Note
Before using this information and the product it supports, read the information in "Notices" on page 23.

This edition applies to version 6, release 3 of IBM Tivoli Monitoring (product number 5724-C04) and to all subsequent releases and modifications until otherwise indicated in new editions.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
## Tables

1. System requirements for the Monitoring Agent for UNIX OS .................................. 9
2. Setting the environment variable KDEBE_FIPS_MODE_ENABLED ................................ 14
Chapter 1. Overview of the agent

The Monitoring Agent for UNIX OS provides you with the capability to monitor and perform basic actions on AIX®, Solaris, and HP-UX operating systems. IBM Tivoli Monitoring is the base software for the Monitoring Agent for UNIX OS.

IBM Tivoli Monitoring overview

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 achieve the following tasks:

- 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. You can use the consolidated view of your environment as seen in the Tivoli Enterprise Portal to monitor and resolve performance issues throughout the enterprise.

Features of the Monitoring Agent for UNIX OS

The Monitoring Agent for UNIX OS offers a central point of management for your UNIX server environment. This monitoring agent provides a way to monitor the availability and performance of all the systems in your enterprise from one or several designated workstations. This monitoring agent also provides useful historical data that you can use to track trends and to troubleshoot system problems. Information is standardized across all systems (AIX, HP-UX, and Solaris).

The Monitoring Agent for UNIX OS lets you easily collect and analyze server-specific information, such as the following:

- Operating system and CPU performance
- UNIX disk information and performance analysis
- Process status analysis
- Network performance

The Monitoring Agent for UNIX 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.
- Scales and ports to a wide variety of UNIX platforms.
• Enhances system performance because you can integrate, monitor, and manage your environment, networks, console, and mission-critical applications. For example, the Monitoring Agent for UNIX OS can alert you when a condition in your environment meet or exceed the thresholds you set. These alerts notify your system administrator to limit and control system traffic. You can view data gathered by the Monitoring Agent for UNIX OS in reports and charts that inform you of the status of your managed UNIX systems.

• Enhances efficiency by monitoring diverse platforms and networks. Depending on the configuration of this monitoring agent, you can collect and monitor data across platforms. The Monitoring Agent for UNIX OS gathers and filters status information at the managed system rather than at the Hub, eliminating unnecessary data transmission and sending only data that is relevant to changes in status conditions.

New in this release

For version 6.3 Fix Pack 2 of the monitoring agent, enhancements include:

• The monitoring agent complies with the Federal Information Processing Standard (FIPS) 140-2. This computer security standard requires stronger checksum algorithms (for example, SHA-256 and SHA-512) when you define situations for checking file changes.

• An internal caching mechanism improves agent performance, in terms of response time and CPU consumption while collecting process information. The agent updates process information in cache, related to process PID, command, and arguments, every 120 seconds by default. To change the cache refresh time from this default value, specify the cache refresh value for the environment variable KUX_PROCESS_CMD_SAMPLE_SECS (minimum valid value is 30 seconds). If the environment variable is set to 0, the internal caching mechanism is disabled.

• Several reports were added to Tivoli Common Reporting, including the Top n Process Usage by WPAR report, WPARs Configuration report and WPAR Utilization report.

• Various metrics were ported from the AIX Premium agent to the Monitoring Agent for UNIX OS.
  - New attribute groups include AIX MPIO Attributes, AIX MPIO Status, AIX Network Adapters, and AIX System IO. To customize the sampling interval for AIX System IO metrics, specify the value of the KUX_MAP_SAMPLING_INTERVAL environment variable (default value: 30 seconds). To specify this sampling interval as variable, set 0 for the environment variable. As a result, the data sampling occurs when an agent receives the request.
  - The AIX Physical Volumes attributes group includes Number of Stale Partitions.
  - The Process attributes group includes Text Size.
  - The Disk Performance attributes group includes Avg Read Transfer MS, Avg Write Transfer MS, Failed Read per Sec, Failed Writes per Sec, Max Read Service MS, Max Request In WaitQ MS, Max Write Service MS, Min Read Service MS, Min Request In WaitQ MS, Min Write Service MS, Read Timeouts per Sec, and Write Timeout per Sec.
  - The Network attribute group includes Domain, Gateway, and Mask.
  - The AIX LPAR attributes group includes CPU Capacity Increment, Max Dispatch Latency, Min Req Virt CPU, Min Virt CPUs, and Num Hypervisor Calls per Sec. The Num Hypervisor Calls per Sec attribute is collected using the perfstat_hyperstat_total() system API, supported by AIX 6.1 TL5 FP2 or later.
New situations are associated with the Process node, Disk Usage node, and Network Adapters node.

The AIX MPIO Storage Information workspace has views that show the AIX Multi-Path I/O (MPIO) Attributes, AIX Connection Status, and AIX Storage Devices Utilization on the current LPAR.

The AIX Network Adapters workspace displays data related to utilization and errors per network adapter.

