name and can come from several different sources depending on the type of job. The attribute monitors in the operational areas of performance and work management. The valid value is an alphanumeric string with a maximum of 10 characters.

Job Log attributes

Use the Job Log attribute group to monitor messages that are sent to active jobs. This attribute group can be used in historical collections but is not collected by default. The group contains sample attributes in the operational areas of work management and problem determination.

Date and time The date and time that the message arrived in the job log. The format is MM/DD/YY HH:mm:SS, where: MM = Month; DD = Day; YY = Year; HH = Hour; mm = Minute; SS = Second.

Job name The name of the job. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Job number The number of the job. Valid entries are alphanumeric strings with a maximum length of 6 characters.

Job user The user name of the job. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Library The name of the message file library. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Message file The name of the message file that contains the message. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Message ID The message identification code, or blank if this is message is immediate. Valid entries are alphanumeric strings with a maximum of seven characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Severity The severity level of the message. Valid entries are integers in the range 0 to 99.

Subsystem The name of the job subsystem. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Subsystem library The name of the library where the subsystem description is stored. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Text (Unicode) The text data with substitution text included. Valid entries are strings with a maximum of 768 characters. This attribute supports UTF-8 characters.

Type The type of message. Valid entries are simple numeric text strings with a maximum length of 2 characters. The following table lists the available types and their associated codes:

01	Completion
02	Diagnostic
04	Informational
05	Inquiry
06	Sender copy
08	Request
10	Request with prompting
14	Notify, exception already handled
15	Escape, exception already handled
16	Notify, exception not handled
17	Escape, exception not handled
21	Reply, not checked for validity
22	Reply, checked for validity
23	Reply, message default used
24	Reply, system default used
25	Reply, from system reply list
26	Reply, from exit program

Job Queue attributes

The Job Queue attribute group includes attributes that you can use to monitor the state of the job queue.

Library The name of the library that includes the job queue. The valid value is an alphanumeric string with a maximum of 10 characters.

Name The name of the job queue. The valid value is an alphanumeric string with a maximum of 10 characters.

Number Jobs The number of jobs in the queue. The valid value is an integer from 0-100000. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Status The status of the job queue. The following values are valid:

RELEASED	The job queue has been released.
HELD	The job queue is held.

Subsystem The name of the subsystem that can retrieve jobs from the queue. The attribute monitors in the operational areas of work management and performance.

The following values are valid: an alphanumeric name with a maximum of 10 characters; or all spaces if the subsystem is not assigned.

Line attributes

The Line Attribute Group includes attributes that you can use to monitor the performance and configuration of lines.

Category The category for the line description. The following values are valid:

- An alphanumeric string with a maximum of 10 characters
- *ASYNC
- *BSC
- *DDI
- *ELAN
- *ETH
- *FAX
- *FR
- *IDLC
- *NET
- *SDLC
- *TDLC
- *TRLAN
- *WLS
- *X25

Name The name or identifier that describes the line. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Status The status that indicates the status of the line. The following values are valid:

00	VARIED OFF
01	OPERATIONAL
02	AS/36_DISABLED
05	DEALLOCATED
06	UNPROTECTED
07	ALLOCATED
08	STAND-ALONE
10	VARY OFF PENDING
20	VARY ON PENDING
21	VARY_ON_PENDING/DETACHED

22	VARY_ON_PENDING/ALLOCATE
30	VARIED ON
31	VARIED_ON/ALLOCATE
32	VARY_ON_or_CNN_PENDING
33	AS/36_ENABLED
40	CONNECT PENDING
50	SIGNON DISPLAY
51	ACTIVE_or_CNN_PENDING
60	ACTIVE
61	ACTIVE/DETACHED
62	ACTIVE/SOURCE
63	ACTIVE READER
64	ACTIVE/TARGET
65	ACTIVE/ALLOCATE
66	ACTIVE WRITER
67	AVAILABLE
70	HELD
71	HELD/DETACHED
72	HELD/SOURCE
73	HELD/TARGET
74	HELD/ALLOCATE
75	POWERED OFF
80	RCYPND
81	RCYPND/DETACHED
82	RCYPND/SOURCE
83	RCYPND/TARGET
84	RCYPND/ALLOCATE
90	RCYCNL
91	RCYCNL/DETACHED
92	RCYCNL/SOURCE
93	RCYCNL/TARGET
94	RCYCNL/ALLOCATE
95	SYSTEM_REQUEST
96	REBUILD
100	FAILED
101	FAILED/DETACHED
102	FAILED/SOURCE
103	FAILED READER
104	FAILED/TARGET
105	FAILED/ALLOCATE
106	FAILED WRITER
107	SHUTDOWN

110	DIAGNOSTIC MODE
111	DAMAGED
112	LOCKED
113	UNKNOWN
114	DEGRADED
200	INVALID_STATUS

Management Central Events attributes

Use the Management Central Events attribute group to monitor for events that are sent by the System i Navigator, Management Central monitoring functions. This attribute group can be used in historical collections but is not collected by default. The Management Central Events attributes are notification attributes in the operational areas of performance, work management, and problem analysis.

Event source The name of the event. Valid entries are simple alphanumeric text strings with a maximum length of 512 characters. This field supports UTF-8 characters.

Event time The system date and time that the event was created.

Event type The source type of the event. Valid entries are simple alphanumeric text strings with a maximum length of 2 characters, and include 01 for a triggered event, 02 for a reset event (automated reset), and 03 for a manual reset event.

File change time The date and time that the status of the monitored file changed (expressed in the format CYYMMDDHHMMSS).

File name The full path name (up to 256 characters) of the file being monitored. Valid entries are simple alphanumeric text strings with a maximum length of 512 characters. This field supports UTF-8 characters.

From job name The name of the job from which the message was sent that caused the event. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

From job number The number of the job from which the message was sent that caused the event. Valid entries are simple alphanumeric text strings with a maximum length of 6 characters.

From job user The user of the job from which the message was sent that caused the event. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Job name The name of the job that caused the event. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Job number The number of the job that caused the event. Valid entries are simple alphanumeric text strings with a maximum length of 6 characters.

Job user The user of the job that caused the event. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Job status The actual status of the job that caused the event to be created. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Message ID The message identification code. Valid entries are simple alphanumeric text strings with a maximum length of 7 characters.

Message queue The name of the message queue being monitored. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Message severity The message severity level. Valid entries are numeric values in the range 0 to 99, or -1. Because you can monitor for message severity level of 0 (zero), when this format represents a manual reset event, this field contains the default value of -1.

Message type The type of message. Valid entries are simple alphanumeric text strings with a maximum length of 2 characters. The following table lists the available types and their associated codes:

01	Completion
02	Diagnostic
04	Informational
05	Inquiry
06	Sender copy
08	Request
10	Request with prompting
14	Notify, exception already handled
15	Escape, exception already handled
16	Notify, exception not handled
17	Escape, exception not handled
21	Reply, not checked for validity
22	Reply, checked for validity
23	Reply, message default used
24	Reply, system default used
25	Reply, from system reply list
26	Reply, from exit program

Metric The name of the metric that caused the event to be created. Valid entries are numeric values in the range 0 to 2147483647. A value of -1 indicates NA. The following table lists metric types and their associated codes:

00	CPU Utilization Percent Busy (Average)
01	CPU Utilization Percent Busy (Interactive)
02	Interactive Response Time in Seconds (Average)
03	Interactive Response Time in Seconds (Maximum)
04	Transaction Rate per Second (Average)
05	Transaction Rate per Second (Interactive)
06	Batch Logical Database I/O per Second

07	Disk Arm Utilization Percent Busy (Average)
08	Disk Arm Utilization Percent Busy (Maximum)
09	Disk Storage Percent Full (Average)
10	Disk Storage Percent Full (Maximum)
11	Disk IOP Utilization Percent Busy (Average)
12	Disk IOP Utilization Percent Busy (Maximum)
13	Communications IOP Utilization Percent Busy (Average)
14	Communications IOP Utilization Percent Busy (Maximum)
15	CPU Utilization Basic Percent Busy (Average)
16	Machine Pool Faults per Second
17	User Pool Faults per Second (Average)
18	User Pool Faults per Second (Maximum)
19	Communications Line Utilization Percent Busy (Average)
20	Communications Line Utilization Percent Busy (Maximum)
21	LAN Utilization Percent Busy (Average)
22	LAN Utilization Percent Busy (Maximum)
23	CPU Utilization Percent Busy (Interactive Feature)
1010	Job CPU Utilization Percent Busy
1020	Job Logical I/O Rate per Second
1030	Job Disk I/O Rate per Second
1040	Job Communications I/O Rate per Second
1050	Job Transaction Rate per Second
1060	Job Transaction Time in Milliseconds
1070	Job Thread Count
1080	Page Fault Rate per Second
2010	Summary CPU Utilization Percent Busy
2020	Summary Logical I/O Rate per Second
2030	Summary Disk I/O Rate per Second
2040	Summary Communications I/O Rate per Second
2050	Summary Transaction Rate per Second
2060	Summary Transaction Time in Milliseconds
2070	Summary Thread Count
2080	Summary Page Fault Rate per Second
4010	Summary Job Count

Metric value The actual value of the metric when the event was created.

Monitor type The type of the Management Central monitor. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters. The following values are enumerated:

- MCES0100: System monitor numeric
- MCEJ0100: Job monitor numeric
- MCEJ0200: Job monitor message

- MCEJ0300: Job monitor status
- MCEG0100: Message Queue monitor
- MCEF0100: File monitor file size
- MCEF0200: File monitor status
- MCEF0300: File monitor text
- MCET0100: B2B Activity monitor

MSGQ library The library of the message queue being monitored.

Operator The operator used on the trigger or reset value (*GE is greater than or equal; *LE is less than or equal; *EQ is equal).

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Owner The owner of the system or job event. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Sending system The name of the endpoint system for which the event was created. Valid entries are simple alphanumeric text strings with a maximum length of 512 characters. This field supports UTF-8 characters.

Trigger The value that triggers or resets the metric. Valid entries are numeric values in the range 0 to 2147483647.

User The user profile that caused the event to occur. On trigger and automated reset events, this profile is the owner of the job monitor. On manual reset events, this profile is the user ID that requested the manual reset. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters.

Messages attributes

The Messages attribute group includes attributes that you can use to monitor i5/OS messages. These attributes refer to message queues.

- If you do not specify a value for the Message Queue attribute, it takes the default, QSYSOPR.
- If you do not specify a value for the Message Queue Library attribute, it takes the default, QSYS.

Only one Message Queue and one Message Queue Library can be specified on a query or situation. These attributes are in the operational area of work management. However, depending on the message they receive, they can have an impact on operational areas other than work management.

Alert option Indicates whether and when an SNA alert is created and sent for the message. Valid entries are simple alphanumeric text strings with a maximum length of 10 characters. The following table shows some valid values and their descriptions:

DEFER	An alert is sent after local problem analysis.
*IMMED	An alert is sent immediately when the message is sent to a message queue that has the allow alerts attribute set to *YES.
*NO	No alert is sent.
*UNATTEND	An alert is sent immediately when the system is running in unattended mode (when the value of the alert status network attribute, ALRSTS, is *UNATTEND).

Data The message help with substitution text. The text of a predefined message with the message data included. If an immediate message is listed, this field includes the immediate message text. The valid value is an alphanumeric string with a maximum of 255 characters.

Data (Unicode) The message help with substitution text. The text of a predefined message with the message data included. If an immediate message is listed, this field includes the immediate message text. The valid value is a string with a maximum of 765 bytes.

Date The date the message arrived in the message queue. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Date and Time The date and time the message arrived in the message queue. When using the attribute, the event data is returned for all messages that satisfy the situation definition including those messages that arrived prior to when the monitoring for the situation. The valid value is a date and time in the format CYYMMDDHHmmSSmmm; for example, 096100210300000.

Help Data The message help with the substitution text (The message help for the message is listed, including the message data. If an immediate message is listed, this field includes blanks.) The valid value is an alphanumeric string with a maximum of 255 characters.

Help Data (Unicode) The message help with the substitution text. (The message help for the message is listed, including the message data. If an immediate message is listed, this field includes blanks.) The valid value is a string with a maximum of 765 bytes.

ID The identifying code of the message received. If an immediate message is received, this field is blank. The valid value is an alphanumeric string with a maximum of 7 characters.

Key The key to the message received. The message key is a unique string of characters that identifies a particular instance of a message in a queue. The key is assigned by the command or attribute that sends the message. If the message-action parameter specifies *REMOVE, this field is blank. The valid value is a hexadecimal number.

Message Queue The name of the message queue. You cannot monitor the QHST message queue. QSYSOPR is the default. The valid value is an alphanumeric string with a maximum of 10 characters.

Message Queue Library The name of the library that includes the message queue. The default is QSYS. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Select Filters by specifying the criteria for the type of message listed. The attribute allows you to do early filtering by specifying selection criteria for which types of messages are listed. Failing to specify this attribute might overload IBM Tivoli Monitoring for i5/OS and the situation does not evaluate. If this is the case, you are notified by a message in the IBM Tivoli Monitoring for i5/OS log that the situation did not evaluate. To view the message log, use the DSPOMALOG command.

The Select attribute input on a query or situation is used as the Select value returned for all messages, regardless of the type of message found. For example, if '*ALL' is used on a query to select all types of messages, then '*ALL' displays in the Select column for all the message found, even if the message requires a reply or had a problem analysis run.

The following values are valid:

*ALL	Displays all messages (default value).
*MNNR	Displays messages that do not require a reply are listed (This includes informational, completion, diagnostic, request notify, escape, reply, answered inquiry, and answered copy messages of sender.)
*MNR	Displays messages that need a reply (This includes unanswered inquiry messages.)
*PAR	Displays messages that have had a problem analysis run
*SCNR	Displays copy messages of sender that require a reply (This includes only unanswered copy messages.)

Send Job Name The name of the job that sent the message. The valid value is an alphanumeric string with a maximum of 10 characters.

Send Job Number The number of the job that sent the message. The valid value is an alphanumeric string with a maximum of 6 characters.

Send User The name of the user profile of the job that sent the message being received. The valid value is an alphanumeric string with a maximum of 10 characters.

Severity The severity level of the message received. The higher the number, the more severe the message. The valid value is an integer from 0 - 99.

Time The time the message arrived in the message queue. (Messages that are received before the situation starts are not returned.) The valid value is a time in the format HHMMSS. (For example, 103000 indicates a time of 10:30:00 a.m.)

Type Indicates or identifies the type of message received. The following values are valid:

01	Completion
02	Diagnostic
04	Informational
05	Inquiry
06	Sender copy
08	Request
10	Request with prompting
14	Notify
15	Escape
21	Reply, not validity checked
22	Reply, validity checked
23	Reply, message default used
24	Reply, system default used
25	Reply, from system reply list

Miscellaneous attributes

The Miscellaneous attribute group contains various items required by other Tivoli products. They include system hardware and i5/OS information.

Brand The IBM system brand of the hardware on which the agent is running. Values are one character in length and can be the following:

i	System i
p	System p™

Host Name The fully qualified host name. Valid values are 256 alphanumeric characters in length.

Manufacturer The name of the manufacturer for the hardware system. Values are ten alphanumeric characters in length.

Model-Feature The model and processor feature codes of the hardware system. Valid entries are nine alphanumeric characters in length in the format MMMM-FFFF where MMMM is the model and FFFF is the feature code.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

OS The operating system name. Valid values are eight alphanumeric characters and can be the following:

OS/400	OS/400 operating system

i5/OS	i5/OS operating system

Processor Speed The speed of the processors in megahertz (MHz), or -1 if the speed cannot be determined. Valid values are integers, and -1 is enumerated as ' Unknown'.

Processors The number of processors installed on the physical machine. If the physical machine has the on-demand processors feature installed, then the number of installed processors equals the number of permanently activated processors plus the number of temporarily activated processors plus the number of processors which are not activated. Valid values are integers.

VRM The version, release, and modification level of the operating system. Valid values are six alphanumeric characters in the format VxRyMz where x is the version, y is the release, and z is the modification level. Examples are V5R4M0 and V5R3M5.

NetServer attributes

The NetServer attribute group includes attributes that you can use to monitor the NetServer support for Microsoft Neighborhood (for example, server sessions, traffic, users, printing, response time, and so on).

Auto disconnects The number of server sessions that were disconnected automatically. Valid entries are integers in the range 0 to 2147483647.

Bytes received The number of server megabytes that were received from the network. Valid entries are integers in the range 0 to 2147483647.

Bytes sent The number of server megabytes that were sent to the network. Valid entries are integers in the range 0 to 2147483647.

Disconnects The number of server sessions that were disconnected normally or ended in error. Valid entries are integers in the range 0 to 2147483647.

File opens The number of file opens for the whole server. Valid entries are integers in the range 0 to 2147483647.

Guest support Indicates whether a guest user profile can be used if an unknown user attempts to access resources on the system. Specify either 1 for `Yes` or zero for `No`.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Password violations The number of server password violations. Valid entries are integers in the range 0 to 2147483647.

Print jobs The number of server print jobs that were spooled. Valid entries are integers in the range 0 to 2147483647.

Reset The system date and time that the server statistics were reset. The format is MM/DD/YY HH:mm:SS, where: MM = Month; DD = Day; YY = Year; HH = Hour; mm = Minute; SS = Second.

Response time The average server response time in milliseconds. Valid entries are integers in the range 0 to 2147483647.

Session starts The number of server session starts. Valid entries are integers in the range 0 to 2147483647.

Started The system date and time that the server was started.

Unknown users The number of unknown users who requested sessions to the server. Valid entries are integers in the range 0 to 2147483647.

Network attributes

Use the Network attribute group to monitor the network attributes set for the system. You can use the i5/OS Display Network Attributes (DSPNETA) command to view the network attributes.

Add to cluster Indicates whether this system can allow another system to add it as a node in a cluster.

Addition resistance The Advanced Peer-to-Peer Networking® (APPN) function routes addition resistance for an APPN *NETNODE or *BEXNODE node type.

Alert Backup Focal Point Identifies the system that provides alert focal-point services if the local system is unavailable and ALRPRIFP is *YES. The backup focal point is only used by systems in the primary sphere of control. The following values are valid:

- An alphanumeric string with a maximum of 16 characters (The first 8 characters are the control point name and the last 8 characters are the network ID.)
- *NONE (indicates no backup focal point is defined)

Alert Controller The name of the controller to be used for alerts in a system service control point-physical unit (SSCP-PU) session. The controller is ignored if the system has a focal point, the node is in the control of another system. The following values are valid:

- an alphanumeric string with a maximum of 10 characters
- *NONE (indicates that no alert controller is defined)

Alert Default Focal Point Specifies whether the system is an alert default focal point. The valid value is an alphanumeric string with a maximum of 10 characters.

Alert Filter The name of the filter object that is used by the alert manager when processing alerts. The following values are valid:

- an alphanumeric string with a maximum 20 characters (The first 10 characters are the filter name, and the last 10 characters are the library name.)
- *NONE (indicates that no alert filter is being used)

Alert Hold Count The maximum number of alerts to be created before the alerts are sent over the system service control point-physical unit (SSCP-PU) session. The system holds alerts until the number of alerts is created. If the Alert Controller (ALTCTLD) attribute is used to send alerts using the SSCP-PU session, alerts are sent automatically, regardless of the ALRHDCNT attribute, when a switched connection is made for other reasons. The following values are valid:

- *NOMAX (-2)
- an integer from 0 - 32767

Alert Log Status Indicates which alerts are to be logged. The following values are valid:

*ALL	Locally created alerts and incoming alerts are logged.
*LOCAL	Only locally created alerts are logged.
*NONE	No alerts are logged.
*RCV	Only alerts received from other nodes are logged.

Alert Primary Focal Point Specifies whether the system is an alert primary focal point. The following values are valid:

*YES	The network is an alert primary focal point.
*NO	The network is not an alert primary focal point.

Alert Request Focal Point Specifies the name of the system that is requested to provide focal point services. If a focal point is already defined for the entry point, it is taken away when the new focal point is requested. The following values are valid:

- An alphanumeric string with a maximum of 16 characters
- *NONE (indicates no focal point is requested)

Alert Status Indicates how the alerts are created. The following values are valid:

*OFF	Alerts are not created by the system.
*ON	Alerts are created by a system for all changeable conditions except unattended conditions.
*UNATTEND	Alerts are created by the system for all alert conditions including those that have the alert indicator in the message description set to *UNATTEND.

Allow AnyNet® Indicates whether this system allows AnyNet support.

Allow HPR tower Indicates whether this system allows the HPR transport tower support to be used with APPN session traffic.

Allow virtual APPN Indicates whether this system allows APPC sessions and devices to use virtual APPN controllers.

APPN Node Type The type of advanced peer-to-peer networking (APPN) node. The following values are valid:

*ENDNODE	The node does not provide network services to other nodes, but it might participate in the APPN network by using the services of an attached network server, or it might operate in a peer environment similar to migration end nodes.
*NETNODE	The node provides intermediate routing, route selection services, and distributed directory services for local users and to the end nodes and migration end nodes that it serves.

Autocreate limit The maximum number of devices that can be created automatically on virtual controllers.

Client access The way in which the system processes Client Access requests from other systems.

Current System Name The name of the system that is currently being used. The valid value is an alphanumeric string with a maximum of 8 characters.

Data compression Indicates whether data compression is used when the system is an SNA end node.

DDM request access Indicates how the system processes distributed data management (DDM) and Distributed Relational Database Architecture™ (DRDA®) requests from other systems.

Default Local Location Name The name of the default local location for the system. The valid value is an alphanumeric string with a maximum of 8 characters.

Default Mode The name of the default mode for the system. The valid value is an alphanumeric string with a maximum of 8 characters.

HPR path switch timers Four 10-character settings for the amount of time, in minutes, to allow for a path switch attempt of a Rapid Transport Protocol (RTP) connection.

Job action The action that is taken for any input stream that the system receives through the SNA distribution services (SNADS) network.

Intermediate data compression The level of data compression to request when this server is an SNA intermediate node.

Local CPNAME The name of the local control point for the system. The valid value is an alphanumeric string with a maximum of 8 characters.

Local NETID The ID assigned to the local network for the system. The valid value is an alphanumeric string with a maximum of 8 characters.

Max hop count The maximum number of times in an SNA distribution services (SNADS) network that a distribution queue entry that originates at this node can be received and routed on the path to its final destination.

Max Intermediate Sessions The maximum number of advanced program-to-program communications (APPC) intermediate sessions for an Advanced Peer-to-Peer Networking (APPN) node type of *NETNODE. The valid value is an integer from 0 - 10000.

Message Queue The name of the message queue used for messages received through the SNA distribution services (SNADS) network sent for users who have no message queue specified in their user profile, or users whose message queue is not available. The valid value is an alphanumeric string with a maximum of 20 characters. (The first 10 characters are the message queue name, and the last 10 characters are the library name.)

Modem country ID The country or region-specific default characteristics for modems that are internal to I/O adapters.

Network server domain The LAN server domain to which all Integrated Servers (also known as file server I/O processors or FSIOP) on the system belong.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Output Queue The name of the output queue used for spooled files received through the SNA distribution services (SNADS) network sent for users whose output queue is not available. The valid value is an alphanumeric string with a maximum of 20 characters. (The first 10 characters are the output queue name and the last 10 characters are the library name.)

Pending System Name If a change is pending, this identifies the pending system. A blank indicates that no change is pending. The valid value is an alphanumeric string with a maximum of 8 characters.

Server network ID The network node server of an Advanced Peer-to-Peer Networking (APPN) network (up to a maximum of five) for an APPN node type of *ENDNODE.

Network Interface attributes

Use the Network Interface attributes to monitor the status and details for network interfaces. Network Interface attributes are sampled attributes in the operational areas of communications and configuration.

Category The network interface category. This alphanumeric string is up to 12 characters long. It is one of the following values:

- *ATM
- *FR
- *ISDN
- *T1

Name The name of the network interface description. This alphanumeric string is up to 12 characters long.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Status Indicates the state or condition (status) of a controller. The following values are valid:

00	VARIED OFF
01	OPERATIONAL
02	AS/36_DISABLED
05	DEALLOCATED
06	UNPROTECTED
07	ALLOCATED
08	STAND-ALONE
10	VARY OFF PENDING
20	VARY ON PENDING
21	VARY_ON_PENDING/DETACHED
22	VARY_ON_PENDING/ALLOCATE
30	VARIED ON
31	VARIED_ON/ALLOCATE
32	VARY_ON_or_CNN_PENDING
33	AS/36_ENABLED
40	CONNECT PENDING
50	SIGNON DISPLAY
51	ACTIVE_or_CNN_PENDING
60	ACTIVE
61	ACTIVE/DETACHED
62	ACTIVE/SOURCE
63	ACTIVE READER
64	ACTIVE/TARGET
65	ACTIVE/ALLOCATE
66	ACTIVE WRITER
67	AVAILABLE
70	HELD
71	HELD/DETACHED
72	HELD/SOURCE
73	HELD/TARGET
74	HELD/ALLOCATE
75	POWERED OFF
80	RCYPND
81	RCYPND/DETACHED
82	RCYPND/SOURCE
83	RCYPND/TARGET

84	RCYPND/ALLOCATE
90	RCYCNL
91	RCYCNL/DETACHED
92	RCYCNL/SOURCE
93	RCYCNL/TARGET
94	RCYCNL/ALLOCATE
95	SYSTEM_REQUEST
96	REBUILD
100	FAILED
101	FAILED/DETACHED
102	FAILED/SOURCE
103	FAILED READER
104	FAILED/TARGET
105	FAILED/ALLOCATE
106	FAILED WRITER
107	SHUTDOWN
110	DIAGNOSTIC MODE
111	DAMAGED
112	LOCKED
113	UNKNOWN
114	DEGRADED
200	INVALID_STATUS

Network Server attributes

Use the Network Server attributes to monitor the status and details for network servers. Network Server attributes are sampled attributes in the operational areas of communications and configuration.

Category The network server category. This alphanumeric string is up to 12 characters long. It is one of the following values:

- *AIX
- *BASE
- *GUEST
- *ISCSI
- *IXSVR
- *LANSERVER
- *NETWARE
- *WINDOWSNT

Name The name of the network server description. This alphanumeric string is up to 12 characters long.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Status The current status of the network interface. The following table lists the valid values:

00	VARIED OFF
01	OPERATIONAL
02	AS/36_DISABLED
05	DEALLOCATED
06	UNPROTECTED
07	ALLOCATED
08	STAND-ALONE
10	VARY OFF PENDING
20	VARY ON PENDING
21	VARY_ON_PENDING/DETACHED
22	VARY_ON_PENDING/ALLOCATE
30	VARIED ON
31	VARIED_ON/ALLOCATE
32	VARY_ON_or_CNN_PENDING
33	AS/36_ENABLED
40	CONNECT PENDING
50	SIGNON DISPLAY
51	ACTIVE_or_CNN_PENDING
60	ACTIVE
61	ACTIVE/DETACHED
62	ACTIVE/SOURCE
63	ACTIVE READER
64	ACTIVE/TARGET
65	ACTIVE/ALLOCATE
66	ACTIVE WRITER
67	AVAILABLE
70	HELD
71	HELD/DETACHED
72	HELD/SOURCE
73	HELD/TARGET
74	HELD/ALLOCATE
75	POWERED OFF
80	RCYPND
81	RCYPND/DETACHED
82	RCYPND/SOURCE
83	RCYPND/TARGET

84	RCYPND/ALLOCATE
90	RCYCNL
91	RCYCNL/DETACHED
92	RCYCNL/SOURCE
93	RCYCNL/TARGET
94	RCYCNL/ALLOCATE
95	SYSTEM_REQUEST
96	REBUILD
100	FAILED
101	FAILED/DETACHED
102	FAILED/SOURCE
103	FAILED READER
104	FAILED/TARGET
105	FAILED/ALLOCATE
106	FAILED WRITER
107	SHUTDOWN
110	DIAGNOSTIC MODE
111	DAMAGED
112	LOCKED
113	UNKNOWN
114	DEGRADED
200	INVALID_STATUS

Object attributes

Use the Object attribute group to monitor storage and usage information for native i5/OS objects located in the QSYS.LIB file system.

Coding specific compare values for Name, Type, and Library reduces the amount of data the product has to handle, which improves performance. Failing to specify one or more of these attributes overloads the product, which might cause situations not to be evaluated. If this happens, a message in the log notifies you that the situation did not evaluate. You can view the log using the DSPOMALOG command.

Change Date The date the object was last changed. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Change Date and Time The date and time the object was last changed. The valid value is a date and time in the format CYYMMDDHHmmSSmmm. For example, 096100210300000 indicates a century bit of 0, a date of October 2, 1996, and a time of 10:30:00:000.

Change Time The time the object was last changed. The valid value is a time in the format HHMMSS. For example, 103000 indicates a time of 10:30:00 a.m.

Compress Status Indicates whether the object is compressed. The following values are valid:

Y	The object is compressed.
N	The object is decompressed permanently and can be compressed.
X	The object is decompressed permanently and cannot be compressed.
T	The object is temporarily decompressed.
F	The compression status cannot be determined (storage freed when saved).

Create Date The date the object was created. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Create Date and Time The date and time the object was created. The valid value is a date and time in the format CYYMMDDHHmmSSmmm. For example, 0961002103000000 indicates a century bit of 0, a date of October 2, 1996, and a time of 10:30:00:000.

Create Time The time the object was created. The valid value is a time in the format HHMMSS. For example, 103000 indicates a time of 10:30:00 a.m.

Extended Attribute The extended attribute for the object such as the program or file type that further describes the object. For example, an object type of *PGM might have a value of RPG (RPG program) or CLP (CL program), and an object type of *FILE might have a value of PF (physical file), LF (logical file), DSPF (display file), or SAVF (save file). The valid value is an alphanumeric string with a maximum of 10 characters long.

Last Used Date The date the object was last used. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Last Used Date and Time The date the object was last used, with the time (HHMMSS) set to 0. If the object has no last used date, the field is blank. The valid value is a date and time in the format CYYMMDDHHmmSSmmm. For example, 0961002103000000 indicates a century bit of 0, a date of October 2, 1996, and a time of 10:30:00:000.

Last Used Time The time the object was last used. The valid value is a time in the format HHMMSS. For example, 1030000 indicates a time of 10:30:00 a.m.

Library The name of the library containing the object. The valid value is an alphanumeric string with a maximum of 10 characters.

Licensed Program If the object is part of a licensed program, the name, release level, and modification level of the licensed program. (The field is blank if the retrieved object is not part of a licensed program.) The valid value has the following format.

- The 7 character name starts in character position 1.
- The version number starts in position 8.
- The release level starts in position 11.
- The modification level starts in position 14.

Name The name of the object. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Owner The name of the user profile that owns the object. The valid value is an alphanumeric string with a maximum of 10 characters.

Percent Days Used The percentage of days that the object was actually used since the days-used count was last reset to 0. The valid value is an integer from 0 - 100. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

PTF Number The number of the program temporary fix (PTF) that caused this object to be replaced. This field is blank if the object was not changed because of a PTF. The valid value is an alphanumeric string with a maximum of 10 characters.

Operating System Level The level of the operating system when the object was created. The valid value is in the format VvvRrrMmm. (The V is followed by a 2-character version number, the R is followed by a 2-character release level, and the M is followed by a 2-character modification level.)

Restore Date The date the object was restored. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Restore Date and Time The date and time when the object was restored. If the object has never been restored, the field is blank. The valid value is a date and time in the format CYYMMDDHHmmSSmmm. For example, 0961002103000000 indicates a century bit of 0, a date of October 2, 1996, and a time of 10:30:000.

Restore Time The time the object was restored. If the object has never been restored, the field is blank. The valid value is a time in the format HHMMSS. For example, 103000 indicates a time of 10:30:00 a.m.

Save Command The command used to save the object. The field is blank if the object was not saved. The valid value is an alphanumeric string with a maximum of 10 characters.

Save Date The date the object was last saved. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Save Date and Time The date and time when the object was last saved. If the object has never been saved, the field is blank. The valid value is a date and time in the format CYYMMDDHHmmSSmmm. For example, 0961002103000000 indicates a century bit of 0, a date of October 2, 1996, and a time of 10:30:00:000.

Save Device Type The type of device to which the object was last saved. The following values are valid:

Blank	The object was not saved.
*SAVF	The object was saved to a save file.
*DKT	The object was saved to a diskette.
*TAP	The object was saved to a tape.

Save File If the object was saved to a save file, the name of the save file. The field is blank if the object was not saved to a save file. The valid value is an alphanumeric string with a maximum of 10 characters.

Save Library If the object was not saved to the save file, the name of the library that includes the save file. The field is blank if the object was not saved. The valid value is an alphanumeric string with a maximum of 10 characters.

Save Time The time the object was last saved. If the object has never been saved, the field is blank. The valid value is a rime in the format HHMMSS. For example, 103000 indicates a time of 10:30:00 a.m.

Size (MB) The size of the object in Megabytes.

True Size The approximate size of the object. If the object is smaller than 1,000,000,000 bytes, the value is exact. The value is within 1024 larger than the actual size if the object is larger than 1,000,000,000 bytes. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Type The type of the object. The following values are valid:

*ALRTBL	Alert table
*AUTL	Authorization list
*BNDDIR	Binding directory
*CFGL	Configuration list
*CHTFMT	Chart format
*CLD	C description
*CLS	Class
*CMD	Command
*CNNL	Connection list
*COSD	Class-of-service description
*CSI	Communications Side Information
*CSPMAP	Cross System Product map
*CSPTBL	Cross System Product table
*CTLD	Controller description
*DEVD	Device description
*DOC	Document
*DTAARA	Data area
*DTADCT	Data dictionary
*DTAQ	Data queue
*EDTD	Edit description
*FCT	Forms control table
*FILE	File
*FLR	Folder
*FNTRSC	Font resources
*FORMDF	Form definition

*FTR	Filter
*GSS	Graphics symbol set
*IGCDCT	Double-byte character set (DBCS) conversion dictionary
*IGCSRT	Double-byte character set (DBCS) sort table
*IGCTBL	Double-byte character set (DBCS) font table
*JOBD	Job description
*JOBQ	Job queue
*JOBSCD	Job schedule
*JRN	Journal
*JRNRCV	Journal receiver
*LIB	Library
*LIND	Line description
*MENU	Menu description
*MODD	Mode description
*MODULE	Compiler unit
*MSGF	Message File
*MSGQ	Message Queue
*NODL	Node list
*NWID	Network interface description
*OUTQ	Output queue
*OVL	Overlay
*PAGDFN	Page definition
*PAGSEG	Page segment
*PDG	Print Descriptor Group
*PGM	Program
*PNLGRP	Panel group definition
*PRDAVL	Product availability
*PRDDFN	Product definition
*PRDLOD	Product load
*QMFORM	Query management form
*QMQRY	Query management query
*QRYDFN	Query definition
*RCT	Reference code translation table
*SBSD	Subsystem description
*SCHIDX	Information search index
*SPADCT	Spelling aid dictionary
*SQLPKG	Structured Query Language package
*SSND	Session description
*S36	System/36 computer description
*TBL	Table
*USRIDX	User index
*USRPRF	User profile

*USRQ	User queue
*USRSPC	User space
*WSCST	Workstation customizing object

Use Reset Date The date when the days-used count was last reset to 0. The valid value is a date in the format YYMMDD (for example, 080117 indicates January 17, 2008.)

Use Reset Date and Time The date and time the days-used count was last reset to 0. If the days-used count was not reset, the date and time is blank. The valid value is a date and time in the format CYYMMDDHHmmSSmmm. For example, 0961002103000000 indicates a century bit of 0, a date of October 2, 1996, and a time of 10:30:00:000.

Use Reset Time The time when the days-used count was last reset to 0. If the days-used count was not reset, the time is blank. The valid value is a time in the format HHMMSS. For example, 103000 indicates a time of 10:30:000 a.m.

Output Queue attributes

Use the Output Queue attributes to monitor the status, configuration, and contents of output queues. The i5/OS Output Queue attributes are sampled attributes in the operational areas of configuration, output, and work management.

Note: The i5/OS programming interfaces used to receive these attributes only permit access to the output queues that the QAUTOMON user profile has authority to access. If the library that contains an output queue does not allow access to QAUTOMON (PUBLIC authority is *EXCLUDE) then that output queue will not have information returned to it. To avoid this situation give at least *USE authority for user profile QAUTOMON for the library containing the output queue. Since the QAUTOMON profile has *SPLCTL special authority, it has the authority to access the output queue itself once it has authority to access the containing library. Output queues shipped with i5/OS will not cause this situation, but those created by product installations or user action might.

Authority The type of authorities to the output queue that you can use to control all the files on the queue, including: *OWNER for queue owner or *DTAAUT for any user with *READ, *ADD, or *DELETE authority.

Autostart The number of printer writers that autostart to this output queue when the system is restarted. Valid entries are integers.

Connection The type of network connection to the remote system, or *NONE if no remote connection exists. The following table shows valid entries:

0	*NONE	
1	*SNA	SNADS network is used as the connectivity to the remote system.
2	*IP	TCP/IP network is used as the connectivity to the remote system
3	*IPX	
4	Reserved	

5	*USRDFN	User-defined connectivity is used as the connectivity to the remote system.

Data queue Name of the data queue that is associated with this output queue, or *NONE. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Data queue library The name of the library that contains the data queue. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Destination The type of destination system to which spooled files are being sent, or *NONE (0) if a remote connection does not exist. This is an integer with enumerated values. Other valid values include *OS400 (1), *OS400v2 (2), *S390 (3), *PSF2 (4), Reserved (5), NETWARE3 (6), *NDS (7), and *OTHER (-1).

Display any file Indicates whether users who have authority to read this output queue can display the data of any output file. Valid values include *YES, *NO, or *OWNER if only the file owner or a user with *SPLCTL authority can access the file data.

File ASP The auxiliary storage pool where the spooled files reside. Valid entries are integers with a range from 0 to 255. *System (1) is a valid value.

Files The number of spooled files that exist on the output queue. Valid entries are integers.

Library The library that contains the output queue. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Max pages The maximum number of pages that a spooled file on the output queue can contain.

Name The name of the output queue. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Operator controlled Indicates whether users with job control authority (SPCAUT(*JOBCTL)) are allowed to manage or control the files on this queue. Valid entries are alphanumeric strings with a maximum length of 10.

Order The order of the spooled files on the output queue; the order is first-in first-out or established by job number. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Printer The name of the first printer device that was started for the output queue, or blank if none have started. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Published Indicates whether the output queue is published in the network directory. Valid values include 1 for Yes or zero for No.

Remote printer queue The printer queue on the remote system to which the remote writer sends spooled files. Valid entries are alphanumeric strings with a maximum length of 256 characters.

Remote system The name, TCP/IP address, or special value for the remote system where files are sent when a remote writer is started to the output queue. Valid entries are alphanumeric strings with a maximum length of 256 characters.

Separators The number of job separators to be placed at the beginning of the output, or *MSG (-2) if a message is sent to the writer message queue at the end of each job.

Status The status for the output queue. Valid values include Released and Held.

Writer name The job name of the first writer for the output queue, or blank if a writer is not started. Valid entries are alphanumeric strings with a maximum length of 10 characters.

Writer status The status of the first writer for the output queue, or blank if no writer is started. Valid entries are alphanumeric strings with a maximum length of 10 characters. The following table shows valid values:

STR	The writer job is started to the output queue.
END	The writer job is ended.
JOBQ	The writer job is on the job queue.
HLD	The writer job is held.
MSGW	The writer job is waiting for a message.

Writers The number of printer writers that were started to this output queue. Valid entries are integers.

Security Jrn AuditJrn attributes

The Security Jrn AuditJrn attribute group includes attributes that you can use to track all changes relating to system security. The attributes in this section apply to all audit journal entries.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Entry Type The type of entry written to the audit journal.

Note: You must specify the Entry Type attribute when you create a situation using the OS400 Security Jrn AuditJrn attribute group. If you do not use the Entry Type attribute in a predicate, the program stops the situation.

The following values are valid:

AF	Authority failure
CA	Authority changes
CP	User profile changes, created, or restored
DS	DST security password reset
JD	Change to user parameter of a job description
NA	Network attribute changed
OW	Object ownership changed
PA	Program changed to adopt authority
PS	Profile swap
PW	Password not valid
RA	Authority change during restore
RJ	Restoring job description with user profile specified
RO	Change of object owner during restore
RP	Restoring adopted authority program
RU	Restoring user profile authority
SE	Subsystem routing entry change
SV	System value changed

Job Name The name of the job that caused the entry to be written in the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Job Number The job number of the job that caused the entry to be written in the audit journal. The valid value is an alphanumeric string with a maximum of 6 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

User Profile The name of the current user profile associated with the job. The valid value is an alphanumeric string with a maximum of 10 characters.

Security Jrn AuthFail attributes

The Security Jrn AuthFail attribute group includes attributes that monitor the journal entries describing authority failures.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Job Name The name of the job. The valid value is an alphanumeric string with a maximum of 10 characters.

Job Number The number the system assigned to the job. The valid value is an alphanumeric string with a maximum of 6 characters.

Object The name of the object. The valid value is an alphanumeric string with a maximum of 10 characters.

Object Library The name of the library that includes the object. The valid value is an alphanumeric string with a maximum of 10 characters.

Object Type The type of object. The following values are valid:

*ALRTBL	Alert table
*AUTL	Authorization list
*BLKSF	Block special file
*BNDDIR	Binding directory
*CFGL	Configuration list
*CHRSF	Character special file
*CHTFMT	Chart format
*CLD	C description
*CLS	Class
*CMD	Command
*CNNL	Connection list
*COSD	Class-of-service description
*CRG	Cluster resource group
*CRQD	Change request description
*CSI	Communications Side Information
*CSPMAP	Cross System Product map
*CSPTBL	Cross System Product table
*CTLD	Controller description
*DDIR	Distributed file directory
*DEVD	Device description
*DIR	Directory
*DOC	Document

*DTAARA	Data area
*DTADCT	Data dictionary
*DTAQ	Data queue
*EDTD	Edit description
*EXITRG	Exit registration
*FCT	Forms control table
*FIFO	First-in-first-out special file
*FILE	File
*FLR	Folder
*FNTRSC	Font resources
*FNTTBL	Font mapping table
*FORMDF	Form definition
*FTR	Filter
*GSS	Graphics symbol set
*IGCDCT	Double-byte character set (DBCS) conversion dictionary
*IGCSRT	Double-byte character set (DBCS) sort table
*IGCTBL	Double-byte character set (DBCS) font table
*IMGCLG	Image Catalog
*IPXD	Internet work packet exchange description
*JOBD	Job description
*JOBQ	Job queue
*JOBSCD	Job schedule
*JRN	Journal
*JRNRCV	Journal receiver
*LIB	Library
*LIND	Line description
*LOCALE	Locale
*M36	i5/OS Advanced 36® machine
*M36CFG	i5/OS Advanced 36 machine configuration
*MEDDFN	Media definition
*MENU	Menu description
*MGTCOL	Management collection
*MODD	Mode description
*MODULE	Compiler unit
*MSGF	Message File
*MSGQ	Message queue
*NODGRP	Node group
*NODL	Node list
*NTDB	NetBIOS description
*NWID	Network interface description
*NWSCFG	Network server configuration
*NWSD	Network server description

*OUTQ	Output queue
*OVL	Overlay
*PAGDFN	Page definition
*PAGSEG	Page segment
*PDFMAP	Portable Document Format map
*PDG	Print Descriptor Group
*PGM	Program
*PNLGRP	Panel group definition
*PRDAVL	Product availability
*PRDDFN	Product definition
*PRDLOD	Product load
*PSFCFG	Print Services Facility™ configuration
*QMFORM	Query management form
*QMQRY	Query management query
*QRYDFN	Query definition
*RCT	Reference code translation table
*S36	System/36 computer description
*SBSD	Subsystem description
*SCHIDX	Information search index
*SOCKET	Local socket
*SPADCT	Spelling aid dictionary
*SQLPKG	Structured Query Language package
*SQLUDT	User-defined SQL type
*SRVPGM	Service program
*SSND	Session description
*STMF	Bytestream file
*SVRSTG	Server storage space
*SYMLNK	Symbolic link
*TBL	Table
*TIMZON	Time zone description
*USRIDX	User index
*USRPRF	User profile
*USRQ	User queue
*USRSPC	User space
*VLDL	Validation List
*WSCST	Workstation customizing object

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

User The name of the user that caused the audit journal entry. The valid value is an alphanumeric string with a maximum of 10 characters.

Validation Value The type of cyclic redundancy check (validation value), which is set only if the violation type is C. The following values are valid:

A	A changed object that might violate security was restored.
B	All authority revoked when object was restored.
C	A copy was restored of the program that was translated.
D	The security requested that the changed object was restored.
E	Detection of a system install-time error.

Violation Type The type of security violation that occurred. The following values are valid:

A	A user attempted to perform an operation or access an object without the required authority.
B	A restricted computer interface instruction was run by a program.
C	A program was restored that failed the restore-time program validation checks. Information about the failure is in the Validation Value Violation Type field of the record. (See the Validation Value attribute.)
D	A program attempted to access an object using an interface that is not supported or a callable program that is not in the callable API list.
J	A submitter without *USE authority for a user profile attempted to submit or schedule a job using the user profile. Submitter did not have *USE authority to the user profile.
P	The use was attempted of a profile handle that is not valid on the QWTSETP API.
R	An update was attempted to an object that is read only. (Enhanced hardware storage protection is logged only at security level 40.)
S	A sign-on was attempted without a user ID and password.

Security Jrn ChgAuth attributes

The Security Jrn ChgAuth attribute group includes attributes that you can use to monitor changes to authorization lists or object authority.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

ADD Indicates whether there has been a change to add authority. The following values are valid:

*YES	ADD authority granted or revoked.
*NO	The authority has not changed.

Auth List Name The name of the authorization list. The valid value is an alphanumeric string with a maximum of 10 characters.

AUTLMGT Indicates whether there has been a change to *AUTLMGT or *AUTL public authority. The following values are valid:

*YES	AUTLMGT authority or *AUTL public authority has been granted or revoked.
*NO	There has been no change to authority.

Command Type Indicates the type of command used. The following values are valid:

GRT	Grant
RVK	Revoke

DLT Indicates whether there has been a change to delete authority. The following values are valid:

*YES	DLT authority has been granted or revoked.
*NO	The authority has not changed.

EXCLUDE Indicates whether there has been change to exclude authority. The following values are valid:

*YES	EXCLUDE authority has been granted or revoked.
*NO	The authority has not changed.

Job User The name of the user profile whose authority is being granted or revoked. The valid value is an alphanumeric string with a maximum of 10 characters.

Object Name The name of the object. The valid values included an alphanumeric string with a maximum of 10 characters.

OBJEXIST Indicates whether there has been a change to object authority. The following values are valid:

*YES	OBJEXIST authority has been granted or revoked.
*NO	The authority has not changed.

Object Library Name The name of the library that includes the object. The valid value is an alphanumeric string with a maximum of 10 characters.

OBJMGT Indicates whether there has been a change to object management authority. The following values are valid:

*YES	OBJMGT authority granted or revoked.
*NO	The authority has not changed.

OBJOPR Indicates whether *OBJOPR authority has been changed. The following values are valid:

*YES	OBJOPR authority has been granted or revoked.
*NO	The authority has not changed.

Object Type The type of object. The valid value is an alphanumeric string with a maximum of 8 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

READ Indicates whether there has been a change to read authority. The following values are valid:

*YES	READ authority has been granted or revoked.
*NO	The authority has not changed.

UPDATE Indicates whether there has been a change to update authority. The following values are valid:

*YES	UPD authority has been granted or revoked.
*NO	The authority has not changed.

Security Jrn ChgOwner attributes

The Security Jrn ChgOwner attributes attribute group includes attributes that you can use to monitor changes to object ownership.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

New Owner The new owner of the object who logged a change in ownership to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Object Name The name of the object. The valid value is an alphanumeric string with a maximum of 10 characters.

Object Library The name of the library that includes the object. The valid value is an alphanumeric string with a maximum of 10 characters.

Object Type The type of object. The valid value is an alphanumeric string with a maximum of 8 characters.

Old Owner The previous owner of the object that logged a change in ownership to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Security Jrn ChgUserProf attributes

The Security Jrn ChgUserProf attribute group includes attributes that you can use to monitor create, change, or restore operation to the user profile.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

ALLOBJ Indicates whether all object authority has been changed. All object authority allows users to work with system resources, such as applying program temporary fixes (PTFs). The following values are valid:

*YES	ALLOBJ special authority has been granted or revoked.
*NO	The authority has no changed.

Command Type The type of command used. The following values are valid:

CRT	Create User Profile (CRTUSRPRF) command
CHG	Change User Profile (CHGUSRPRF) command
RST	Restore User Profile (RSTUSRPRF) command
DST	Change Dedicated Service Tools Password (CHGDSTPWD) command

JOBCTL Indicates whether job control authority has been changed. Job control authority allows user to work with jobs, such as changing, holding, and cancelling. The following values are valid:

*YES	JOBCTL special authority has been granted or revoked.
*NO	The authority has not changed.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Password Changed Indicates whether the password has changed for the user profile. The following values are valid:

*YES	Indicates the password for the user profile has changed.
*NO	Indicates there has been no change to the password for the user profile.

Password Expired Indicates whether a password has expired. The following values are valid:

*YES	The password is expired.
*NO	The password did not expire.

SAVSYS Indicates whether save system authority has been changed. Save system authority allows users to save, restore, and free storage for system objects. The following values are valid:

*YES	SAVSYS special authority has been granted or revoked.
*NO	The authority has not changed.

SECADM Indicates whether security administrator authority has been changed. A security administrator can create, change, or delete user profiles. The following values are valid:

*YES	SECADM special authority has been granted or revoked.
*NO	The authority has not changed.

SERVICE Indicates whether service authority has been changed. Service authority allows users to perform service functions, such as working with the problem log. The following values are valid:

*YES	SERVICE special authority has been granted or revoked.
*NO	The authority has not changed.

SPLCTL Indicates whether spool control authority has been changed. Spool control authority allows users to perform all spool-related functions. The following values are valid:

*YES	SPLCTL special authority has been granted or revoked.
*NO	The authority has not changed.

USER The name of the user profile that was changed. The valid value is an alphanumeric string with a maximum of 10 characters.

Security Jrn JobDesc attributes

The Security Jrn JobDesc attribute group includes attributes that you can use to monitor changes to job descriptions and job owners.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Job Description Indicates that a change to the name of the job description was logged to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

New User Indicates the new name of the user profile specified for the USER parameter that was logged to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Old User Indicates the old name of the user profile specified for the USER parameter that was logged to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Security Jrn Network attributes

The Security Jrn Network attribute group includes attributes that you can use to monitor changes to network attributes.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Changed Attribute Indicates a change to the named network attribute was logged to the audit journal. The following values are valid:

SYSNAME	Current system name
PNDSYSNAME	Pending system name
LCLNETID	Local network ID
LCLCPNAME	Local control point name
LCLLOCNAME	Local location name
DFTMODE	Default mode name
NODETYPE	APPN node type
DTACPR	Current level of data compression
DTACPRINM	Current level of intermediate node data compression
MAXINTSSN	Maximum number of intermediate sessions
RAR	Route addition resistance
NETSERVER	List of network node servers
ALRSTS	Alert status
ALRPRIFP	Alert primary focal point
ALRDFTFP	Alert default focal point
ALRLOGSTS	Alert logging status
ALRBCKFP	Name of the system that provides alert focal point services if the primary focal point is unavailable
ALRRQSFP	Name of the system that is requested to provide alert focal point services
ALRCTLD	Name of the controller through which alert messages are sent on a SSCP-PU session

ALRHLDCNT	Maximum number of alerts that are created before the alerts are sent over the alert controller session (ALRCTLD network attribute)
ALRFTR	Name of the active alert filter
ALRFTRLIB	Name of the library that includes the alert filter definition
MSGQ	Name of the system-default network message queue
MSGQLIB	Name of the library that includes the system-default message queue
OUTQ	Name of the system-default network output queue
OUTQLIB	Name of the library that includes the system-default network message queue
JOBACN	Current job action for job streams received through the network
MAXHOP	Maximum number of times in the SNADS network that a distribution queue originating at this node can be received and rerouted on the path to its final destination
DDMACC	Current system action for DDM requests from other systems
DDMACCLIB	Name of the library that includes the DDM access program
PCSACC	Current system action for Client Access for i5/OS requests
PCSACCLIB	Name of the library that includes the Client Access for i5/OS access program
DFTNETTYPE	System default value for the Integrated Services Digital Network (ISDN) network type
DFTCNNLST	System default value for the ISDN connection list

New Attribute Value The value of the network attribute after it was changed. The valid value is an alphanumeric string with a maximum of 250 characters.

Old Attribute Value The value of the network attribute before it was changed. The valid value is an alphanumeric string with a maximum of 250 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Security Jrn Password attributes

The Security Jrn Password attribute group includes attributes that you can use to monitor for incorrect passwords or incorrect user IDs.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Device Name The name of the device where the password or user ID was entered. The valid value is an alphanumeric string with a maximum of 40 characters.

Job User The system name of the person using the job. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Violation Type Indicates whether the security violation was the result of an invalid user ID or password. The following values are valid:

P	Password is not valid
U	User ID is not valid.

Security Jrn ProfSwap attributes

The Security Jrn ProfSwap attribute group includes attributes that you can use to monitor for users or jobs that have changed user profiles while performing system operations.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Entry Type The type of entry. The following values are valid:

A	Profile swap during pass-through
H	Profile handle generated by the Get Profile Handle (QSYGETPH) API

New Target A new pass-through target user profile was logged to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Old Target The original pass-through target user profile was logged to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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 Location The pass-through source location was logged to the audit journal. The valid value is an alphanumeric string with a maximum of 8 characters.

User Profile The user profile name. The valid value is an alphanumeric string with a maximum of 10 characters.

Security Jrn ProgAdopt attributes

The Security Jrn ProfAdopt attribute group includes attributes that you can use to monitor program adopt changes to the audit journal.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Owner The name of the owner who logged a program adopt change to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Program library The name of the library where the program is found. The valid value is an alphanumeric string with a maximum of 10 characters.

Program name The name of the program. The valid value is an alphanumeric string with a maximum of 10 characters.

Security Jrn RestoreJob attributes

The Security Jrn RestoreJob attribute group includes attributes that you can use to monitor for job descriptions containing a user profile name has been restored.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Job Description The name of the job description that was restored and logged to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Job Description Library The name of the library to which the job description was restored. The valid value is an alphanumeric string with a maximum of 10 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

User The name of the user profile specified in the job description. The valid value is an alphanumeric string with a maximum of 10 characters.

Security Jrn RestoreProg attributes

The Security Jrn RestoreProg attribute group includes attributes that you can use to monitor for restored jobs that adopt owner authority.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Program The name of the restored program. The valid value is an alphanumeric string with a maximum of 10 characters.

Program Library The name of the library where the program is found. The valid value is an alphanumeric string with a maximum of 10 characters.

Program Owner The name of the owner of the program. The valid value is an alphanumeric string with a maximum of 10 characters.

Security Jrn SYSVAL attributes

The Security Jrn SYSVAL attribute group includes attributes that you can use to monitor for system values that have changed.

Note: The i5/OS programming interfaces used to access the security auditing journal do not permit access by the agent's user profile QAUTOMON. Therefore, in order for any of the security journal attribute groups to return data for situations, you must give QAUTOMON access to the security auditing journal and its receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers before starting any related situations.

Note: This attribute group is implemented as a pure event only. That means it should not be used in queries for reports and workspaces, but should only be used in situations. Attempting to use it in reports always results in no data being returned.

New Value The value of the system value after it was changed. The valid value is an alphanumeric string with a maximum of 250 characters.

Old Value The value of the system value before it was changed. The valid value is an alphanumeric string with a maximum of 250 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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 Name The name of the system value that was changed and logged to the audit journal. The valid value is an alphanumeric string with a maximum of 10 characters.

Storage Pool attributes

The Storage Pool attribute group includes attributes that you can use to monitor the performance of storage. These attributes allow you to collect information about pool performance based on the cumulative values of storage pool counters. These attributes are in the operational areas of performance, work management, and storage.

Activity Level The maximum number of processes that can be active in the pool at the same time. The valid value is an integer from 0 - 100000. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Active to Ineligible For the processes assigned to this pool, this attribute is the rate of active-to-ineligible transitions per second during the last monitor interval. (Such a transition results when a transaction does not complete during a single time slice.) The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

ATI ATW Ratio The ratio from Active to Ineligible to Active to Wait. The valid value is an integer from 0.0 - 3276.7.

Database Fault The rate of interruptions to processes per second. The interruptions were required to transfer data into the pool, which permitted work to be done on the database function during the last monitor interval. The valid value is an integer from 0 - 214743647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Database Pages The rate in pages per second at which database pages are brought into the storage pool.

Name Storage pool name.

Nondatabase Fault The rate of interruptions to processes per second. The interruptions were required to transfer data into the pool, which permitted work to be done on the nondatabase function during the last monitor interval. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

NonDatabase Pages The rate in pages per second at which non-database pages are brought into the storage pool.

Number The unique identifier for the storage pool. The valid value is an integer from 1 - 16. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Reserved Amount of storage in Kilobytes that is reserved for system use.

Size The amount of main storage assigned to the pool (in kilobytes). The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Total Fault Total number of interruptions to processes per second required to transfer data into the pool to permit work to continue on database and nondatabase functions. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions. The attribute is the sum of these values:

- Database Fault
- Nondatabase Fault

Wait to Ineligible For the processes assigned to this pool, this attribute is the rate of wait-to-ineligible transitions per second during the last monitor interval. Such a transition results when a job is leaving a wait state but there is no available activity level. The valid value is an integer from 0 - 2147483647. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

WTI ATW Ratio The ratio of Wait to Ineligible to Active to Wait. The valid value is a decimal number from 0.0 - 32767.0.

Subsystem attributes

The Subsystem attribute group includes attributes that you can use for work management by monitoring all the subsystems (including subsystems that are inactive).

Current Jobs Active The number of jobs currently active in the subsystem, including held jobs, but excluding jobs that are disconnected or suspended because of a transfer secondary job or transfer group job. The valid value is an integer from 0 to no limit. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Description Library The name of the library where the subsystem description is stored. The valid value is an alphanumeric string with a maximum of 10 characters.

Max Jobs Active The maximum number of jobs that can run or use resources in the subsystem at one time. If the subsystem description specifies *NOMAX, no maximum exists, and the value is -1. The valid value is an integer from 0 - 1000. The attribute can be used with the *AVG, *MAX, *MIN, and *SUM functions.

Name The name of the subsystem about which information is being returned. The valid value is an alphanumeric string with a maximum of 10 characters.

Number Pools The number of storage pools defined for the subsystem. The valid value is an integer from 1 - 100000.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Pool Activity Level The maximum number of threads that can be active in the pool at one time, or zero for a system-defined pool.

Pool Name The name of the pool for the subsystem. The valid value is an alphanumeric name with a maximum of 10 characters or one of these values:

- *USERPOOL
- *BASE
- *INTERACT
- *NOSTG
- *SHRPOOL1
- *SHRPOOL2
- *SHRPOOL3
- *SHRPOOL4
- *SHRPOOL5
- *SHRPOOL6
- *SHRPOOL7
- *SHRPOOL8
- *SHRPOOL9
- *SHRPOOL10
- *SPOOL

Status The status of the subsystem. The following values are valid:

*ACTIVE	The status is active (default value).
*INACTIVE	The status is inactive.

System Statistics attributes

Use the System Statistics attributes to monitor the current batch job and user statistics. System Statistics attributes are sampled attributes in the operational area of operations.

Batch jobs ended with output waiting The number of completed batch jobs that produced printer output that is waiting to print.

Batch jobs ending The number of batch jobs that are in the process of ending. This is caused by one of the following conditions:

- The job finishes processing normally.
- The job ends before its normal completion point and is being removed from the system.

Batch jobs held on job queue The number of batch jobs that were submitted, but were held before they can begin running.

Batch jobs held while running The number of batch jobs that had started running, but are now held.

Batch jobs on held job queue The number of batch jobs that are on job queues that have been assigned to a subsystem, but the job queues are being held.

Batch jobs on an unassigned job queue The number of batch jobs on job queues that have not been assigned to a subsystem.

Batch jobs running The number of batch jobs currently running on the system.

Batch jobs waiting on messages The number of batch jobs waiting for a reply to a message before they can continue to run.

Batch jobs waiting to run The number of batch jobs on the system that are currently waiting to run, including those that were submitted to run at a future date and time.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Users signed on The number of users currently signed on the system. System request jobs and group jobs are not included in this number.

Users signed off with waiting printer output The number of sessions that have ended with printer output files waiting to print.

Users suspended by group jobs The number of user jobs that have been temporarily suspended by group jobs so that another job might be run.

Users suspended by system request The number of user jobs that have been temporarily suspended by system request jobs so that another job might be run.

Users temporarily signed off The number of jobs that have been disconnected caused by either the selection of option 80 (Temporary sign-off) or the entry of the Disconnect Job (DSCJOB) command.

System Status attributes

The System Status attribute group includes attributes that you can use to monitor the resources for a system.

% Aux Storage Used The percentage of total auxiliary storage used in all online auxiliary storage pools.

% Database CPU The percentage of CPU used by database related activity. NA (-1) indicates this system does not report the amount of CPU used for database processing.

% Interactive CPU The percentage of interactive performance assigned to this logical partition.

% Interactive Limit The percentage of the interactive limit that was used.

% Maximum Jobs The percentage of the maximum number of jobs allowed on the system that are currently in use. When the percentage of jobs reaches 100% of the maximum, you can no longer submit nor start more jobs on the system.

% Secondary Work CPU The percentage of CPU used by secondary workloads.

% Shared Processors The percentage of the total shared processor pool capacity used by all partitions using the pool during the elapsed time. NA (0) indicates this partition does not share processors, or this operating system release does not support the metric.

% Uncapped CPU The percentage of the uncapped shared processing capacity that was used during the elapsed time. NA (0) indicates this partition cannot use more than its configured processing capacity, or this operating system release does not support the metric.

Active Jobs The number of jobs active in the system (jobs that have been started, but have not yet ended), including user and system jobs.

CPU Percent The average percent that the available processing units were in use during the elapsed time.

Main Storage Size The amount of main storage, in megabytes, in the system. On a partitioned system the main storage size can change while the system is active.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Partition ID The identifier for this partition.

Perm Address Percent Used The percentage of the maximum possible addresses for permanent objects that have been used.

Processing Capacity The amount of current processing capacity of the partition. For a partition sharing physical processors, this attribute represents its share of the physical processors in the pool. For a partition using dedicated processors, the value represents the number of virtual processors that are currently active in the partition.

System ASP Used The percentage of the system auxiliary storage pool currently in use.

Temp Address Percent Used The percentage of the maximum possible addresses for temporary objects that have been used.

Total Job Count The total number of user jobs and system jobs that are currently in the system. The total includes all jobs on job queues waiting to be processed, all jobs currently being processed, and all jobs that have completed running but still have output on output queues to be produced. The valid value is an integer from 0 - 1000000.

Up Time The total amount of time, in seconds, that the operating system has been operational since it was last 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.

Up Time Days The total amount of time that the operating system has been operational since it was last started, formatted as days, hours, minutes, and seconds. Valid entries are in the format DDDdHH:MM:SS.

System Values Acct attributes

The System Values Acct attribute group includes attributes that you can use to monitor system values for accounting.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

QABNORMSW Indicates the status of a previous end of a system. The following values are valid:

*YES	Previous end of system was not normal.
*NO	Previous end of system was normal.

QACGLVL The accounting level of the system. The following values are valid:

*NONE	Indicates that no accounting information is written to a journal.
*JOB	Indicates that job resource use is written to a journal.
*PRINT	Indicates that resource use for spooled and nonspooled print files is written to a journal.

QACTJOB The initial number of active jobs for which auxiliary storage is to be allocated during an initial program load (IPL). The valid value is an integer from 1 - 32767.

QADLACTJ Indicates the additional number of active jobs for which auxiliary storage is to be allocated when the initial number of active jobs (the system value *QACTJOB) is reached. The valid value is an integer from 1 - 32767.

QADLSPLA Indicates the additional storage to add to the spooling control block. The valid value is an integer from 1024 - 32767.

QADLTOTJ Indicates the additional number of jobs for which auxiliary storage is to be allocated when the initial number of jobs (system value QTOTJOB) is reached. The valid value is an integer from 1 - 32767.

QAUDCTL This system value that controls whether auditing is done for objects and actions of the users. It also allows you to specify the level to be performed. The following values are valid:

*NONE	The following changes are not audited: • Object • User actions • QAUDLVL
*OBJAUD	Objects selected by the Change Object Auditing Value (CHGOBJAUD) command are audited.
*AUDLVL	*QAUDLVL system value and CHGUSRAUD (AUDLVL) changes are audited.

QAUDENDACN Indicates the action to be taken if auditing data cannot be written to the security auditing journal. The following values are valid:

*NOTIFY	A journal entry was not written to the security auditing journal and a message was sent to the QSYSOPR and QSYSMSG message queues. The action that caused the audit to be attempted continues.
*PWRDWNSYS	If sending the audit data to the security audit journal fails, the system is ended with a system reference code (SRC). The system is subsequently started in a restricted state on the following IPL.

QAUDLVL The security auditing level. The system values specifies the level of security auditing that must occur on the system. The following values are valid:

*NONE	No auditing occurred.
*AUTFAIL	The following failures are audited. • All access failures (sign-on) • Incorrect password or user IDs entered from a device
*CREATE	These objects are audited. (Objects created in the QTEMP library are not audited.) • New objects • Objects created to replace existing objects
*DELETE	All delete operations of external objects on system. (Objects deleted from QTEMP are not audited.)
*JOBDTA	These actions are audited. • Job start and job stop data • Hold, release, change, disconnect, end, end abnormally, PSR (program start request) attached to prestart job entries, change to another user profile
*OBJMGT	These actions are audited. • Moves of objects • Renames of objects

*OFCSRV	These Office Vision for i5/OS tasks are audited. • Changing the system distribution directory • Opening a mail log for a different user
*PGMADP	Adopting authority from a program owner is audited.
*PGMFAIL	Integrity violations are audited (blocked instruction, validation value failure, domain violation).
*PRTDTA	These printing functions are audited. • Printing a spooled file • Printing with parameter SPOOL(*NO)
*SAVRST	These save and restore functions are audited. Restores for: • Objects • Programs that adopt the user profile for the owner • Job descriptions that contain user names • Objects with changed ownership and authority • Authority for user profiles
*SECURITY	These security functions are audited. Changes to: • Object authority • Profiles • Object ownership • Programs that now adopt the profile for the owner • System values • Network attributes • Subsystem routing • QSECOFR passwords reset to the value shipped by DST • DST security officer password is requested to be defaulted
*SERVICE	These commands for system service tools are audited. • Dump Object (DMPOBJ) • Dump System Object (DMPSYSOBJ) • Dump Document Library Object (DMPDLO) • Start Copy Screen (STRCPYSCN) • Start Communications Trace (STRCMNTRC) • End Communications Trace (ENDCMNTRC) • Print Communications Trace (PRTCMNTRC) • Delete Communications Trace (DLTCMNTRC) • Print Error Log (PRTERRLOG) • Print Internal Data (PRTINTDTA) • Start Service Job (STRSRVJOB) • Start System Service Tools (STRSST) • Trace Internal (TRCINT)

*SPLFDTA	These actions for spooled files are audited. • Create • Delete • Display • Copy • Get data • Hold • Release • Change
*SYSMGT	These tasks for system management are audited. • Changes for Operational Assistant* functions • Operations with network files • Changes to the system reply list • Changes to HFS registration • Changes to the DRDA* relational database directory

QBASACTLVL The base-storage-pool activity level. The value indicates how many system and user jobs can simultaneously compete for storage in the base storage pool. The valid value is an integer from 1 - 32767.

System Values attributes

The System Values attribute group includes attributes that you can use to monitor the system values for the configuration.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

QAUTOCFG Indicates whether the system automatically configures devices that are added to the system. The following values are valid:

*YES	Devices are automatically configured.
*NO	Devices are not automatically configured.

QAUTOVRT The system value for the number of virtual devices to be automatically configured. The valid value is an integer from 0 - 9999.

QBASPOOL The minimum size of the base storage pool specified in kilobytes. The base pool includes all the main storage not allocated by other pools. The valid value is an integer from 32 - 2147483647.

QDSCJOBITV Indicates the length of time, in minutes, an interactive job can be disconnected before it is ended. The following values are valid:

A number from 5 - 1440	The number of minutes that can be specified for the disconnect interval.
*NONE (5555)	There is no disconnect interval.

QMODEL The model number for the system. The valid value is an alphanumeric string with a maximum of 4 characters.

QPWEXPITV Allows you to specify the minimum number of days a problem is kept in the problem log. The valid value is an integer from 0 - 999.

QPWDEXPITV System value for the password expiration interval. The value controls the number of days that passwords are valid by specifying the frequency that they might or must be changed. The following values are valid:

*NOMAX (666)	No maximum number of days is set for the password.
A number from 1 - 366	Maximum number of days the password can be used.

QPWRRSTIPL Specifies whether the system must automatically perform an IPL when utility power is restored after a power failure. The following values are valid:

*YES	If the power fails, there is no auto-IPL after the power is restored.
*NO	If the power fails, there is not an auto-IPL after the power is restored.

QRCLSPLSTG The system value for the reclaim spool storage. It allows for the automatic removal of empty spool database members. The following values are valid:

*NOMAX (666)	The maximum retention interval is used.
*NONE (5555)	There is no retention interval.
A number from 1 - 366	Number of days empty spool database members are kept for new spooled file use.

QRMTSIGN Specifies how the system responds to remote sign-on requests. The user can specify a program and library to decide which remote sessions are allowed and which user profiles can automatically sign on from which locations. The first 10 characters contain the program name, and the last 10 characters contain the library name. The following values are valid:

*FRCSIGNON	Normal sign-on processing is required for all remote sign-on processing.
*SAMEPRF	For remote sign-on attempts, sign-on might be bypassed for remote sign-on attempts.
*VERIFY	For users with access to the system, the user is allowed to bypass the sign-on after access is verified.
*REJECT	No remote sign-ons are allowed.

QSECURITY Indicates the level of system security. The following values are valid:

10	No password is required to access all system resources.
20	A password is required at sign-on and user is required to have authority to access all system resources.
30	A password is required at sign-on and user is required to have authority to access objects and system resources.
40	A password is required at sign-on and user is required to have authority to access objects and system resources. Programs that use unsupported interfaces to access objects fail.
50	A password is required at sign-on and the user is required to have authority to access objects and system resources. Security and integrity is enforced for the QTEMP library and user domain objects. Security and integrity of the QTEMP library and user domain (*USR_xxx) objects are enforced. Use system value QALWUSRDMN to change the libraries that allow *USR_xxx objects. Programs fail if they try to pass unsupported parameter values to supported interfaces, or if they try to access objects through unsupported interfaces.

Note: If this system value has been changed since the last IPL, this is not the security level the system is currently using. This value is in effect after the next IPL.

QSFWERRLOG Specifies whether software errors must be logged by the system. The valid values include an alphanumeric string with a maximum of 10 characters or one of the following values.

- *LOG (Software errors are logged.)
- *NOLOG (No logging occurs.)

QSRLNBR The serial number for the system. The valid value is an integer with a maximum of 8 characters.

QUPSMSGQ The name of the message queue and library that is to receive uninterrupted power supply messages. The valid value is an alphanumeric string with a maximum 20 characters. The first 10 characters indicate the name of the message queue and the last 10 characters indicate the name of the library.

System Values Device attributes

The System Values Device attribute group includes attributes that you can use to monitor systems values for devices.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

QDEVNAMING The device naming convention. This value specifies what naming convention is used when the system automatically creates device descriptions. The following values are valid:

*NORMAL	Naming conventions must follow current system standards.
*S36	Naming conventions must follow System/36 standards.
*DEVADR	Device names are derived from the device address.

QDEVRCYACN Specifies what action to take when an I/O error occurs on the workstation for an interactive job. The following values are valid:

*MSG	Signals the I/O error message to the user application program.
*DSCENDRQS	Disconnects the job. When signing-on again, a cancel request function is performed to return control of the job back to the last request level.
*DSCMSG	Disconnects the job. When signing-on again, an error message is sent to the user application.
*ENDJOB	Ends the job. A job log is produced for the job.
*ENDJOBNOLIST	Ends the job. A job log is not produced for the job.

System Values IPL attributes

The System Values IPL attribute group includes attributes that you can use to monitor system values used to IPL the system.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

QABNORMSW Indicates the status of the previous end of a system. The following values are valid:

*YES	Previous end of system was abnormal.
*NO	Previous end of system was normal.

QIPLDATTIM The system value for the date and time that specifies when an automatic IPL of the system must occur. The valid value include:

- a numeric date and time
- *NONE (indicates that an automatic IPL is scheduled)

QIPLSTS The IPL status indicator. This value indicates what type of IPL occurred last. The following values are valid:

*OPR	Operator panel IPL
*AUTO	automatic IPL after power restored
*RESTR	Restart IPL
*TOD	Time-of-day IPL
*RMT	Remote IPL

QIPLTYPE Indicates the type of IPL to perform. This value specifies the type of IPL performed when the system is powered on manually with the key in the normal position. The following values are valid:

*UNATTEND	The IPL is unattended.
*DST	The IPL is attended with dedicated service tools.
*DBG	The IPL is attended with console in debug mode.

QPWRRSTIPL Specifies whether the system must automatically perform an IPL when utility power is restored after a power failure. The following values are valid:

*YES	If the power fails, there is an auto-IPL after the power is restored.
*NO	If the power fails, there is not an auto-IPL after the power is restored.

QRMTIPL The remote power on and IPL indicator. The following values are valid:

*YES	A telephone line can be used for a remote power on.
*NO	A telephone line cannot be used for a remote power on.

System Values Perf attributes

The System Values Perf attribute group includes attributes that you can use to monitor the configuration values for performance.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

QHSTLOGSIZ The maximum number of records for each version of the history log, or *DAILY if a new version is created each time that the date in the history log messages changes.

QINACTITV Specifies the inactive job time-out interval in minutes. It specifies when the system takes action on inactive interactive jobs. The following values are valid:

*NONE (555)	The system does not check for inactive interactive jobs.
A number from 5 - 300	The value indicates the number of minutes that job can be inactive before the action is taken.

QINACTMSGQ Name and library of a message queue that receives message CPI1126 when a job has been inactive, or special values indicating the action to take. The following values are valid:

An alphanumeric string	There is a maximum of 20 characters. The list can contain up to 2 10-character values where the first is the message queue name and the second is the library name.
DSCJOB	The interactive job and any jobs associated with are disconnected.
ENDJOB	The interactive job and any jobs associated with it are ended.

QMAXACTLVL The maximum activity level of the system. This is the number of jobs that can compete at the same time for main storage and processor resources. The following values are valid:

- *NOMAX (There is no maximum level for the system.)
- a number from 0 - 32767

QMAXSGNACN Specifies the action taken when the maximum number of consecutive incorrect sign-on attempts is reached. The action can be to disable a device, profile, or to take both actions. The following values are valid:

*DEV	If limit is reached, varies off device.
*PRF	If limit is reached, disables user profile.
*DEVPRF	If limit is reached, varies off device and disables user profile.

QMAXSIGN The maximum number of incorrect sign-on attempts allowed. The following values are valid:

- *NOMAX (666) (There is no maximum number of sign-on attempts.)
- a number from 1 - 25

QMCHPOOL The size of the computer storage pool (in kilobytes). The computer storage pool includes shared computer programs and licensed programs. The valid values include an integer from 256 - 2147483647.

QPFRADJ Indicates whether the system must adjust values during IPL and adjust values dynamically for system pool sizes and activity levels. The following values are valid:

*NONE	No performance adjustment.
*IPL	Performance adjustment at IPL.
*DYNAMIC	Performance adjustment at IPL and dynamically.
*IPLDYN	Dynamic performance adjustment.

QSRVDMP Specifies whether service dumps are created for unmonitored escape messages. You can also specify to create service dumps for system jobs and user jobs only. The following values are valid:

*DMPALLJOB	Service dumps for unmonitored escape messages are created for all jobs.
*DMPSYSJOB	Service dumps for unmonitored escape messages are created only for system jobs, not user jobs.

*DMPUSRJOB	Service dumps for unmonitored escape messages are created only for user jobs and not system jobs. System jobs include the system arbiter, subsystem monitors, LU services process, spool readers and writers, and the start-control-program-function (SCPF) job.
*NONE	Service dumps are not done.

QSTRPRTWTR Specifies whether printer writers are started at IPL. The following values are valid:

*YES	Start printer writers.
*NO	Do not start printer writers.

QSTRUPPGM The name of the startup program called from an autostart job when the controlling subsystem is started. The following values are valid:

- *NONE or a value with these characteristics
- an alphanumeric string with a maximum of 20 characters (The first 10 characters contain the program name, and the last 10 characters contain the library name.)

QTOTJOB The initial number of jobs for which auxiliary storage is allocated during IPL. The valid value is an integer from 1 - 32767.

QTSEPOOL The time-slice end pool. This value specifies whether interactive jobs must be moved to another main storage pool when they reach time-slice end. The following values are valid:

*NONE	When time-sloe end is reached, jobs are not moved tot he base storage pool.
*BASE	When time-slice end is reached, jobs are moved to the base pool.

System Values Prob attributes

The System Values Prob attributes are attributes you can use to monitor for specific values for problems.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

QPRBFTR Indicates the name of the filter object that the service activity manager uses when processing problems. The following values are valid:

- *NONE or a value with these characteristics
- an alphanumeric string with a maximum of 20 characters (The list can consist of up to two 10-character values where the first value is the problem filter name, and the second value is the library name.)

QPRBHLDITV Indicates the minimum number of days a problem is kept in the problem log. The valid values include an integer from 0 - 999.

System Values User attributes

The System Values User attributes are attributes you can use to monitor for specific values for users.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

QCCSID The system value for coded character set identifiers. The valid is an integer from 1 - 65535.

QCHRID System value for the default character set and code page. The system value is retrieved as a single-character value. The valid value is an alphanumeric string with a maximum of 20 characters. The first 10 characters contain the character-set identifier right-justified, and the last 10 characters contain the code-page identifier right-justified.

QCMNRCYLMT The system value for communications recovery limits. The valid value is an alphanumeric string with a maximum of 20 characters. The first 10 characters contain the count limit right-justified, and the last 10 characters contain the time interval.

QCNTRYID The system value for the country identifier. This value specifies the country identifier to be used as the default on the system. The valid value is an alphanumeric string with a maximum of 2 characters.

QCTLSBSD The system value for the description for the controlling subsystem. The controlling subsystem is the first subsystem to start after an IPL. The valid value is an alphanumeric string with a maximum of 20 characters. The list can consist of up to two 10-character values, where the first value is the subsystem description name, and the second value is the library name.

QDATE The system value for date. The valid format is CYYMMDD, and the following values are valid:

C	Century (0 for the twentieth century and 1 for the twenty-first century
YY	Year
MM	Month
DD	Day

QDATFMT The system value for the date format. The valid format is YMD, MDY, DMY, or JUL (Julian format), and the following values are valid:

Y	Year
M	Month
D	Day

QDAY The system value for the day of the month. The valid value is an integer in the 1 - 31. If the value for QDATFMT is Julian, the range 1-366.

QHOUR The system value for the hour of the day based on a 24 hour clock. The valid value is an integer from 0 - 23.

QMINUTE The system value for the minute of the hour. The valid value is an integer from 0 - 59.

QMONTH The system value for the month of the year. This field is blank if the Julian (JUL) date format is specified in system value QDATFMT. The valid value is an integer from 1 - 12. If the value for QDATFMT is Julian, the field is blank.

QSECOND The system value for seconds. The valid value is an integer from 0 - 59.

QSYSLIBL The system part of the library list. The list can contain as many as 15 library names. The valid value is an alphanumeric string with a maximum of 150 characters.

QTIME The system value for the time of day, represented in hours (*QHOUR), minutes (*QMINUTE), and seconds (*QSECOND). The valid value consists of QHOUR, QMINUTE, and QSECOND.

QUPSDLYTIM The system value for the amount of time that elapses before the system automatically powers down following a power failure. When a change in power activates the uninterruptible power supply, messages are sent to the UPS message queue (the system value QUPMSGQ). This system value is only meaningful if your system has a battery power unit or an uninterrupted power supply attached. A change to this system value takes effect the next time a power failure occurs. The shipped value is *CAL. The following values are valid:

*BASIC	Powers only the PRC, IOP cards, and Load Source direct-access storage device. The appropriate wait time, in seconds, is calculated. (This must be used only if you have the battery power unit or an uninterrupted power supply without every rack being connected.)

Note: All other values indicate an uninterrupted power supply on all racks. The following values are valid:

*CALC	The appropriate wait time is calculated.
*NOMAX	The system does not start any action on its own.
0	The system automatically powers down when system utility power fails.
1 - 99999	The delay time specified in seconds before the system powers down. The value is in a 2 item list that consists of: • first, the value specified using the Change System Value (CHGSYSVAL) command • second, the delay time (The delay time is either specified by the user or calculated using *CALC or *BASIC.).

QUSRLIBL The default for the user part of the library list. The list can contain as many as 25 names. The valid value is an alphanumeric string with a maximum of 250 characters.

QUTCOFFSET The system value that indicates the difference in hours and minutes between Universal Time Coordinated (UTC), also known as Greenwich mean time, and the current system time (local). The valid value is an alphanumeric string with a maximum of 5 characters.

QYEAR The system value that specifies the last 2 digits for the year. The valid value is an integer from 0 - 99.

TCP/IP Logical Interface attributes

Use the TCP/IP interface attributes to monitor the status and details for the logical TCP/IP interfaces, including IPv4 and IPv6 TCP/IP versions. TCP/IP interface attributes are sampled attributes in the operational areas of communications and configuration.

Note: Unless TCP/IP is active on the monitored system, an error message is issued.

Automatically Started Indicates whether the interface is started automatically when the TCP/IP stack is activated. Valid entries are as follows:

- NO - This interface is not started automatically.
- YES - This interface is started automatically.

Change Date The date of the most recent change to this interface in the dynamic tables used by the TCP/IP protocol stack. It is returned as 8 characters in the form YYYYMMDD, where YYYY is the year, MM is the month, and DD is the day.

Change Time The time of the most recent change to this interface in the dynamic tables used by the TCP/IP protocol stack. It is returned as 6 characters in the form HHMMSS, where HH is the hour, MM is the minutes, and SS is the seconds.

Change Status The status of the most recent change to this interface in the dynamic tables that the TCP/IP protocol stack uses. The following values are valid:

Value	Description
NA (0)	Not applicable for IPv6 interfaces
Add interface 1)	Add interface request processed
Change interface (2)	Change interface request processed
Start interface (3)	Start interface request processed
End interface (4)	End interface request was processed

Host Address Host portion of the internet address. It is in dotted decimal notation for IP version 4, as determined by the subnet mask specified for this interface. For IP version 6 it is in address format, as determined by the prefix length configured for this interface. This alphanumeric string is up to 48 characters long.

Internet Address The internet address, in dotted decimal notation, of the interface. This alphanumeric string is up to 48 characters long.

Line Description Name of the communications line description that identifies the physical network associated with an interface. This alphanumeric string is up to 12 bytes long. The following values are special:

Value	Description
*IPI	This interface is used by Internet Protocol (IP) over Internetwork Packet Exchange (IPX). Note that as of OS/400 V5R2, IP over IPX is no longer supported.
*IPS -	This interface is used by Internet Protocol (IP) over SNA.
*LOOPBACK	For this loopback interface, processing associated with a loopback interface does not extend to a physical line.
*OPC	This interface is attached to the optical bus (OptiConnect).
*VIRTUALIP	The virtual interface is a interface that does not have a circuit. It is used with the associated local interface (LCLIFC) when adding standard interfaces.

Line Type Type of line used by an interface. The following link protocols are supported:

Note: TRLAN, FR, ASYNC, PPP, WLS, X.25, DDI, TDLC, L2TP and IPv6 Tunneling Line values are no longer supported.

Line type	Number	Description
ASYNC	4	Asynchronous communications protocol.
DDI	8	Distributed Data Interface protocol.
ELAN	1	Ethernet local area network protocol.
Error	-3	This value is displayed if any system errors other than those for *NOTFND are received while trying to determine the link type for an interface.
FR	3	Frame relay network protocol.
IPv6_Tunneling	11	Any kind of IPv6 over IPv4 tunnel.
L2TP	10	Layer Two-Tunneling Protocol. (Virtual PPP)
None	-2	Line is not defined. This is used for the following interfaces: *LOOPBACK, *VIRTUALIP, *OPC. There is no line type value for these interfaces.
Not_Found	-4	Not found. This value is displayed if the line description object for this interface cannot be found.
Other	-1	One of: IPI - An Internet Protocol (IP) over Internetwork Pack Exchange (IPX) interface. IPS - An Internet Protocol (IP) over SNA interface. PPPoE - Point-to-Point over Ethernet protocol. Note: As of OS/400 V5R2, IP over IPX is no longer supported.
PPP	5	Point-to-point protocol.
TDLC	9	Twinaxial Datalink Control. Used for TCP/IP over Twinax.
TRLAN	2	Token-ring local area network protocol.
WLS	6	Wireless local area network protocol.

X.25	7	X.25 protocol

Local Interface The internet address, in dotted decimal notation, of the local interface that has been associated with this interface. This alphanumeric string is up to 16 characters long. NONE is a special value indicating that no association has been made between this interface and another local interface.

Network Address Internet address, in dotted decimal notation, of the IP network or subnetwork to which the interface is attached. This alphanumeric string is up to 16 characters long.

Network Name The complete 24-character name of the network that this interface is a part of. This alphanumeric string is up to 24 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Status Current status of this logical interface. The following values are valid:

Status	Value	Description
0	Inactive	The interface has not been started.
1	Active	The interface has been started and is running.
2	Starting	The system is processing the request to start this interface.
3	Ending	The system is processing the request to end this interface.
4	RCYPND	An error with the physical line associated with this interface was detected by the system. The line description associated with this interface is in the recovery pending (RCYPND) state.
5	RCYCNL	A hardware failure has occurred and the line description associated with this interface is in the recovery canceled (RCYCNL) state.
6	Failed	The line description associated with this interface has entered the failed state.
7	Failed (TCP)	An error was detected in the IBM TCP/IP Vertical Licensed Internal Code.
8	DOD	Point-to-Point Dial-on-Demand.

Subnet Mask The subnet mask for the network, subnet, and host address fields of the internet address, in dotted decimal notation, that defines the subnetwork for an interface. This alphanumeric string is up to 16 characters long.

Type The interface type. The following interface types are valid for IPv4 interfaces:

- Broadcast_capable (40)
- Non-broadcast_capable (41)
- Unnumbered_network (42)

For IPv6 the valid interfaces types are:

- Unicast (61)
- Multicast (62)
- Anycast (63)

TCP/IP Service attributes

Use the i5/OS TCP/IP service attributes to monitor the status and details for the TCP/IP services, for versions IPv4 and IPv6 of TCP/IP. The i5/OS TCP/IP service attributes are sampled attributes in the operational areas of communications and configuration.

Note:
TCP/IP must be active on the monitored system. If TCP/IP is not active on the monitored system, an error message is issued.

Alias 1 The first alternative name for the service. This alphanumeric string consists of up to 32 characters.

Alias 2 The second alternative name for the service. This alphanumeric string consists of up to 32 characters.

Alias 3 The third alternative name for the service. This alphanumeric string consists of up to 32 characters.

Alias 4 The fourth alternative name for the service. This alphanumeric string consists of up to 32 characters.

Name The name of the TCP/IP service. This alphanumeric string consists of up to 32 characters.

Origin node The managed system name. The form should be *hostname*:*agent_code*.

Examples include spark:KA4 or deux.raleigh.ibm.com:KA4.

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.

Port The port number assigned to the service. Valid values are 1-65535.

Protocol A character string that contains the name of the protocol that the service is using. This alphanumeric string consists of up to 32 characters.

State The connection state for the service. The following values for connection state are valid:

- Listen - Waiting for a connection request from any remote host.
- SYN-sent - Waiting for a matching connection request after having sent connection request.
- SYN-received - Waiting for a confirming connection request acknowledgement.
- Established - The normal state in which data is transferred.
- FIN-wait-1 - Waiting for the remote host to acknowledge the local system request to end the connection.

- FIN-wait-2 - Waiting for the remote host request to end the connection.
- Close-wait - Waiting for an end connection request from the local user.
- Closing - Waiting for an end connection request acknowledgement from the remote host.
- Last-ACK - Waiting for the remote host to acknowledge an end connection request.
- Time-wait - Waiting to allow the remote host enough time to receive the local system's acknowledgement to end the connection.
- Closed - The connection has ended.
- Unknown - State value not supported by protocol.
- *UDP - The connection is using the stateless UDP protocol.
- Not_Started - The service is not currently connected.

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 upon 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 11 on page 144 provides the following information required to calculate disk space for the Monitoring Agent for i5/OS:

- *DB table name* is the table name as it would appear in the warehouse database, if the attribute group is configured to be written to the warehouse.
- *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 11. Capacity planning for historical data logged by component i5

DB table name	Attribute group	Bytes per instance (agent)	Database bytes per instance (warehouse)	Aggregate bytes per instance (warehouse)
KA4APPN	OS400_APPN_Topology	177	183	259
KA4ACCTJ	OS400_Acct_Jrn	210	233	477
KA4ALERT	OS400_Alert	189	201	277
KA4ASYNC	OS400_Comm_Async	128	153	292
KA4BSYNC	OS400_Comm_Bisync	132	170	360
KA4ENET	OS400_Comm_Ethernet	136	187	377
KA4SDLC	OS400_Comm_SDLC	144	221	564
KA4TKRNG	OS400_Comm_Token_Ring	136	187	428
KA4X25	OS400_Comm_X25	148	154	464
KA4CTLD	OS400_Controller	116	114	151
KA4DBMBR	OS400_DB_Member	173	180	412
KA4DEVD	OS400_Device	162	165	241
KA4DISK	OS400_Disk_Unit	202	158	468
KA4PFIOP	OS400_I/O_Processor	203	161	351
KA4PFJOB	OS400_Job	339	429	1063
KA4JOBQ	OS400_Job_Queue	136	136	212
KA4LIND	OS400_Line	116	114	151
KA4MSG	OS400_Message	2332	2275	2312
KA4NETA	OS400_Network	560	570	685
KA4OBJ	OS400_Object	398	439	605
KA4SJAJ	OS400_Security_Jrn_AuditJrn	138	119	156
KA4SJAF	OS400_Security_Jrn_AuthFail	166	151	188
KA4SJCA	OS400_Security_Jrn_ChgAuth	170	162	199
KA4SJOW	OS400_Security_Jrn_ChgOwner	158	140	177
KA4SJCP	OS400_Security_Jrn_ChgUserProf	131	118	155
KA4SJJD	OS400_Security_Jrn_JobDesc	140	120	157
KA4SJNA	OS400_Security_Jrn_Network	620	600	637
KA4SJPW	OS400_Security_Jrn_Password	161	141	178
KA4SJPS	OS400_Security_Jrn_ProfSwap	149	131	168
KA4SJPA	OS400_Security_Jrn_ProgAdopt	140	120	157
KA4SJRJ	OS400_Security_Jrn_RestoreJob	140	120	157
KA4SJRP	OS400_Security_Jrn_RestoreProg	140	120	157
KA4SJSV	OS400_Security_Jrn_SYSVAL	620	600	637
KA4POOL	OS400_Storage_Pool	172	211	725
KA4SBS	OS400_Subsystem	152	151	344
KA4SYSTS	OS400_System_Status	160	328	1145
KA4SVAL	OS400_System_Values	173	180	217
KA4SVACT	OS400_System_Values_Acct	413	418	650

Table 11. Capacity planning for historical data logged by component i5 (continued)

DB table name	Attribute group	Bytes per instance (agent)	Database bytes per instance (warehouse)	Aggregate bytes per instance (warehouse)
KA4SVDEV	OS400_System_Values_Device	122	119	156
KA4SVIPL	OS400_System_Values_IPL	110	111	148
KA4SVPRF	OS400_System_Values_Perf	175	183	220
KA4SVPRB	OS400_System_Values_Prob	116	113	150
KA4SVUSR	OS400_System_Values_User	615	627	664
KA4ASP	i5OS_Auxiliary_Storage_Pool	152	208	488
KA4DISKI5	i5OS_Disk	172	231	370
KA4DISTQ	i5OS_Distribution_Queue	164	172	287
KA4HISTLOG	i5OS_History_Log	936	945	982
KA4IFSOBJ	i5OS_Integrated_File_System_Object	3246	3290	3507
KA4JOBLOG	i5OS_Job_Log	956	967	1004
KA4MGTCNT	i5OS_Management_Central	1560	1592	1668
KA4MISC	i5OS_Miscellaneous	380	386	423
KA4NETSRVR	i5OS_Net_Server	168	176	213
KA4NWI	i5OS_Network_Interface	120	118	155
KA4NWS	i5OS_Network_Server	120	118	155
KA4OUTPUTQ	i5OS_Output_Queue	760	786	877
KA4SYSSTAT	i5OS_System_Statistics	148	157	404
KA4TCPINT	i5OS_TCPIP_Logical_Interface	308	317	354
KA4TCPSRVC	i5OS_TCPIP_Service	292	295	332

For more information about historical data collection, see the *IBM Tivoli Monitoring Administrator's Guide*.

Chapter 6. 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 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 the Monitoring Agent for i5/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. It is best not to edit these situations and save them since software updates might write over any of the changes that you make to these situations. Instead, clone the situations that you want to change to suit your enterprise.

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

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 alphabetically:

OS400_Address_Critical

Raises an alert if the OS400_ASP_Warning, OS400_Perm_Address_Warning, or the OS400_Temp_address_Warning situations raises an alert.

The formula for this situation is:

```
SIT(OS400_Perm_Addresses_Warning) == True OR SIT(OS400_System_ASP_Warning) == True
 OR SIT(OS400_Temp_Addresses_Warning) == True
```

OS400_ASP_Nearing_Capacity

Monitors for an Auxiliary Storage Pool (ASP) storage capacity filling beyond a comfortable threshold. A warning alert is raised if the default threshold of 80 percent of capacity is exceeded.

The formula for this situation is:

```
i5OS_Auxiliary_Storage_Pool.Utilization Percent >= 80.0
```

OS400_ASP_Overflow_Warning

Monitors for an Auxiliary Storage Pool (ASP) that was full and overflowed into the system ASP. Object allocations directed into the user ASP were directed instead into the system ASP. The ASP that overflowed might now have available capacity if storage was freed after the overflow occurred.

The formula for this situation is:

```
i5OS_Auxiliary_Storage_Pool.Overflow Storage > 0 AND i5OS_Auxiliary_
Storage_Pool.Status == 'VARIED ON'
```

OS400_Aux_Stor_Near_Guidelines

Monitors the total auxiliary storage capacity for usage that is approaching its guideline value. By default, the guideline for maximum storage usage is 90 percent. This situation triggers at 80 percent. The auxiliary storage capacity is the total of all basic ASP and active independent ASP capacities.

The formula for this situation is:

```
OS400_System_Status.% Aux Storage Used >= 80.0
```

OS400_Aux_Stor_Over_Guidelines

Monitors the total auxiliary storage capacity for usage beyond its guideline value. By default, this situation triggers at the guideline for maximum storage usage of 90 percent. The auxiliary storage capacity is the total of all basic ASP and active independent ASP capacities.

The formula for this situation is:

```
OS400_System_Status.% Aux Storage Used >= 90.0
```

OS400_Comm_IOP_Util_Warning

Monitors the total IOP processor time that was used by communications tasks during the monitor interval. A warning alert is sent when the level is equal to or greater than 25 percent. This situation can signal you to potential slow-downs when there is excess traffic on communications lines.

The formula for this situation is:

```
OS400_I/O_Processor.Comm Percent >= 25.0
```

OS400_Communication_Line_Failed

Monitors for messages that indicate the failure of a communications line. The situation raises an alert when either of these messages are reported to QSYSOPR. This predefined situation was supplied with earlier releases with the name OS400_Communications_Line_Failed, which was too long for a valid situation name. If you customized the previous version you will need to make the same changes to the new version named OS400_Communication_Line_Failed. The previous version of the situation will not successfully run on this release and should be deleted using the Situation Editor.

- CPA58CC (line failure probably caused by a hardware problem)
- CPA58CD (line failure probably caused by a communications subsystem problem)

The formula for this situation is:

```
OS400_Message.ID == 'CPA58CC' OR OS400_Message.ID == 'CPA58CD'
```

OS400_CPU_Guidelines_Warning

Monitors the overall CPU utilization and checks if it is over default guidelines. The guideline thresholds are based on the processing capacity in use. The following values are defaults:

- 85 percent for less than or equal to one processor
- 88 percent for more than one and less than or equal to two processors
- 91 percent for more than two and less than or equal to three processors
- 95 percent for more than three processors

The formula for this situation is:

```
( OS400_System_Status.CPU Percent >= 85.0 AND OS400_System_Status.Processing
Capacity <= 1.00 )
OR ( OS400_System_Status.CPU Percent >= 88.0 AND OS400_System_Status.Processing
Capacity > 1.00 AND OS400_System_Status.Processing Capacity <= 2.00 )
OR ( OS400_System_Status.CPU Percent >= 91.0 AND OS400_System_Status.Processing
Capacity > 2.00 AND OS400_System_Status.Processing Capacity <= 3.00 )
OR ( OS400_System_Status.CPU Percent >= 95.0 AND
OS400_System_Status.Processing Capacity > 3.00 )
```

OS400_CPU_Util_Warning

Monitors for extended periods of high CPU utilization. A warning alert is sent when the usage is equal to or greater than 95 percent. By recognizing when the CPU reaches this threshold level, you can detect and further prevent serious slow downs in your operations. Extended or repeated occurrences might indicate the need to submit jobs during off-peak hours or obtain additional CPU resources.

The formula for this situation is:

```
OS400_System_Status.CPU Percent => 95.0
```

OS400_Disk_Capacity_Critical

Monitors for potential disk capacity problems and raises a critical alert when usage of an individual disk unit is equal to or greater than 90 percent. This situation can help you avoid lost or corrupted data caused by lack of space.

The formula for this situation is:

```
AVG(OS400_Disk_Unit.Percent Used) >= 90
```

OS400_Disk_IOP_Util_Warning

Monitors for the percentage of IOP processor time that was used by disk tasks during the monitor interval. A warning alert occurs when the disk IOP processor time is equal to or greater than 25 percent.

The formula for this situation is:

```
OS400_I/O_Processor.Disk Percent >= 25.0
```

OS400_Disk_Mirroring_Not_Active

Monitors for active disk units that are configured for mirroring but are not actively being mirrored.

The formula for this situation is:

```
i5OS_Disk.Mirror Status != NA AND i5OS_Disk.Status != 'Not configured'
AND i5OS_Disk.Mirror Status != Active
```

OS400_Disk_Util_Critical

Tracks the percentage of time the actuator for the disk is busy during the monitor interval and raises a critical warning when usage is greater than or equal to 60 percent. Extremely high disk utilization can negatively impact system performance and cause unpredictable interruptions to system operations.

The formula for this situation is:

```
OS400_Disk_Unit.Percent Busy >= 60
```

OS400_Disk_Util_Warning

Monitors the percentage of time the actuator for the disk is busy during the monitor interval and raises a warning alert when usage is greater than or equal to 40 percent. High disk utilization is a possible cause of poor system performance.

The formula for this situation is:

```
OS400_Disk_Unit.Percent Busy >= 40
```

OS400_Interactive_Feature_CPU

Monitors the percent of the interactive CPU feature that is being used by interactive jobs. This situation triggers at the default value of 90 percent.

The formula for this situation is:

```
OS400_System_Status.% Interactive Limit >= 90.0
```

OS400_Interactive_Jobs_CPU_High

Watches for interactive jobs that are using 20 percent or more of system CPU time. Using this amount or more of processor time limits the amount available for other jobs. By identifying jobs requiring large CPU time usage, you can suggest that these jobs be run during off-peak hours and/or in batch mode.

The formula for this situation is:

```
OS400_Job.Type == '*INT' AND OS400_Job.CPU Percent >= 20.0
```

OS400_Job_AvgResponse_Time_High

Watches interactive jobs for periods of poor response time. Using this situation, you can determine the causes and redirect jobs to different queues or submit them for processing at different time intervals. This predefined situation was supplied with earlier releases with the name OS400_Job_Avg_Response_Time_High which was too long for a valid situation name. If you customized the previous version you will need to make the same changes to the new version named OS400_Job_AvgResponse_Time_High. The previous version of the situation will not successfully run on this release and should be deleted using the Situation Editor.

The formula for this situation is:

```
OS400_Job.Type == '*INT' AND AVG(OS400_Job.Response Time) >= 5.0
```

OS400_Job_Queue_Not_Active

Monitors for job queues that are not active but have jobs queued and ready to run. The queued jobs do not run until the job queue is active.

The formula for this situation is:

```
OS400_Job_Queue.Number Jobs >= 1 AND OS400_Job_Queue.Status != 'RELEASED'
```

OS400_Job_Queue_Not_Assigned

Monitors for job queues that are not assigned to any subsystem but have jobs queued and ready to run. The queued jobs do not run until the job queue is assigned to a subsystem.

The formula for this situation is:

```
OS400_Job_Queue.Number Jobs >= 1 AND OS400_Job_Queue.Subsystem == ''
```

OS400_Management_Central_Events

Monitors for any events that have been created by i5/OS Management Central monitors since this situation started running. The Management Central monitors create events that are based on user-defined thresholds and values for system statistics, files, jobs, message queues, and Business to Business activity. The monitors are created and managed using the i5/OS Navigator graphical user interface.

The formula for this situation is:

```
COUNT(OS400_Management_Central_Events.ORIGINNODE') > 0
```

OS400_Network_Attribute_Changed

Raises an alert when any changes to network attributes are logged in the audit journal. This is useful for alerting you to changes that may affect or compromise the security of your system and/or network. Journaling must be active on your i5/OS system to run this situation. You must also specify a value for Entry Type.

The formula for this situation is:

```
OS400_Security_Jrn_AuditJrn.Entry Type == 'NA'
```

OS400_OMA_Message_Log

Monitors for messages arriving in QAUTOMON/KMSOMLOG, which is the IBM Tivoli Monitoring: i5/OS Agent message log. This situation allows you to view messages arriving that are related to IBM Tivoli Monitoring: i5/OS Agent operations. You can modify the situation to monitor for specific messages that require your attention.

The formula for this situation is:

```
(OS400_Message.Message Queue Library == 'QAUTOMON'
AND OS400_message.Message Queue == 'KMSOMLOG' AND
OS400_Message.ID == 'CNB7002')
OR (OS400_Message.Message Queue Library == 'QAUTOMON' AND
OS400_Message.Message Queue == 'KMSOMLOG' AND OS400_Message.ID == 'CNB7007')
OR (OS400_Message.Message Queue Library == 'QAUTOMON'
AND OS400_Message.Message Queue == 'KMSOMLOG' AND OS400_Message.ID == 'CNB7008')
OR (OS400_Message.Message Queue Library == 'QAUTOMON'
AND OS400_Message.Message Queue == 'KMSOMLOG' AND OS400_Message.ID == 'CNB7025')
OR (OS400_Message.Message Queue Library == 'QAUTOMON'
AND OS400_Message.Message Queue == 'KMSOMLOG' AND OS400_Message.ID == 'CNB7026')
```

OS400_Output_Queue_No_Writer

Monitors for output queues that have no assigned writer, but do have files spooled to them and ready for processing. The spooled files cannot be processed until the appropriate writer is assigned to the output queue.

The formula for this situation is:

```
i5OS_Output_Queue.Files >= 1 AND i5OS_Output_Queue.Writers <= 0
```

OS400_Perm_Address_Warning

Monitors for the percentage (in thousandths) of the maximum possible addresses for permanent objects that have been used. A warning alert is issued when the number used is equal to or greater than 95 percent.

The formula for this situation is:

```
OS400_System_Status.Perm Address Percent Used >= 95.000
```

OS400_Pool_Faulting_Warning

Monitors for high pool faulting rates and issues a warning alert when the rate is equal to or greater than 30 percent. High pool faulting rates might indicate a need for performance tuning on your system.

The formula for this situation is:

```
OS400_Storage_Pool.Total Fault >= 30
```

OS400_Pool_Transitions_High

Monitors for any pool active-to-ineligible transitions. These transitions occur when a transaction does not complete during a single time slice. This situation might help to isolate performance problems. It might be necessary to adjust the system pool to improve performance and prevent thrashing.

The formula for this situation is:

```
OS400_Storage_Pool.Active to Ineligible > 0
```

OS400_Snads_Critical

Raises an alert when either of these situations raises an alert.

- OS400_Snads_Ended
- OS400_Snads_Router_Failed

The formula for this situation is:

```
If situation OS400_Snads_Ended OR situation OS400_Snads_Router_Failed
SIT(OS400_Snads_Ended) == True) OR SIT(OS400_Snads_Router_Failed) == True
```

OS400_Snads_Ended

Monitors QSYSOPR for message CPF0927, which indicates the QSNADS subsystem has ended. The QSNADS subsystem must be active for SNA distributions to work.

The formula for this situation is:

```
OS400_Message.ID == 'CPF0927' AND SCAN(OS400_Message.Data) == QSNADS
```

OS400_Snads_Job_Missing

Monitors the system or systems and raises an alert when the QROUTER job is not detected.

The formula for this situation is:

```
MISSING(OS400_Job.Name) == (QROUTER)
```

OS400_Snads_Router_Failed

Monitors for message CPC8803 (Snads Router Ended Abnormally) and raises an alert when this message is detected. This is useful for identifying potential interruptions and limitations in SNA distributions. This situation is particularly useful for early detection and correction of line problems or early intermittent hardware failures.

The formula for this situation is:

```
OS400_Message.ID == 'CPC8803'
```

OS400_System_ASP_Warning

Monitors the auxiliary storage pool use and issues a warning alert when usage is greater than or equal to 90 percent.

The formula for this situation is:

```
OS400_System_Status.System ASP Used >= 90.0000
```

OS400_System_Value_Changed

Raises an alert when any changes to system values are logged in the audit journal. This situation is useful for monitoring changes that affect how your system and operating environment are set. Journaling must be active on your i5/OS system to run this situation.

The formula for this situation is:

```
OS400_Security_Jrn_AuditJrn.Entry Type == 'SV'
```

OS400_Temp_Address_Warning

Monitors for the percentage (in thousandths) of the maximum possible addresses for temporary objects that have been used. A warning alert is sent when the number used is equal to or greater than 95 percent.

The formula for this situation is:

```
OS400_System_Status.Temp Address Percent Used >= 95.000
```

Chapter 7. Take Action commands reference

This chapter contains an overview of Take Action commands and references for detailed information about Take Action commands.

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 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.

Advanced automation uses policies to perform actions, schedule work, and automate manual tasks. A policy comprises a series of automated steps called activities that 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.

More information about Take Action commands

For more information about working with Take Action commands, see the *IBM Tivoli Monitoring User's Guide* and Appendix A, "Take Action commands," on page 163.

Predefined Take Action commands

This monitoring agent contains the following Take Action command:

Send Break Message

The following section contains a description of this Take Action command. The following information is provided:

Description
Which actions the command performs on the system to which it is sent

Arguments
List of arguments, if any, for the Take Action command with a short description and default value for each one

Destination systems
Where the command is to be run: 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 relevant notes for using the Take Action command

Send Break Message action

Processing

Sends an immediate message to one or more workstation message queues.

Arguments

MSG Specifies the text of the message. Enter a text string with a maximum of 512 characters.

TOMSGQ
Specifies one or more workstation message queues to which the break message is sent. Specify *ALLWS to send the message to all workstation message queues or specify the name of the message queue to which the break message is sent.

Destination systems

Managed system

Usage notes

For more information, see the Send Break Message (SNDBRKMSG) command in your System i documentation.

Chapter 8. Policies reference

This chapter contains an overview of policies and references for detailed information about policies.

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 following Predefined policies section and the information in that section for each individual policy.

Predefined policies

This monitoring agent contains the following predefined policies:

- OS400_Address_Critical_Message
- OS400_Comm_Critical_Message
- OS400_High_CPU_Message
- OS400_Snads_Critical_Message

OS400_Address_Critical_Message policy

When the OS400_Address_Critical situation is true, the following break message is sent:

```
Permanent, Temporary or System ASP addresses are getting full.
```

The formula for this policy is as follows:

```
IF situation OS400_Address_Critical is true then execute the take action command
SNDBRKMSG('Permanent, Temporary or System ASP addresses are getting full.')
TOMSGQ(QSYS/QCONSOLE)
```

OS400_Comm_Critical_Message policy

When the OS400_Communication_Line_Failed situation is true, the following break message is sent:

```
Communications line has failed.
```

The formula for this policy is as follows:

```
IF situation OS400_Communication_Line_Failed is true, then execute the take action
command SNDBRKMSG('Communications line has failed.') TOMSGQ(QSYS/QCONSOLE)
```

OS400_High_CPU_Message policy

When the OS400_CPU_Util_Warning situation is true, the following break message is sent:

Warning: System CPU is at *CPU_Percent*.

The formula for this policy is as follows:

```
IF situation OS400_CPU_Util_Warning is true, then execute the take action command
SNDBRKMSG('Warning: System CPU is at &OS400_System_Status.CPU_Percent.')
TOMSGQ(QSYS/QCONSOLE)
```

OS400_Snads_Critical_Message policy

When the OS400_Snads_Critical situation is true, the following break message is sent:

```
Snads is down or the router has failed.
```

The formula for this policy is as follows:

```
IF situation OS400_Snads_Critical is true, then execute the command
SNDBRKMSG('Snads is down or the router has failed.') TOMSGQ(QSYS/QCONSOLE)
```

Upgrading for warehouse summarization

The Monitoring Agent for i5/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.

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, ka4acctj.
- 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, ka4acctj_H, ka4acctj_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 12 contains a list of the time periods and the suffixes for the summary tables and views.

Table 12. Time periods and suffixes for summary tables and views

Data collection time period	Summary table suffixes	Summary view suffixes
Hourly	_H	_HV
Daily	_D	_DV
Weekly	_W	_WV
Monthly	_M	_MV

Table 12. Time periods and suffixes for summary tables and views (continued)

Data collection time period	Summary table suffixes	Summary view suffixes
Quarterly	_Q	_QV
Yearly	_Y	_YV

Table 13 shows the expansion to summary columns of some of the most commonly used attribute types.

Table 13. 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 into 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.

The following attribute groups' primary keys were changed in this release. In previous releases the primary key for each was only the ORIGINNODE attribute. Now, one or more additional attributes are included in the key.

- OS400_Security_Jrn_AuthFail
- OS400_Security_Jrn_AuditJrn
- OS400_Security_Jrn_ChgAuth
- OS400_Security_Jrn_ChgUserProf
- OS400_Security_Jrn_JobDesc
- OS400_Security_Jrn_Network
- OS400_Security_Jrn_ChgOwner
- OS400_Security_Jrn_ProgAdopt
- OS400_Security_Jrn_ProfSwap
- OS400_Security_Jrn_Password
- OS400_Security_Jrn_RestoreJob
- OS400_Security_Jrn_RestoreProg
- OS400_Security_Jrn_SYSVAL

As a result of these changes all summarizations performed before the upgrade of the Tivoli Enterprise Portal Server support files for the Monitoring Agent for i5/OS will have a NULL value for the new primary key attribute. All summarizations performed after the upgrade of the support files for the agent will have the appropriate value for key. However, there could be two sets of summarizations for a given summarization period: one set with the new primary key column value of NULL (summarizations performed before the upgrade) and another with the proper value (summarizations performed after the upgrade). The old summarization column for the attribute being changed will have a NULL value for all new summarization calculations.

Because none of the attribute groups that were changed have numeric fields and all of the fields are of type Property, there would be no summarization. The affect of these changes is not major, but is described here for your information.

Appendix A. Take Action commands

You can use simple automation, or Take Action, provided with the Monitoring Agent for i5/OS to associate an action with a situation. For example, you can specify that i5/OS lower the job priority when it detects an interactive job that is using more processing unit resource than what you have determined is reasonable. You associate this action with the situation by choosing an i5/OS command to run when CPU utilization reaches a specified percentage.

Within the Monitoring Agent for i5/OS, these actions are run under the authority of an individual user profile. Commands run from a Take Action window are always run using the QAUTOMON user profile. For actions associated with a situation you can run under the user profile of the person who created, or last modified the situation, or you can run using the QAUTOMON profile. This option is set from the i5/OS non–programmable terminal interface using the **Action user Profile** field of the CFGOMA, Config i5/OS Monitoring Agent command. The valid values are QAUTOMON or * (asterisk). If * is set, the name of the Tivoli Enterprise Portal user who created or last modified the situation is used as an i5/OS user profile name to run the reflex automation command. To be successful the user profile must exist and be enabled on the i5/OS. You should not use an IBM supplied i5/OS user profile's name for this user.

Action is taken on i5/OS using the native command-line interface. The command is specified using the Action tab that is available on the Situations window that is displayed when you are creating a situation, or in the Command field of a Take Action window. QShell commands can be used by enclosing them, separated by semicolons, in the QSH, Start QSH, command.

Replying to inquiry messages using Reflex Automation

There is a CL program (RPYMSG) that is packaged with the Monitoring Agent for i5/OS that calls the SNDRPY command to reply to a specific inquiry message.

Using the Reflex Automation feature, you can call the RPYMSG program to send replies to inquiry messages. To do this, follow these steps:

1. Create a situation to monitor for inquiry message.

   To set up a situation to automatically reply to an inquiry message, first you need to create a situation using the following message attributes:

   - OS400_Message.Type
   - OS400_Message.ID

   Specifying a value equal to 05 for type and a value equal to CPA5305 for ID, monitors for the CPA5305 inquiry message in the QSYSOPR queue in the library QSYS. (This is the default queue that is always used unless another queue and library queue are specified.) To monitor another queue, add the Message Queue Name value and the Message Queue Library Name value as predicates for this situation.

   For example, to monitor for an inquiry message with the ID CPA5305 create the following situation:

   ```
   *IF *VALUE OS400_Message.Type *EQ 05 and *VALUE OS400_Message.ID *EQ CPA5305
   ```

   CPA5305 is *Record not added. Member <member_name> is full.* This message requires either a *c* (cancel) or *i* (ignore and increment size).

2. Add Reflex Automation to reply to the messages.

   In the Situation Editor, after you have selected your situation predicates to monitor for inquiry messages, click **Action** to display the Action window. In the Action window, call the RPYMSG program using the CALL command.

   For example, specify the following command and parameters in the Action window:

   ```
   CALL QUATOMON/RPYMSG PARM('&OS400_Message.Key'
   '&OS400_Message.Message_Queue' '&OS400_Message.
   Message_Queue_Library' 'c')
   ```

   The *c* indicates the reply text to send in the reply. The reply text can be any value that is expected by this message as a reply.

   The Action window automatically puts spaces around each attribute name inside the single quotes. To use this command, you must follow these guidelines:

   - Remove the space inside the single quotes.
   - Enclose the parameters in single quotes.
   - Put a space between each parameter that is enclosed in single quotes

   Before closing the Action window, click **Advanced** and select the following options:

   Take action on each item
   The command replies to each message that is returned.

   Take action in each interval
   The command replies to each message that is returned.

   Execute the Action at each Managed Resources (by agent)
   The RPYMSG command is on the same system as the agent.

3. Customize the RPYMSG program.

   The RPYMSG program is in the QAUTOMON library on the system on which the Monitoring Agent for i5/OS is installed. You can retrieve this source and customize it by using the following command on the i5/OS command line:

   ```
   RTVCLSRC PGM(QAUTOMON/RPYMSG) SRCFILE(your_library/your_source_file)
   ```

   Where:

   your_library
   Is the library that contains the source file in which to copy the CL source

   your_source_file
   Is the name of the source file in which to copy the CL source

   The parameters for the RPYMSG program are as follows:

   - Message Key (char[10])
   - Message Queue Name (char[10])
   - Message Queue Library Name (char[10])
   - Reply Text (char[1])

Appendix B. IBM Tivoli Enterprise Console event mapping

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 14 on page 166. 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, *install_dir*/cms/TECLIB for Windows systems and *install_dir*/tables/*TEMS_hostname*/TECLIB for UNIX systems). 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.

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 Completion Code attribute from the OS400_Acct_Jrn attribute group, the event class that is sent once the situation is triggered is ITM_OS400_Acct_Jrn.

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 KA4_Base. The KA4_Base event class can be used for generic rules processing for any event from the Monitoring Agent for i5/OS.

Table 14. Overview of attribute groups to event classes and slots

Attribute group	event classes and slots
OS400_Acct_Jrn	ITM_OS400_Acct_Jrn event class with these slots: • originnode: STRING • cpu_time: REAL • transaction_time: INTEGER • transaction_number: INTEGER • database_io_operations: INTEGER • completion_code: INTEGER • job_name: STRING • user: STRING • job_number: STRING • accounting_code: STRING • date_and_time: STRING • ka4_date: STRING • time: STRING • start_date_and_time: STRING • start_time: STRING • job_type: STRING • job_type_enum: STRING
OS400_Alert	ITM_OS400_Alert event class with these slots: • originnode: STRING • id: STRING • analysis_available: STRING • analysis_available_enum: STRING • delayed: STRING • delayed_enum: STRING • held: STRING • held_enum: STRING • local: STRING • local_enum: STRING • operator_generated: STRING • operator_generated_enum: STRING • message_severity: INTEGER • message_id: STRING • description: STRING • first_cause: STRING • origin_system: STRING • problem_id: STRING • resource: STRING • resource_type: STRING • type: STRING • description_u: STRING • first_cause_u: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_APPN_Topology	ITM_OS400_APPN_Topology event class with these slots: • originnode: STRING • transgroup_number: INTEGER • netid: STRING • cpname: STRING • node_type: STRING • node_type_enum: STRING • date_and_time: STRING • ka4_date: STRING • time: STRING • node_congestion: STRING • node_congestion_enum: STRING • update_type: INTEGER • update_type_enum: STRING • transgroup_destnode_netid: STRING • transgroup_destnode_cpname: STRING • transgroup_operational: STRING • transgroup_operational_enum: STRING • transgroup_controller_name: STRING
OS400_Comm_Async	ITM_OS400_Comm_Async event class with these slots: • originnode: STRING • line_description: STRING • iop_name: STRING • utilization_percent: REAL • error_percent: REAL • iop_bus_number: INTEGER • iop_bus_number_enum: STRING • iop_bus_address: INTEGER • iop_bus_address_enum: STRING
OS400_Comm_Bisync	ITM_OS400_Comm_Bisync event class with these slots: • originnode: STRING • line_description: STRING • iop_name: STRING • utilization_percent: REAL • receive_error_percent: REAL • send_error_percent: REAL • iop_bus_number: INTEGER • iop_bus_number_enum: STRING • iop_bus_address: INTEGER • iop_bus_address_enum: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	**event classes and slots**
OS400_Controller	ITM_OS400_Controller event class with these slots: • originnode: STRING • ka4_status: INTEGER • ka4_status_enum: STRING • name: STRING • category: STRING • category_enum: STRING
OS400_DB_Member	ITM_OS400_DB_Member event class with these slots: • originnode: STRING • file: STRING • library: STRING • member: STRING • file_attribute: STRING • file_attribute_enum: STRING • source_member_type: STRING • source_file_flag: STRING • source_file_flag_enum: STRING • records_used: INTEGER • percent_delete_records: INTEGER • sql_type: STRING • sql_type_enum: STRING • increments_left: INTEGER • percent_used: INTEGER • records_unused: INTEGER
OS400_Device	ITM_OS400_Device event class with these slots: • originnode: STRING • ka4_status: INTEGER • ka_status_enum: STRING • name: STRING • category: STRING • category_enum: STRING • job_name: STRING • job_user: STRING • job_number: STRING • passthru_device: STRING • type: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Disk_Unit	ITM_OS400_Disk_Unit event class with these slots: • originnode: STRING • arm_number: STRING • drive_type: INTEGER • drive_capacity: INTEGER • average_queue_length: INTEGER • aux_storage_pool_number: INTEGER • checksum_number: INTEGER • average_service_time: INTEGER • percent_busy: INTEGER • percent_permanent_used: INTEGER • percent_used: INTEGER • iop_name: STRING • iop_bus_number: INTEGER • iop_bus_number_enum: STRING • iop_bus_address: INTEGER • iop_bus_address_enum: STRING
OS400_Comm_Ethernet	ITM_OS400_Comm_Ethernet event class with these slots: • originnode: STRING • line_description: STRING • iop_name: STRING • utilization_percent: REAL • remote_rnr_percent: REAL • local_rnr_percent: REAL • response_time_percent: REAL • iop_bus_number: INTEGER • iop_bus_number_enum: STRING • iop_bus_address: INTEGER • iop_bus_address_enum: STRING
OS400_Job_Queue	ITM_OS400_Job_Queue event class with these slots; • originnode: STRING • library: STRING • name: STRING • number_jobs: INTEGER • ka4_status: STRING • ka4_status_enum: STRING • subsystem: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Line	ITM_OS400_Line event class with these slots: • originnode: STRING • ka4_status: INTEGER • ka4_status_enum: STRING • name: STRING • category: STRING • category_enum: STRING
OS400_Message	ITM_OS400_Message event class with these slots: • originnode: INTEGER • ka4_severity: INTEGER • type: STRING • type_enum: STRING • key: STRING • message_queue: STRING • message_queue_library: STRING • send_job_name: STRING • send_user: STRING • send_job_number: STRING • select: STRING • date_and_time: STRING • ka4_date: STRING • time: STRING • data: STRING • help_data: STRING • alert_option: STRING • id: STRING • data_u: STRING • help_data_u: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Network	ITM_OS400_Network event class with these slots: • originnode: STRING • data_compression: INTEGER • intermediate_data_compression: INTEGER • max_intermediate_session: INTEGER • max_hop_count: INTEGER • addition_resistance: INTEGER • alert_backup_focal_point: STRING • alert_controller: STRING • alert_default_focal_point: STRING • alert_filter: STRING • alert_hold_count: INTEGER • alert_hold_count_enum: STRING • alert_log_status: STRING • alert_log_status_enum: STRING • alert_primary_focal_point: STRING • alert_primary_focal_point_enum: STRING • alert_request_focal_point: STRING • alert_status: STRING • alert_status_enum: STRING • ddm_request_access: STRING • default_mode: STRING • job_action: STRING • local_cpname: STRING • default_local_location_name: STRING • local_netid: STRING • message_queue: STRING • server_network_id: STRING • appn_node_type: STRING • appn_node_type_enum: STRING • output_queue: STRING • pending_system_name: STRING • client_access: STRING • current_system_name: STRING • add_to_cluster: STRING • allow_anynet: STRING • allow_hpr_tower: STRING • allow_virtual_appn: STRING • hpr_path_switch_timers: STRING • autocreate_limit: INTEGER • modem_country_id: STRING • network_server_domain: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Object	ITM_OS400_Object event class with these slots: • originnode: STRING • name: STRING • library: STRING • type: STRING • type_enum: STRING • extended_attribute: STRING • owner: STRING • compress_status: STRING • operating_system_level: STRING • license_program: STRING • ptf_number: STRING • save_command: STRING • save_device_type: STRING • save_device_type_enum: STRING • save_file: STRING • save_library: STRING • true_size: INTEGER • create_date_and_time: STRING • create_date: STRING • create_time: STRING • change_date_and_time: STRING • change_date: STRING • change_time: STRING • save_date_and_time: STRING • save_date: STRING • save_time: STRING • restore_date_and_time: STRING • restore_date: STRING • restore_time: STRING • last_used_date_and_time: STRING • last_used_date: STRING • last_used_time: STRING • use_reset_date_and_time: STRING • use_reset_date: STRING • percent_days_used: INTEGER • use_reset_time: STRING • size_mb: REAL

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_IO_Processor	ITM_OS400_IO_Processor event class with these slots: • originnode: INTEGER • utilization_percent: REAL • comm_percent: REAL • disk_percent: REAL • type: STRING • type_enum: STRING • name: STRING • iop_bus_number: INTEGER • iop_bus_number_enum: STRING • iop_bus_address: INTEGER • iop_bus_address_enum: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Job	ITM_OS400_Job event class with these slots: • originnode: STRING • timeslice: INTEGER • cpu_time_overall: REAL • transaction_count_overall: INTEGER • transaction_time_overall: INTEGER • cpu_time: REAL • cpu_percent: REAL • transaction_count: INTEGER • transaction_time: INTEGER • response_time_overall: REAL • response_time: REAL • synch_io: INTEGER • async_io: INTEGER • name: STRING • user: STRING • number: STRING • type: STRING • type_enum: STRING • subtype: STRING • subtype_enum: STRING • multiple_request_terminal_job: STRING • multiple_request_terminal_job_enum: STRING • s36_environment: STRING • s36_environment_enum: STRING • priority: INTEGER • pool: STRING • acct_code: STRING • function_name: STRING • function_type: STRING • job_queue: STRING • job_queue_library: STRING • job_queue_priority: STRING • message_queue: STRING • message_queue_library: STRING • acct_status: STRING • acct_status_enum: STRING • subsystem: STRING • submit_date_and_time: STRING • submit_date: STRING • submit_time: STRING • start_date_time: STRING • start_date: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	**event classes and slots**
OS400_Job (continued)	• start_time: STRING • end_status: STRING • mode: STRING • signed_on_user: STRING • signed_on_user_enum: STRING • time_active: INTEGER • time_in_system: INTEGER
OS400_Storage_Pool	ITM_OS400_Storage_Pool event class with these slots: • originnode: INTEGER • number: STRING • activity_level: INTEGER • size: INTEGER • reserved: INTEGER • database_pages: REAL • nondatabase_pages: REAL • database_fault: INTEGER • nondatabase_fault: INTEGER • total_fault: INTEGER • active_to_ineligible: INTEGER • wait_to_ineligible: INTEGER • ati_atw_ratio: REAL • wti_atw_ratio: REAL
OS400_Subsystem	ITM_OS400_Subsystem event class with these slots: • originnode: STRING • max_jobs_active: INTEGER • max_jobs_active_enum: STRING • current_jobs_active: INTEGER • number_pools: INTEGER • name: STRING • description_library: STRING • ka4_status: STRING • ka4_status_enum: STRING • pool_name: STRING • pool_name_enum: STRING • pool_activity_level: INTEGER

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Comm_SDLC	ITM_OS400_Comm_SDLC event class with these slots: • originnode: STRING • line_description: STRING • iop_name: STRING • remote_rnr_percent: REAL • local_rnr_percent: REAL • receive_error_percent: REAL • send_error_percent: REAL • controller_poll_percent: REAL • utilization_percent: REAL • iop_bus_number: INTEGER • iop_bus_address: INTEGER • iop_bus_address: INTEGER • iop_bus_address_enum: STRING
OS400_Security_Jrn_AuthFail	ITM_OS400_Security_Jrn_AuthFail event class with these slots: • originnode: STRING • violation_type: STRING • violation_type_enum: STRING • object: STRING • object_library: STRING • object_type: STRING • validation_value: STRING • validation_value_enum: STRING • job_name: STRING • user: STRING • job_number: STRING
OS400_Security_Jrn_AuditJrn	ITM_OS400_Security_Jrn_AuditJrn event class with these slots: • originnode: STRING • entry_type: STRING • job_name: STRING • user_profile: STRING • job_number: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Security_Jrn_ChgAuth	ITM_OS400_Security_Jrn_ChgAuth event class with these slots: • originnode: STRING • object_name: STRING • object_library_name: STRING • object_type: STRING • job_user: STRING • auth_list_name: STRING • objexist: STRING • objexist_enum: STRING • objmgt: STRING • objmgt_enum: STRING • objopr: STRING • objopr_enum: STRING • autlmgt: STRING • autlmgt_enum: STRING • read: STRING • read_enum: STRING • add: STRING • add_enum: STRING • update: STRING • update_enum: STRING • dlt: STRING • dlt_enum: STRING • exclude: STRING • exclude_enum: STRING • command_type: STRING • command_type_enum: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Security_Jrn_ChgUserProf	ITM_OS400_Security_Jrn_ChgUserProf event class with these slots: • originnode: STRING • user: STRING • command_type: STRING • command_type_enum: STRING • password_changed: STRING • password_changed_enum: STRING • password_expired: STRING • password_expired_enum: STRING • allobj: STRING • allobj_enum: STRING • jobctl: STRING • jobctl_enum: STRING • savsys: STRING • savsys_enum: STRING • secadm: STRING • secadm_enum: STRING • splctl: STRING • splctl_enum: STRING • service: STRING • service_enum: STRING
OS400_Security_Jrn_JobDesc	ITM_OS400_Security_Jrn_JobDesc event class with these slots: • originnode: STRING • job_description: STRING • old_user: STRING • new_user: STRING
OS400_Security_Jrn_Network	ITM_OS400_Security_Jrn_Network event class with these slots: • originnode: STRING • old_attribute_value: STRING • changed_attribute: STRING • new_attribute_value: STRING
OS400_Security_Jrn_ChgOwner	ITM_OS400_Security_Jrn_ChgOwner event class with theses slots: • originnode: STRING • object_name: STRING • object_library: STRING • object_type: STRING • old_owner: STRING • new_owner: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	**event classes and slots**
OS400_Security_Jrn_ProgAdopt	ITM_OS400_Security_Jrn_ProgAdopt event class with these slots: • originnode: STRING • program_name: STRING • program_library: STRING • owner: STRING
OS400_Security_Jrn_ProfSwap	ITM_OS400_Security_Jrn_ProfSwap event class with these slots • originnode: STRING • entry_type: STRING • entry_type_enum: STRING • user_profile: STRING • source_location: STRING • old_target: STRING • new_target: STRING
OS400_Security_Jrn_Password	ITM_OS400_Security_Jrn_Password event class and these slots: • originnode: STRING • violation_type: STRING • violation_type_enum: STRING • job_user: STRING • device_name: STRING
OS400_Security_Jrn_RestoreJob	ITM_OS400_Security_Jrn_RestoreJob event class with these slots: • originnode: STRING • job_description: STRING • job_description_library: STRING • user: STRING
OS400_Security_Jrn_RestoreProg	ITM_OS400_Security_Jrn_RestoreProg event class with these slots: • originnode: STRING • program: STRING • program_library: STRING • program_owner: STRING
OS400_Security_Jrn_SYSVAL	ITM_OS400_Security_Jrn_SYSVAL event class with these slots: • originnode: STRING • system_name: STRING • new_value: STRING • old_value: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_System_Values_Acct	ITM_OS400_System_Values_Acct event class with these slots: • originnode: STRING • qactjob: INTEGER • qadlactj: INTEGER • qadlspla: INTEGER • qadltotj: INTEGER • qbasactlvl: INTEGER • qabnormsw: STRING • qabnormsw_enum: STRING • qacglvl: STRING • qacglvl_enum: STRING • qaudctl: STRING • qaudctl_enum: STRING • qaudendacn: STRING • qaudendacn_enum: STRING • qaudlvl: STRING •
OS400_System_Values	ITM_OS400_System_Values event class with these slots: • qautovrt: INTEGER • qbaspool: INTEGER • originnode: STRING • qrmtsign: STRING • qrmtsign_enum: STRING • qupsmsgq: STRING • qrclsplstg: INTEGER • qsfwerrlog: STRING • qsfwerrlog_enum: STRING • qdscjobitv: INTEGER • qsrlnbr: STRING • qpwdexpitv: INTEGER • qpwdexpitv_enum: STRING • qmodel: STRING • qsecurity: STRING • qsecurity_enum: STRING • qpwrrstipl: STRING • qpwrrstipl_enum: STRING • qautocfg: STRING • qautocfg_enum: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_System_Values_Device	ITM_OS400_System_Values_Device event class with these slots: • originnode: STRING • qdevnaming: STRING • qdevnaming_enum: STRING • qdevrcyacn: STRING • qdevrcyacn_enum: STRING
OS400_System_Values_IPL	ITM_OS400_System_Values_IPL event class with these slots: • originnode: STRING • qrmtipl: STRING • qrmtipl_enum: STRING • qipldattim: STRING • qiplsts: STRING • qiplsts_enum: STRING • qipltype: STRING • qipltype_enum: STRING • qabnormsw: STRING • qabnormsw_enum: STRING • qpwrrstipl: STRING • qpwrrstipl_enum: STRING
OS400_System_Values_Prob	ITM_OS400_System_Values_Prob event class with these slots: • originnode: STRING • qprbhlditv: INTEGER • qprbftr: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_System_Values_Perf	ITM_OS400_System_Values_Perf event class with these slots: • originnode: STRING • qtotjob: INTEGER • qhstlogsiz: INTEGER • qhstlogsiz_enum: STRING • qmaxactlvl: INTEGER • qmaxactlvl_enum: STRING • qmchpool: INTEGER • qsrvdmp: STRING • qstrprtwtr: STRING • qstrprtwtr_enum: STRING • qstruppgm: STRING • qstruppgm_enum: STRING • qtsepool: STRING • qtsepool_enum: STRING • qinactitv: INTEGER • qinactitv_enum: STRING • qinactmsgq: STRING • qinactmsgq_enum: STRING • qmaxsgnacn: STRING • qmaxsgnacn_enum: STRING • qmaxsign: INTEGER • qmaxsign_enum: STRING • qpfradj: STRING • qpfradj_enum: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_System_Values_User	ITM_OS400_System_Values_User event class with these slots: • originnode: STRING • qccsid: INTEGER • qsecond: INTEGER • qsyslibl: STRING • qtime: STRING • qupsdlytim: STRING • qupsdlytim_enum: STRING • qusrlibl: STRING • qutcoffset: STRING • qyear: INTEGER • qchrid: STRING • qcmnrcylmt: STRING • qcntryid: STRING • qctlsbsd: STRING • qdate: STRING • qdatfmt: STRING • qday: INTEGER • qhour: INTEGER • qminute: INTEGER • qmonth: INTEGER

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	**event classes and slots**
OS400_System_Status	ITM_OS400_System_Status event class with these slots: • originnode: STRING • cpu_percent: REAL • total_job_count: INTEGER • perm_address_percent_used: REAL • temp_address_percent_used: REAL • system_asp_used: REAL • pct__uncapped_cpu: REAL • pct__uncapped_cpu_enum: STRING • pct__shared_processors: REAL • pct__shared_processors_enum: STRING • pct__interactive_cpu: REAL • pct__interactive_limit: REAL • pct__database_cpu: REAL • pct__database_cpu_enum: STRING • pct__secondary_work_cpu: REAL • processing_capacity: REAL • pct__aux_storage_used: REAL • partition_id: INTEGER • main_storage_size: INTEGER • active_jobs: INTEGER • pct__maximum_jobs: REAL • up_time: INTEGER • up_time_days: STRING
OS400_Comm_Token_Ring	ITM_OS400_Comm_Token_Ring event class with these slots: • originnode: STRING • line_description: STRING • iop_name: STRING • utilization_percent: REAL • remote_rnr_percent: REAL • local_rnr_percent: REAL • response_time_percent: REAL • iop_bus_number: INTEGER • iop_bus_number_enum: STRING • iop_bus_address: INTEGER • iop_bus_address_enum: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
OS400_Comm_X25	ITM_OS400_Comm_X25 event class with these slots: • originnode: STRING • line_description: STRING • iop_name: STRING • send_utilization_percent: INTEGER • receive_utilization_percent: INTEGER • average_utilization_percent: INTEGER • remote_rnr_percent: INTEGER • local_rnr_percent: INTEGER • send_error_percent: INTEGER • receive_error_percent: INTEGER • iop_bus_number: INTEGER • iop_bus_number_enum: STRING • iop_bus_address: INTEGER • iop_bus_address_enum: STRING
i5OS_Auxiliary_Storage_Pool	ITM_i5OS_Auxiliary_Storage_Pool event class with these slots: • originnode: STRING • number: INTEGER • name: STRING • capacity: INTEGER • utilization_percent: REAL • protected_capacity: INTEGER • protected_used_percent: REAL • unprotected_capacity: INTEGER • unprotected_used_percent: REAL • overflow_storage: INTEGER • number_of_disk_units: INTEGER • system_storage_percent: REAL • type: INTEGER • type_enum: STRING • ka4_status: INTEGER • ka4_status_enum: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
i5OS_TCPIP_Logical_Interface	ITM_i5OS_TCPIP_Logical_Interface event class with these slots: • originnode: STRING • internet_address: STRING • subnet_mask: STRING • line_description: STRING • line_type: INTEGER • line_type_enum: STRING • ka4_status: INTEGER • ka4_status_enum: STRING • local_interface: STRING • host_address: STRING • network_address: STRING • network_name: STRING • type: INTEGER • type_enum: STRING • automatically_started: INTEGER • automatically_started_enum: STRING • change_date: STRING • change_time: STRING • change_status: INTEGER • change_status_enum: STRING
i5OS_TCPIP_Service	ITM_i5OS_TCPIP_Service event class with these slots: • originnode: STRING • name: STRING • port: INTEGER • protocol: STRING • state: INTEGER • state_enum: STRING • alias_1: STRING • alias_2: STRING • alias_3: STRING • alias_4: STRING
i5OS_Network_Interface	ITM_i5OS_Network_Interface event class with these slots: • originnode: STRING • name: STRING • category: STRING • ka4_status: INTEGER • ka4_status_enum: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
i5OS_Network_Server	ITM_i5OS_Network_Server event class with these slots: • originnode: STRING • name: STRING • category: STRING • ka4_status: INTEGER • ka4_status_enum: STRING
i5OS_System_Statistics	ITM_i5OS_System_Statistics event class with these slots: • originnode: STRING • batch_jobs_ending: INTEGER • batch_jobs_ended_with_output_waiting: INTEGER • batch_jobs_held_on_job_queue: INTEGER • batch_jobs_held_while_running: INTEGER • batch_jobs_on_held_job_queue: INTEGER • batch_jobs_on_unassigned_job_queue: INTEGER • batch_jobs_running: INTEGER • batch_jobs_waiting_on_messages: INTEGER • batch_jobs_waiting_to_run: INTEGER • users_signed_on: INTEGER • users_temporarily_signed_off: INTEGER • users_suspended_by_system_request: INTEGER • users_suspended_by_group_jobs: INTEGER • users_signed_off_with_waiting_printer_output: INTEGER

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
i5OS_Disk	ITM_i5OS_Disk event class with these slots: • originnode: STRING • unit_number: INTEGER • name: STRING • ka4_status: INTEGER • ka4_status_enum: STRING • capacity: REAL • percent_used: REAL • percent_busy: REAL • percent_busy_enum: STRING • percent_reserved: REAL • asp_number: INTEGER • parity: INTEGER • parity_enum: STRING • raid_type: INTEGER • raid_type_enum: STRING • mirror_status: INTEGER • mirror_status_enum: STRING • multipath: INTEGER • multipath_enum: STRING • compressed: INTEGER • compressed_enum: STRING • unit_type: STRING • unit_model: STRING • serial_number: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
i5OS_Output_Queue	ITM_i5OS_Output_Queue event class with these slots: • originnode: STRING • name: STRING • library: STRING • ka4_status: STRING • order: STRING • files: INTEGER • file_asp: INTEGER • file_asp_enum: STRING • separators: INTEGER • separators_enum: STRING • connection: INTEGER • connection_enum: STRING • destination: INTEGER • destination_enum: STRING • max_pages: INTEGER • published: INTEGER • published_enum: STRING • writers: INTEGER • autostart: INTEGER • writer_name: STRING • writer_status: STRING • printer: STRING • operator_controlled: STRING • data_queue: STRING • data_queue_library: STRING • display_any_file: STRING • authority: STRING • remote_system: STRING • remote_printer_queue: STRING
i5OS_History_Log	ITM_i5OS_History_Log event class with these slots: • originnode: STRING • message_id: STRING • ka4_severity: INTEGER • type: STRING • type_enum: STRING • send_job_name: STRING • send_job_user: STRING • send_job_number: STRING • date_and_time: STRING • message_file: STRING • library: STRING • text: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	event classes and slots
i5OS_Integrated_File_System_Object	ITM_i5OS_Integrated_File_System_Object event class with these slots: • originnode: STRING • name: STRING • path: STRING • size: INTEGER • size_mb: REAL • allocated_pct: REAL • links: INTEGER • access: INTEGER • type: STRING • owner: STRING • group: STRING • last_change: STRING • last_access: STRING • link_name: STRING
i5OS_Job_Log	ITM_i5OS_Job_Log event class with these slots: • originnode: STRING • message_id: STRING • ka4_severity: INTEGER • job_name: STRING • job_user: STRING • job_number: STRING • subsystem: STRING • subsystem_library: STRING • type: STRING • type_enum: STRING • date_and_time: STRING • message_file: STRING • library: STRING • text: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	**event classes and slots**
i5OS_Net_Server	ITM_i5OS_Net_Server event class with these slots: • originnode: STRING • response_time: INTEGER • file_opens: INTEGER • bytes_received: INTEGER • bytes_sent: INTEGER • password_violations: INTEGER • print_jobs: INTEGER • session_starts: INTEGER • auto_disconnects: INTEGER • disconnects: INTEGER • guest_support: INTEGER • guest_support_enum: STRING • unknown_users: INTEGER • started: STRING • reset: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	**event classes and slots**
i5OS_Management_Central	ITM_i5OS_Management_Central event class with these slots: • originnode: STRING • monitor_type: STRING • monitor_type_enum: STRING • event_time: STRING • sending_system: STRING • event_source: STRING • owner: STRING • metric: INTEGER • metric_enum: STRING • metric_value: INTEGER • operator: INTEGER • operator_enum: STRING • trigger: INTEGER • job_name: STRING • job_user: STRING • job_number: STRING • job_status: STRING • user: STRING • event_type: STRING • event_type_enum: STRING • message_id: STRING • message_severity: INTEGER • message_type: STRING • message_type_enum: STRING • message_queue: STRING • msgq_library: STRING • from_job_name: STRING • from_job_user: STRING • from_job_number: STRING • file_name: STRING • file_change_time: STRING

Table 14. Overview of attribute groups to event classes and slots (continued)

Attribute group	**event classes and slots**
i5OS_Distribution_Queue	ITM_i5OS_Distribution_Queue event class with these slots: • originnode: STRING • name: STRING • status_high: STRING • depth_high: INTEGER • send_depth_high: INTEGER • from_time_high: STRING • to_time_high: STRING • force_time_high: STRING • status_normal: STRING • depth_normal: INTEGER • send_depth_normal: INTEGER • from_time_normal: STRING • to_time_normal: STRING • force_time_normal: STRING
i5OS_Miscellaneous	ITM_i5OS_Miscellaneous event class with these slots: • originnode: STRING • processors: INTEGER • processor_speed: INTEGER • processor_speed_enum: STRING • brand: STRING • model-feature: STRING • os: STRING • vrm: STRING • host_name: STRING • manufacturer: STRING

Appendix C. Object access authority

The Monitoring Agent for i5/OS runs under the authority of the QAUTOMON user profile. The profile is created during installation with system operator user class (*SYSOPR), and has the following special authorities:

- *AUDIT Auditing authority
- *JOBCTL Job control authority
- *SAVSYS Save system authority
- *SERVICE Service authority
- *SPLCTL Spool control authority

The QAUTOMON user profile is not created with a password. This prevents anyone from signing on as QAUTOMON. Its initial menu is created as *SIGNOFF, so that if a password is assigned and someone signs on as QAUTOMON, its default action is to immediately sign off.

Since QAUTOMON does not have all object authority (*ALLOBJ) by default it cannot access every object on the system. In order to accomplish its monitoring tasks additional object access authorities are required for the agent. These include authority to call Application Programming Interface (API) programs and service programs, and authority to use commands to gather information. So during installation of the product the following authorities are granted to the QAUTOMON user profile:

- *CHANGE authority for library QUSRSYS
- *USE authority for program QSYS/QPMWKCOL
- *USE authority for program QSYS/QPMLPFRD
- *USE authority for program QSYS/QNMDRGFN
- *USE authority for program QSYS/QNMRGFN
- *USE authority for service program QSYS/QYPSSRVS
- *USE authority for service program QSYS/QYPSJNI
- *USE authority for service program QSYS/QUSRGFA1
- *USE authority for service program QSYS/QYPSCOLL
- *USE authority for command QSYS/WRKDSTQ
- *USE authority for command QSYS/DMPOBJ
- *USE authority for user profile QSYSOPR (used during History Log access)

Other object access authorities may be required for the agent, but they cannot be determined during installation. These authorities will need to be granted by you after installation. These include access to:

- Security auditing journal and receivers. Grant QAUTOMON *ALL object authority to QSYS/QAUDJRN auditing journal and to its receivers. The current receiver is shown using command WRKJRN QSYS/QAUDJRN, then option 5.
- Output Queues. Grant QAUTOMON at least *USE authority to libraries containing output queues created by product installations or user action. Output queues shipped with i5/OS should already have PUBLIC *USE authority for their containing libraries.
- Integrated File System objects. Grant QAUTOMON at least *USE authority to IFS directories and objects that have PUBLIC *EXCLUDE access authorities.

You can grant the QAUTOMON user profile all object authority (*ALLOBJ) if you want the agent to monitor every object on the system and prefer not to set individual object access authorities.

Appendix D. Monitoring Agent for i5/OS data collection

In general, the Monitoring Agent for i5/OS 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 such that the agent will not put a significant load on the system as it gathers the data.

Most of the attributes gathered by the Monitoring Agent for i5/OS come from i5/OS Application Programming Interfaces (API). The APIs are described in the i5/OS Information Center available online at web site: http://publib.boulder.ibm.com/iseries/. A few Machine Instructions (MI) are used and these are also described in the online i5/OS Information Center. When no API nor MI is available for a particular function, Command Language (CL) commands have been used. Information about the CL commands is available on the i5/OS system using the contextual help function, and is also described in the online i5/OS Information Center.

The Monitoring Agent for i5/OS maintains long running processes for the agent that communicate with the Tivoli Enterprise Management Server and the collector that drives data collection. Depending on the data to collect there are also short running processes used to access system data, data queues created to receive events from the system, and long running processes to interact with performance data gathering APIs.

The following table shows each i5/OS attribute group, the mechanism used to gather the attributes, and notes. The abbreviations used in the Collection Methods column are:

- API - Application Programming Interface
- CL - Command Language command
- DTAQ - Data queue
- HLL - High Level Language program
- MI - Machine Instruction

Table 15. Mechanisms used to gather attributes

Attribute group	Collection methods	API/MI/CL names	Notes
i5OS Auxiliary Storage Pool	MI	MATRMD, Materialize Resource Management Data	Option Hex 20
i5OS Disk	MI	MATRMD, Materialize Resource Management Data	Option Hex 22
i5OS Distribution Queue	CL	WRKDSTQ, Work with Distribution Queues	OUTPUT(*PRINT) option, then the spool file is read and deleted
i5OS History Log	HLL	_Ropen, _Rreadf, _Rclose	The history file records are accessed using high level programming language functions

Table 15. Mechanisms used to gather attributes (continued)

Attribute group	Collection methods	API/MI/CL names	Notes
i5OS Integrated File System Object	API	QlgOpendir, QlgReaddir, closedir, QlgLstat64, QlgReadlink	IFS related APIs for directories and objects
i5OS Job Log	API	QMHLJOBL, List Job Log Messages	
i5OS Management Central	API, DTAQ	QypsRegMCEvent Notifications, QypsDeregMCEvent Notifications	Qyps APIs to register and deregister a data queue which receives the events
i5OS Miscellaneous	API, MI	QWCRSVAL, Retrieve System Values; MATMATR1, Materialize Machine Attributes; gethostname	MATMATR1 for VPD
i5OS Net Server	API	QZLSLSTI, List Server Information	
i5OS Network Interface	API	QDCLCFGD, List Configuration Descriptions	
i5OS Network Server	API	QDCLCFGD, List Configuration Descriptions	
i5OS System Statistics	API	QWCRSSTS, Retrieve System Status	
i5OS TCPIP Logical Interface	API	QtocLstNetIfc, List Network Interfaces	
i5OS TCPIP Service	API	QtocLstNetCnn, List Network Connections	
OS400 Acct Jrn	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Alert	API, DTAQ	QNMDRGFN, Deregister Filter Notifications; QNMRGFN, Register Filter Notifications	
OS400 APPN Topology	API	QNMRGTI, Register APPN Topology Information	
OS400 Comm Async	API	QPMWKCOL, Work with Collector; QPMLPFRD, List Performance Data	
OS400 Comm Bisync	API	QPMWKCOL, Work with Collector; QPMLPFRD, List Performance Data	

Table 15. Mechanisms used to gather attributes (continued)

Attribute group	Collection methods	API/MI/CL names	Notes
OS400 Comm Ethernet	API	QPMWKCOL, Work with Collector; QPMLPFRD, List Performance Data	
OS400 Comm SDLC	API	QPMWKCOL, Work with Collector; QPMLPFRD, List Performance Data	
OS400 Comm Token Ring	API	QPMWKCOL, Work with Collector; QPMLPFRD, List Performance Data	
OS400 Comm X25	API	QPMWKCOL, Work with Collector; QPMLPFRD, List Performance Data	
OS400 Controller	API	QDCLCFGD, List Configuration Descriptions	
OS400 DB Member	API	QUSLMBR, List Database File Members	
OS400 Device	API	QDCLCFGD, List Configuration Descriptions	
OS400 Disk Unit	API	QPMWKCOL, Work with Collector; QPMLPFRD, List Performance Data	
OS400 I/O Processor	API	QPMWKCOL, Work with Collector; QPMLPFRD, List Performance Data	
OS400 Job	API	QGYOLJOB, Open List of Jobs; QGYGTLE, Get List Entries; QGYCLST, Close List	
OS400 Job Queue	API	QSPRJOBQ, Retrieve Job Queue Information	
OS400 Line	API	QDCLCFGD, List Configuration Descriptions	
OS400 Message	API	QMHLSTM, List Nonprogram Messages	
OS400 Network	CL	QWCRNETA, Retrieve Network Attributes	

Table 15. Mechanisms used to gather attributes (continued)

Attribute group	Collection methods	API/MI/CL names	Notes
OS400 Object	API	QUSLOBJ, List Objects	
OS400 Security Jrn AuditJrn	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn AuthFail	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn ChgAuth	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn ChgOwner	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn ChgUserProf	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn JobDesc	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn Network	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn Password	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn ProfSwap	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn ProgAdopt	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn RestoreJob	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Security Jrn RestoreProg	CL, HLL	RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	

Table 15. Mechanisms used to gather attributes (continued)

Attribute group	Collection methods	API/MI/CL names	Notes
OS400 Security Jrn	CL, HLL	SYSVAL RCVJRNE, Receive Journal Entry; Exit program to receive the entries.	
OS400 Storage Pool	API	QWCRSSTS, Retrieve System Status	
OS400 Subsystem	API	QWDRSBSD, Retrieve Subsystem Information	
OS400 System Status	API	QWCRSSTS, Retrieve System Status; MATRMD, Materialize Resource Management Data	MATRMD Option Hex 20
OS400 System Values	API	QWCRSVAL, Retrieve System Values	
OS400 System Values Acct	API	QWCRSVAL, Retrieve System Values	
OS400 System Values Device	API	QWCRSVAL, Retrieve System Values	
OS400 System Values IPL	API	QWCRSVAL, Retrieve System Values	
OS400 System Values Perf	API	QWCRSVAL, Retrieve System Values	
OS400 System Values Prob	API	QWCRSVAL, Retrieve System Values	
OS400 System Values User	API	QWCRSVAL, Retrieve System Values	

Appendix E. Problem determination

This appendix explains how to troubleshoot the IBM Tivoli Monitoring: i5/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, "Installation and Configuration of the monitoring agent," on page 7.

This appendix provides agent-specific problem determination information. See the following documents for general information about using the product:

- *IBM Tivoli Monitoring Problem Determination Guide*
- *IBM Tivoli Monitoring Administrator's Guide*
- *IBM Tivoli Monitoring User's Guide*
- *IBM Tivoli Monitoring Problem Determination Guide*

Also see "Support for problem solving" on page 220 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 16. Information to gather before contacting IBM Software Support

Information type	**Description**
Log files	Collect trace log files from failing systems. See "Configuring trace logging" on page 204 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
Messages	Messages and other information displayed on the screen
Version numbers for IBM Tivoli Monitoring	Version number of the components of the IBM Tivoli Monitoring monitoring environment.

Upload files for review to the following FTP site: `ftp.emea.ibm.com`. Log in as **anonymous** and place your files in the directory that corresponds to the IBM Tivoli Monitoring component that you use.

Built-in problem determination features

The primary troubleshooting feature in the IBM Tivoli Monitoring: i5/OS Agent is logging. *Logging* refers to the text messages and trace data generated by the IBM Tivoli Monitoring: i5/OS Agent. Messages are sent to the agent's message queue and a file is used to store trace data.

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 "Configuring trace logging" on page 204 for more information.

Problem classification

The following types of problems might occur with the IBM Tivoli Monitoring: i5/OS Agent:

- Installation and configuration
- General usage and operation
- Display of monitoring data
- Take Action commands

This appendix 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 Problem Determination Guide* for general problem determination information.

Problem determination process

Use the following process to determine the source of problems in Monitoring Agent for i5/OS:

1. View the message queue for the agent by entering the DSPOMALOG command on an i5/OS command line.
2. When you want further information about an item that you see in the message queue, view the trace logs that are described in "Configuring trace logging."
3. Some problems leave messages in the agent's job log. The agent's job log can be viewed by:
   a. Enter the command WRKUSRJOB USER(QAUTOMON) on an i5/OS command line to see the list of active and completed agent jobs. The agent jobs have the name CT_AGENT.
   b. If an agent's job in the list shows a status of ACTIVE then the job log can be viewed using option 5, Work with, then option 10, Display job log.
   c. If an agent's job in the list shows a status of OUTQ then the job log can be viewed using option 5, Work with, then option 4, Work with spooled files, then option 5, Display.
4. Some problems initiate dumps of information or print data areas for debugging purposes. These dumps and print files are saved as spool files for the QAUTOMON user profile. They can be viewed by entering the command 'WRKSPLF SELECT(QAUTOMON)' on an i5/OS command line. The names of the spool files help to indicate their contents. Some names you might see include:
   - QPJOBLOG -- job log for a completed job
   - QPRINT -- standard output from a job
   - QPSRVDMP -- dump file (possibly from DMPOBJ, Dump Object command)

Configuring trace logging

This section describes the configuration of trace logging. The member KBBENV in file QAUTOTMP/KMSPARM stores the variables for trace logging in Monitoring Agent for i5/OS. By default, trace logs are stored in the **QAUTOTMP** library.

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. See the following sections to learn how to configure and use trace logging:

- "Managing log files"
- "Targeting which modules to trace" on page 206
- "Using trace logs" on page 206

Note: The documentation refers to the RAS facility in IBM Tivoli Monitoring as ″RAS1″.

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.

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.

Managing log files

By default, trace log data goes to three files (KA4AGENT01, KA4AGENT02, and KA4AGENT03) that are defined by the following configuration variable:

```
KBB_RAS1_LOG=(QAUTOTMP/KA4AGENT01 QAUTOTMP/KA4AGENT02 QAUTOTMP/KA4AGENT03 )\
INVENTORY=QAUTOTMP/KA4RAS.INV LIMIT=5 PRESERVE=1
```

The files are used as follows:

1. The files fill with trace log data in order:
   a. The KA4AGENT01 file receives trace log data until it reaches the size of 5 MB, the default setting defined by the LIMIT=5 parameter.
   b. The KA4AGENT02 file receives trace log data until it reaches the size of 5 MB.
   c. The KA4AGENT03 file receives trace log data until it reaches the size of 5 MB.
2. Trace logging continues in the second log file, KA4AGENT02. The **PRESERVE=1** setting prevents the overwriting of the first log file.
3. When you want to troubleshoot the monitoring agent, refer to the time stamp of the three trace log files. The most recent file could be any of the three files, depending on when trace logging transferred from one file to the other.

You can modify the KBB_RAS1_LOG variable to modify logging behavior. You must ensure that QAUTOMON has sufficient authority to access the files if you use a library other than QAUTOTMP.

- **PRESERVE parameter:** You can configure logging to preserve the initial log file, which contains useful startup information. The default is 1, which means that the first log file is never overwritten when logs roll.
- **LIMIT parameter:** You can configure logging to have a different maximum size of files in MB (LIMIT).

  Note: Do not configure the LIMIT setting to be greater than 100 MB. On i5/OS, when file size reaches 100 MB, the process associated with the file is suspended, and the system sends notification to the system administrator. Monitoring stops and the file size status must be resolved manually.

Targeting which modules to trace

The type of trace messages to log and which modules to log messages for are controlled by configuration settings. By default the KBB_RAS1=ERROR configuration setting logs the trace statements for type ″Error″ in all the modules.

The modules written specifically for the i5/OS agent have names staring with ′ka4′, and modules common to agents have names starting with ′kra′, ′kbb′, ′kdc′, and others. The following setting logs all the trace statements for all the modules starting ka4 and kra.

```
KBB_RAS1=ERROR (UNIT:KA4 ALL) (UNIT:KRA ALL)
```

The ka4 and kra strings are wild cards in this statement. You can also enter the names of individual modules in a UNIT statement.

Using trace logs

Typically IBM Software Support applies specialized knowledge to analyze trace logs to determine the source of problems. However, you can view trace logs to learn some basic facts about your IBM Tivoli Monitoring environment.

Problems and workarounds

Agent problem determination

This section lists problems that might occur with agents.

This appendix provides agent-specific problem determination information. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

Unique names for monitoring components

If you have multiple instances of a monitoring agent, 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 hostname
- Agent product node type

An agent name truncation problem can occur when the network domain name is included in the network hostname portion of the agent name. For example, instead of just the hostname myhost1 being used, the resulting hostname 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.

The agent name truncation is only a problem if there is more than one monitoring agent on the same system. In this case, the agent name truncation can result in collisions between agent products attempting to register using the same truncated name value. When truncated agent names collide on the same system, this can lead to Tivoli Enterprise Monitoring Server problems with corrupted EIB tables. The agent name collision in the Tivoli Enterprise Monitoring Server might cause a registered name to be associated with the wrong product.

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 the following path:
   - **On Windows:** `*install_dir*\tmaitm6\K*product_code*CMA.INI`. For example, the product code for the Monitoring Agent for Windows OS is NT file name for is `KNTCMA.INI`.
   - **On UNIX and Linux®:** *install_dir*/tmaitm6/*product_code*.ini and *product_code*.config. For example, the file names for the Monitoring Agent for UNIX OS is `ux.ini` and `ux.config`.
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 A4, 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 KA4ENV file in the same path mentioned in the preceding row.
   - For z/OS® agents, find the **RKANPAR** library.
   - For i5/OS agents, find the **QAUTOTMP/KMSPARM** library in member **KBBENV**.
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.
   - **On UNIX and Linux:** Add the variable to the config/*product_code*.ini and to config/*product_code*.config files.
   - **On z/OS:** Add the variable to the **RKANPAR** library, member K*product_code*ENV.
   - **On i5/OS:** Add the variable to the **QAUTOTMP/KMSPARM** library in member **KBBENV**.
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.

Table 17. Agent problems and solutions

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. However, EPHEMERAL endpoints are restricted: data warehousing cannot be performed on an ephemeral endpoint.
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)″ -- for example, ″Description (Unicode)″ might support only ASCII characters.

Table 17. Agent problems and solutions (continued)

Problem	Solution
Historical reporting fails.	The location of short-term history files depends on the configuration variable CTIRA_HIST_DIR in the **QAUTOTMP/KMSPARM(KBBENV)** file. The default value is CTIRA_HIST_DIR=/QIBM/USERDATA/IBM/ITM/HIST. If you change the CTIRA_HIST_DIR variable to another directory, you must do the following to ensure success of historical data collection: • Create the directory in Integrated File System (IFS). • Give QAUTOMON read, write, and execute (*RWX) access to the new directory.
You see the following message when you select **Display Tivoli Monitoring: i5/OS Agent Log**: Function check. MCH2002 unmonitored by QNMDRGTI at statement *N instruction X'0024	This problem occurs whenever the following situations stop: • Any situation based on the APPN topology attributes • All situations, when agents lose connection to the monitoring server (In this case, all situations are automatically stopped.) These messages are generated during the cleanup process for a stopped situation. For example, in the case of APPN topology attributes, threads are used in QNMDRGTI and must be cleaned up. These messages are harmless and you can ignore them. To restore monitoring activity, restart the agent or restore connectivity with the monitoring server, as appropriate. The following excerpt shows related information from the joblog of the CT_Agent job. You can also ignore this information: Event monitor does not exist. Dump output directed to spooled file 1, job 304099/QAUTOMON/CT_AGENT created on system MINERVA on 09/05/05 13:08:35. The requested information cannot be dumped. Dump output directed to spooled file 3, job 304099/QAUTOMON/CT_AGENT created on system MINERVA on 09/05/05 13:08:37. Software problem data for QNMDRGTI has been detected. Event monitor does not exist. Function check. MCH2002 unmonitored by QNMTIXT at statement *N, instruction X'001A'.
The user account used for reflex automation commands is invalid.	QAUTOMON is the default user that is used to execute reflex automation or Take Action commands. To change this assignment, set the **Action** user profile in **Configure Tivoli Monitoring: i5/OS Agent** to different value. The valid values are QAUTOMON or a value that starts with an asterisk (*). If you set a value starting with an asterisk, like ***SIT**, the user who created the situation is used to run the reflex automation commands. To assign a user other than QAUTOMON, create a user with that name on the Tivoli Enterprise Portal. Log in using that user ID and create a situation with some action to be executed on the monitoring agent. If that situation is started and triggered, the action configured in that situation is executed under the user who created the situation.

Table 17. Agent problems and solutions (continued)

Problem	**Solution**
High CPU utilization by the CT_AGENT job.	Possible causes Check for the following problems: 1. SNTP implemented for time synchronization on System i server. This can be verified by doing the following simple test a. Add a environment variable using the following command ADDENVVAR ENVVAR('QIBM_GETTIMEOFDAY_USE_SFWCLK') VALUE('N') REPLACE(*YES) LEVEL(*SYS) b. Stop the monitoring Agent(A4) c. Signoff the System i session and sign back in. d. Verify that Environment variable QIBM_GETTIMEOFDAY_USE_SFWCLK exists using WRKENVVAR command. e. Start the monitoring Agent(A4) CPU Utilization should be normal if it is caused by SNTP . This is not a permanent solution, you must to follow the procedure to make this change only applicable to this CT_AGENT program. 2. Some situations may be causing the monitoring agent to drive more data collection. To identify such situations, a. Stop all the custom situations and uncheck "Run at startup". b. Start the monitoring agent with only product provided situations and verify the CPU utilization. c. If the CPU utilization is normal , start one situation at a time and verify the process. Continue this process for all the situations until you identify the situation that is causing the CT_AGENT job to consume high CPU. Correct the situations by changing the formula or increasing the interval to consume fewer CPU cycles.

DASD fill with *MGTCOL objects and objects in QMPGDATA library.	This can be reduced to some extent by not collecting the data as frequently as set for various types of resources other than defaults using the configuration variables in QAUTOTMP/KMSPARM(KBBENV).
	`KA4_JOB_DATA_INTERVAL=15`
	`KA4_IOP_DATA_INTERVAL=30`
	`KA4_DISK_DATA_INTERVAL=30`
	`KA4_POOL_DATA_INTERVAL=15`
	`KA4_COMM_DATA_INTERVAL=60`
	More information on these variables is provided in XREFChapter 2, "Installation and Configuration of the monitoring agent," on page 7.

Table 17. Agent problems and solutions (continued)

Problem	Solution

Monitoring Agent for i5/OS crashes with more jobs on the system or the data not displayed on Tivoli Enterprise Portal quickly.	Systems running with large number of jobs is the major cause of failures or the poor response. The following configuration variables in QAUTOTMP/KMSPARM(KBBENV) can be used to reduce the number of jobs being monitored:
	• **KA4_JOB_COUNT=20480** By default, it allocates space for 20480 jobs, can be increased to higher value on systems with more jobs.
	• **KA4_LJOB_NAME=*ALL** JOB NAME FILTER ,Any name with maximum of 10 chars.
	• **KA4_LJOB_USER=QUSER** JOB USER FILTER , Any name with maximum of 10 chars.
	• **KA4_LJOB_NBR=*ALL** JOB NUMBER FILTER , Any 6 digit number.
	• **KA4_LJOB_TYPE=*** JOB TYPE 1 char valid values * A B I M R S W X
	`* This value lists all job types.`
	`A The job is an autostart job.`
	`B The job is a batch job.`
	`I The job is an interactive job.`
	`M The job is a subsystem monitor job.`
	`R The job is a spooled reader job.`
	`S The job is a system job.`
	`W The job is a spooled writer job.`
	`X The job is the start-control-program-function (SCPF) system job.`
	• **KA4_LJOB_STS=*ACTIVE** JOB TYPE 10 char Valid Values *ACTIVE *JOBQ *OUTQ *ALL

Workspace problem determination

Table 18 shows problems that might occur with workspaces. This appendix provides agent-specific problem determination information. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

Table 18. 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 each view, you see the following Historical workspace KFWITM220E error: **Request failed during execution**.	Ensure that you configure all groups that supply data to the view. In the Historical Configuration view, ensure that data collection is started for all groups that supply data to the view.

Table 18. Workspace problems and solutions (continued)

Problem	Solution
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, "Installation and Configuration of the monitoring agent," on page 7 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 collect specific amounts and types of historical data. Be aware that historical 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.
Messages and Spool workspace does not display data.	The views based on the **Message** attribute group such as **Operator Message** view and **Managed Systems for i5/OS Logs** display the data based on the time span set for those views. By default it displays messages for last 2 hours. To change this behavior, click the Timespan icon on the left hand corner of the view on Tivoli Enterprise Portal. The time zone between System i server and Tivoli Enterprise Portal Server also affects the data collected on these views. Consider the following scenario: • Monitoring Agent for i5/OS runs on a System i server which in operating in the Pacific time zone. • The Tivoli Enterprise Portal Server runs in the Central time zone. In this scenario, the data might not be displayed in the Messages views. Change the Timespan setting accordingly to enable the Tivoli Enterprise Portal to show the data. **Note:** If you assign a Timespan of the last 24 hours, you would satisfy all time zones. However, this setting would increase the overhead if both systems are in same time zone and are slightly different.

Situation problem determination

This section provides information about both general situation problems and problems with the configuration of situations. See the *IBM Tivoli Monitoring Problem Determination Guide* for more information about problem determination for situations.

General situation problems

Table 19 on page 213 lists problems that might occur with specific situations.

Table 19. Specific situation problems and solutions

Problem	**Solution**
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.
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.
Monitoring activity requires too much disk space.	Check the RAS trace logging settings that are described in “Configuring trace logging” on page 204. For example, trace logs grow rapidly when you apply the **ALL** logging option.
Monitoring activity requires too many system resources.	Table 20 on page 215 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 appears 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 i5/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 6.1.0 or later.
Situations that you create display the severity UNKNOWN in IBM Tivoli Enterprise Console.	For a situation to have the correct severity in TEC for those situations which are not mapped, you need to ensure that an entry exists in the **tecserver.txt** file for the situation and that **SEVERITY** is specified. See the “Configuring Tivoli Enterprise Console integration” chapter in the *IBM Tivoli Monitoring Administrator’s Guide* for more information.
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.

Table 19. Specific situation problems and solutions (continued)

Problem	Solution
Security Audit journal based situations don't trigger.	QAUTOMON user needs to have sufficient authority on the journal QSYS/QAUDJRN and the current associated journal receiver for QAUDJRN. Provide *ALL authority for QAUTOMON user on QAUDJRN and the receivers associated with it. Set the system values QAUDLVL & QAUDCTL with appropriate value for the type of audit data to be journaled. DSPSECAUD/CHGSECAUD can be used to verify the current security auditing values. Make sure that journal entries with correct type are journaled to the QAUDJRN journal.
Historical data collection not working on the attributes based on OS400_Securiy_Jrn_* and short term history files are not created in /QIBM/USERDATA/IBM/ITM/HIST directory. Currently, Historical Data collection is only working for few of the OS400_Security_Jrn based journal entry types.	QAUTOMON user needs to have sufficient authority on the journal QSYS/QAUDJRN and the current associated journal receiver for QAUDJRN. Provide *ALL authority for QAUTOMON user on QAUDJRN and the receivers associated with it. Set the system values QAUDLVL & QAUDCTL with appropriate value for the type of audit data to be journaled. DSPSECAUD/CHGSECAUD can be used to verify the current security auditing values. Make sure that journal entries with correct type are journaled to the QAUDJRN journal.
Accounting Journal based situations don't trigger.	QAUTOMON user needs to have sufficient authority on the journal QSYS/QACGJRN and the current associated journal receiver for QACGJRN. Provide *ALL authority for QAUTOMON user on QACGJRN and the receivers associated with it. The system value QACGLVL need to have *JOB for account journaling to work correctly.
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 into a second buffer, this additional data is not examined, and it is not included in events sent to the Tivoli Enterprise Console server.
Situations based on APPN topology attributes don't trigger quickly.	The configuration variable KA4_COMM_SIT_INTERVAL determines the interval for APPN related situations with a default value of 3600 secs. This can be set in the file QAUTOTMP/KMSPARM member KBBENV. Setting a smaller value for this variable enables triggering of the APPN related situations quickly as required.
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_name*_forward_tbsm_event_cb.sh 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 20 on page 215 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 20 you must avoid referencing that attribute group, as suggested in this list:

- Disable the attribute group.
- Never select workspaces that reference the attribute group.
- Disable situations that reference the attribute group by using the ″Undistributed situations″ option in the Situation Editor.
- Disable 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.

See the *IBM Tivoli Monitoring User's Guide* for additional information on controlling attribute group usage.

Table 20. Performance Impact by attribute group

Attribute group	High	Medium	Low
Acct_Jrn		✓	
Alert			✓
APPN_Topology		✓	
Auxiliary Storage Pool		✓	
Comm_Async		✓	
Comm_Bisync		✓	
Comm_Ethernet		✓	
Comm_SDLC		✓	
Comm_Token_Ring		✓	
Comm_X25		✓	
Controller		✓	
Device			✓
Disk_Unit	✓		
Database_Member			✓
Distribution Queue		✓	
History Log	✓		
i5 Disk		✓	
I/O_Processor		✓	
Integrated File System Object		✓	
Job	✓		
Job Log		✓	
Job_Queue		✓	
Line			✓
Management Central		✓	
Messages	✓		
Miscellaneous			✓

Table 20. Performance Impact by attribute group (continued)

Attribute group	High	Medium	Low
Net Server		✓	
Network		✓	
Network Interface		✓	
Network Server		✓	
Object	✓		
Output Queue		✓	
Security_Jrn		✓	
Security Jrn AuditJrn		✓	
Security Jrn AuthFail		✓	
Security Jrn ChgAuth		✓	
Security Jrn ChgOwner		✓	
Security Jrn ChgUserProf		✓	
Security Jrn JobDesc		✓	
Security Jrn Network		✓	
Security Jrn Password		✓	
Security Jrn ProfSwap		✓	
Security Jrn ProgAdopt		✓	
Security Jrn RestoreJob		✓	
Security Jrn RestoreProg		✓	
Security Jrn SYSVAL		✓	
Spool_File		✓	
Storage_Pool		✓	
Subsystem		✓	
System Statistics		✓	
System_Status			✓
System_Values		✓	
System Values Acct		✓	
System Values Device		✓	
System Values IPL		✓	
System Values Perf		✓	
System Values Prob		✓	
System Values User		✓	
TCPIP Logical Interface		✓	
TCPIP Service		✓	

Problems with configuration of situations

Table 21 on page 217 lists problems that might occur with situations.

This section provides information for problem determination for agents. Be sure to consult the *IBM Tivoli Monitoring Problem Determination Guide* for more general problem determination information.

Table 21. 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 i5/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.
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 22. 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**.
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 23. 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.

Take Action command problem determination

This section lists general problems that might occur with Take Action commands. When each Take Action command runs it generates a log file.

This appendix provides agent-specific problem determination information. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

Messages for a Take Action command might consist of a long string of ″at″ symbols (@) in a pop-up message. (The **Reflex automation** Take Action command, which is configured in situations, does not have this problem.) A resolution for this problem is under construction. This problem might be resolved by the time of the product release. If you see this problem, contact IBM Software Support.

Optimizing Take Action commands

This section contains information about how you can maintain the performance of situations that use Take Action commands.

Considerations for taking action: The flow of activities specified with Take Action is controlled by the IBM Tivoli Monitoring: i5/OS Agent jobs running in the

QAUTOMON subsystem. These jobs compete for system resources along with other jobs in your system. Because of this, there might be a delay between the completion of one activity and the start of the successor activity.

If you want to minimize delays in execution of your user action choices, you can increase the priority of the IBM Tivoli Monitoring: i5/OS Agent jobs. To change the priority of jobs, use the Change Class (CHGCLS) command to change the run priority of the QAUTOMON class.

Note: Remember that increasing the priority of the IBM Tivoli Monitoring: i5/OS Agent jobs might increase the impact of situation monitoring and policy execution on other jobs in your system.

Response time for Take Action commands: Some of the Take Action commands must communicate with the jobs running in the QAUTOMON subsystem. The response time of these commands can be affected by the monitoring and automation tasks that are currently active.

Problem determination for i5/OS

Table 24 lists problems that might occur on the system or application that you are monitoring. See the *IBM Tivoli Monitoring Problem Determination Guide* for general problem determination information.

Table 24. i5/OS problems and solutions

Problem	Solution
You need to optimize performance by choosing attribute groups that have the least effect on performance.	See “Consider performance impact of each attribute group” on page 214 and “Using attribute grouping to reduce the demand for disk space.”
You need to monitor inactivity in the i5/OS files.	The QAUTOTMP library contains the temporary data collected by the IBM Tivoli Monitoring: i5/OS Agent. The library could be empty if IBM Tivoli Monitoring: i5/OS Agent has not been started. Display the library to see the current size of the temporary data.
Performance problems with the IBM Tivoli Monitoring: i5/OS Agent can take the following forms: • Long response time when working with the IBM Tivoli Monitoring: i5/OS Agent on an NPT • Long process time for activating or deactivating situations • Long process time for starting or stopping activity programs • Connection problems between the managing system and monitoring agents • Connection problems between the managing system and the Tivoli Enterprise Portal	The subsystem QAUTOMON uses the *BASE pool. Thus, you might need to tune some parameters related to the *BASE pool if you experience performance problems with the IBM Tivoli Monitoring: i5/OS Agent. Use the Work with Active Jobs (WRKACTJOB) command and look at the status of the jobs in subsystems QAUTOMON. If one or more of the jobs have status ineligible (INEL), the activity level for the pool might be too small. To avoid this, you can make one or more of these changes. • Increase the activity level of the *BASE pool. • Increase *BASE pool size. • Create another pool for the QAUTOMON jobs.

Using attribute grouping to reduce the demand for disk space

Some multiple-instance attributes can cause a very large number of sets of data to be gathered. Specifying predicates for additional attributes in the same attribute group might reduce the amount of data that needs to be collected and reduce the performance impact. You must specify key attributes for each of the following functional areas:

Accounting Journal Notification (Acct_Jrn) attributes
Specify one or more of these attributes.

- Acct_Jrn.Job_Name
- Acct_Jrn.User

File Member (DB_Member) attributes
Specify one or more of these attributes.

- DB_Member.Member
- DB_Member.File
- DB_Member.Library

Object (Object) attributes
Specify one or more of these attributes.

- Object.Library
- Object.Name
- Object.Type

Spooled file (Spool_File) attributes
Specify one or more of these attributes.

- Spool_File.Form_Type
- Spool_File.User_Data
- Spool_File.Job_User
- Spool_File.Output_Queue_Name
- Spool_File.Output_Queue_Library

Minimizing the starting and stopping of monitoring

When a situation raises an event, monitoring for the conditions does not stop. Attribute data is collected as long as the situation is active.

If monitoring has not been started for a situation named in an **Evaluate a Situation Now** activity (which is available in policies), monitoring starts when the *EVALUATE_SITUATION activity starts. Monitoring ends when the activity program has analyzed the conditions in the situation.

When possible, use embedded situations rather than the **Evaluate a Situation Now** activity. If you want to use the **Evaluate a Situation Now** activity, start the situation before the *EVALUATE_SITUATION activity begins to lessen performance impact.

Support for problem solving

If you have a problem with your IBM software, you want to resolve it quickly. This section describes the following options for obtaining support for IBM software products:

- “Using IBM Support Assistant” on page 221
- “Obtaining fixes” on page 221
- “Contacting IBM Software Support” on page 221

Using IBM Support Assistant

The IBM Support Assistant is a free, stand-alone application that you can install on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products you use.

The IBM Support Assistant saves you the time it takes to search the product, support, and educational resources. The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem.

The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, and to download the IBM Support Assistant Version 3, see http://www.ibm.com/software/support/isa. After you download and install the IBM Support Assistant, follow these steps to install the plug-in for IBM Tivoli Monitoring:

1. Start the IBM Support Assistant application.
2. Select **Updater** on the Welcome page.
3. Select **New Properties and Tools**.
4. Under Tivoli, select **IBM Tivoli Monitoring 6.2**, and then click **Install**. Be sure to read the license and description.
5. Restart the IBM Support Assistant.

Obtaining fixes

A product fix might be available to resolve your problem. To determine which fixes are available for your Tivoli software product, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Under **Select a brand and/or product**, select **Tivoli** and click **Go**.
3. Under **Select a category**, select a product and click **Go**.
4. Under **Download**, click the name of a fix to read its description and, optionally, to download it.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

Contacting IBM Software Support

IBM Software Support provides assistance with product defects. The easiest way to obtain that assistance is to open a PMR or ETR directly from the IBM Support Assistant (see “Using IBM Support Assistant”).

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus®, and Rational® products, as well as DB2 and WebSphere® products that run on Windows or UNIX operating systems), enroll in Passport Advantage® in one of the following ways:

  Online
  Go to the Passport Advantage Web site at http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm .

  By phone
  For the phone number to call in your country, go to the IBM Software Support Web site at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.
- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request Web site at https://techsupport.services.ibm.com/ssr/login.
- For customers with IBMLink™, CATIA, Linux, OS/390®, iSeries, pSeries®, zSeries®, and other support agreements, go to the IBM Support Line Web site at http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- For IBM eServer™ software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web site at http://www.ibm.com/servers/eserver/techsupport.html.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the *IBM Software Support Handbook* on the Web at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region for phone numbers of people who provide support for your location.

To contact IBM Software support, follow these steps:

1. "Determining the business impact"
2. "Describing problems and gathering information" on page 223
3. "Submitting problems" on page 223

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Use the following criteria TO understand and assess the business impact of the problem that you are reporting:

Severity 1
The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2
The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3
The problem has *some* business impact. The program is usable, but less significant features (not critical to operations) are unavailable.

Severity 4

The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- Which software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you re-create the problem? If so, what steps were performed to re-create the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.
- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online

Click **Submit and track problems** on the IBM Software Support site athttp://www.ibm.com/software/support/probsub.html. Type your information into the appropriate problem submission form.

By phone

For the phone number to call in your country, go to the contacts page of the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Software Support Web site daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix F. Documentation library

This appendix contains information about the publications related to the Monitoring Agent for i5/OS. These publications are listed in the following categories:

- Monitoring Agent for i5/OS library
- Prerequisite publications
- Related publications

See the *IBM Tivoli Monitoring and OMEGAMON$^{®}$ XE Products Documentation Guide*, for information about accessing and using publications. You can find the *IBM Tivoli Monitoring and OMEGAMON XE Products Documentation Guide* in the IBM Tivoli Monitoring and OMEGAMON XE Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v15r1/.

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 information centers** on the Welcome page for the product.

Monitoring Agent for i5/OS library

There is one document specific to the Monitoring Agent for i5/OS: *IBM Tivoli Monitoring: i5/OS Agent User's Guide*. This user's guide provides agent-specific reference and problem determination information for configuring and using the IBM Tivoli Monitoring for i5/OS Agent.

Use the configuration chapter in this guide with the *IBM Tivoli Monitoring Installation and Setup Guide* to set up the software.

Use the information in this guide with the *IBM Tivoli Monitoring User's Guide* to monitor i5/OS resources.

Prerequisite publications

To use the information in this publication effectively, you must have some prerequisite knowledge, which you can obtain from the following IBM Tivoli Monitoring publications:

- *Exploring IBM Tivoli Monitoring*
- *IBM Tivoli Monitoring Administrator's Guide*
- *IBM Tivoli Monitoring Agent Builder User's Guide*
- *IBM Tivoli Monitoring Command Reference*
- *IBM Tivoli Monitoring Installation and Setup Guide*
- *IBM Tivoli Monitoring: Messages*
- *IBM Tivoli Monitoring Migration Toolkit User's Guide*
- *IBM Tivoli Monitoring Problem Determination Guide*
- *IBM Tivoli Monitoring: Upgrading from Tivoli Distributed Monitoring*
- *IBM Tivoli Monitoring User's Guide*
- *IBM Tivoli Monitoring: Upgrading from V5.1.2*

- *IBM Tivoli Monitoring Configuring Tivoli Enterprise Monitoring Server on z/OS*
- *IBM Tivoli Monitoring: Windows OS Agent User's Guide*
- *IBM Tivoli Monitoring: UNIX OS Agent User's Guide*
- *IBM Tivoli Monitoring: Linux OS Agent User's Guide*
- *IBM Tivoli Monitoring: i5/OS Agent User's Guide*
- *IBM Tivoli Monitoring: UNIX Log Agent User's Guide*
- *IBM Tivoli Monitoring Universal Agent User's Guide*
- *IBM Tivoli Monitoring Universal Agent API and Command Programming Reference Guide*
- *Introducing IBM Tivoli Monitoring Version 6.1.0*

Related publications

The following documents also provide useful information:

- *IBM Tivoli Enterprise Console Adapters Guide*
- *IBM Tivoli Enterprise Console Event Integration Facility User's Guide*
- *IBM Tivoli Enterprise Console Reference Manual*
- *IBM Tivoli Enterprise Console Rule Builder's Guide*

Other sources of documentation

You can also obtain technical documentation about Tivoli Monitoring and OMEGAMON XE products from the following sources:

- IBM Tivoli Open Process Automation Library (OPAL)

  http://www.ibm.com/software/tivoli/opal

  OPAL is an online catalog that contains integration documentation as well as other downloadable product extensions. This library is updated daily.
- Redbooks

  http://www.redbooks.ibm.com/

  IBM Redbooks®, Redpapers, and Redbooks Technotes provide information about products from platform and solution perspectives.
- Technotes

  You can find Technotes through the IBM Software Support Web site at http://www.ibm.com/software/support/probsub.html, or more directly through your product Web site, which contains a link to Technotes (under **Solve a problem**).

  Technotes provide the latest information about known product limitations and workarounds.

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:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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.

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 systems. 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 system 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.

If you are viewing this information in softcopy form, the photographs and color illustrations might not appear.

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.

Trademarks

IBM, the IBM logo, IBMLink, Advanced 36, Advanced Peer-to-Peer Networking, AIX®, AnyNet, AS/400®, Candle, CandleNet Portal®, DB2, developerWorks®, Distributed Relational Database Architecture, DRDA, eServer, i5/OS, iSeries, Lotus, MVS™, NetServer, OMEGAMON, OS/390, OS/400, Passport Advantage, Print Services Facility, pSeries, Rational, Redbooks, REXX, System i, System p, System Storage, System/36, Tivoli, the Tivoli logo, Tivoli Enterprise, Tivoli Enterprise Console, WebSphere, z/OS, and zSeries are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft, and Windows are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds 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

Printed in USA

SC32-9448-01