New situations associated with the Disk Usage node, Network node, and Process node.

The AIX Physical Volumes attributes group now includes the Number of Stale Partitions attribute.

The UNIX Memory attributes group now includes Available File Cache MB (AIX), Computational Memory MB (AIX), and Non Computational Memory MB (AIX). The System Memory view in the System Details workspace reports these new attributes. In addition, the UNIX Memory attributes group now includes Percent Real Memory Process (AIX), Percent Real Memory System (AIX), Percent Page Replacement Memory Current Value (AIX), Percent Page Replacement Memory Min Value (AIX), and Percent Page Replacement Memory Max Value (AIX).

The AIX Memory Per Page attributes group contains information about memory statistics per page size. The AIX Memory Details workspace contains views of AIX-specific data collected for the Unix Memory group and the AIX Memory Per Page group. To customize the sampling interval for Zero Frames Per Sec (MB), Page Steals Per Second (MB), Paged In Pages from Page Space Per Sec (MB), Paged Out Pages from Page Space Per Sec (MB), and Page Scans Frames By Clock Per Sec (MB) metrics, specify the value of the KUX_MAP_SAMPLING_INTERVAL environment variable (default value: 30 seconds). To specify this sampling interval as variable, set 0 for the environment variable. As a result, the data sampling occurs when an agent receives the request.

The Disk Performance attributes group now includes Volume Group Name (AIX). The Disk Performance view in the Disk Usage Details workspace reports this new attribute.

For the Utilization Details for Single Resource report, you can specify the resources to display (CPU, Memory, Disk, Network, or Process).

In addition to monitoring the status of the mount_stat, aixdp_daemon, and stat_daemon subprocesses used by the UNIX OS Agent to collect data from the system, you can monitor the health of the stat_daemon children: kux_vmstat for CPU and memory statistics, ifstat for network interface statistics, nfs_stat for NFS and RPC statistics, and kuxdstat (or iostat, for AIX) for disk I/O statistics. You can disable the kuxdstat data provider at startup, by specifying the environment variable KUX_DISABLEUNIXDPERF=TRUE. As a result, the status of the Data Provider kuxdstat (or iostat for AIX) is set to “Disabled”. The Data Collection Status attribute group now includes Process ID.

A new situation, UNIX_Agent_Processes_Failure, is associated with the System Information node.

For version 6.3 of the monitoring agent, enhancements include:

• Various metrics were ported from the AIX Premium agent to the Monitoring Agent for UNIX OS.

• New attribute groups include AIX Logical Volumes, AIX Physical Volumes, AIX Volume Groups, Top CPU Processes, Top Memory Processes, and UNIX Devices.

• The UNIX workspace, Process workspace, and All Processes workspace were updated with revised views to incorporate data that is offered by the Top CPU Processes, Top Memory Processes, and UNIX Devices attribute groups.
- The AIX Storage workspace contains views of data that is related to logical volumes, physical volumes, and volume groups. The views for this workspace include the Physical Volume Sizes bar chart, Physical Volume Details table view, Volume Group Sizes bar chart, Volume Group Details table view, Logical Volume Sizes bar chart, and Logical Volume Details table view.

- The AIX Devices Status workspace was superseded by the Devices Status workspace. In addition, the UNIX_Device_Stopped_Warning situation indicates whether a specific UNIX device stopped.

- The Data Collection Status attributes group reports on the health of internal data collectors of the Monitoring Agent for UNIX OS. The Data Collection Status table view of the UNIX workspace provides specific details.

- The UNIX Memory attributes group now includes Percent Available File Cache (AIX), Percent Computational Memory (AIX), and Percent Non Computational Memory (AIX). The System Virtual Memory view in the System Details workspace reports these new attributes.

- For attribute values calculated as an average of the cumulative CPU ticks between two samples, the sample time differs depending on how the agent is invoked to return the values. If the agent is invoked to return the values on-demand (for example, after a workspace refresh), the default sample time is 30 seconds for total CPU metrics and 60 seconds for the CPU metrics per process. If, however, the agent is invoked to return the values by a situation or a historical collection request, the sample time is the same as that of the situation or of the collection interval. The affected attributes include:
  - SMP CPU attribute group: User CPU, System CPU, Idle CPU, Wait I/O, CPU Busy, and CPU Usage attributes
  - SMP CPU attribute group, for SUN Solaris OS agents: Minor Faults, Major Faults, Cross Calls, Interrupts, Interrupts As Threads, Context Switches, Involuntary Context Switches, Thread Migrations, Spins On Mutexes, Spins On RW Locks, and System Calls attributes
  - Process attribute group: CPU Pct attribute
  - Top CPU Processes attribute group: CPU Pct attribute
  - Top Memory Processes attribute group: CPU Pct attribute

  You can customize the sampling intervals by specifying two variables in the ux.ini file: KUX_CPUSTAT_SAMPLE_SECS for the total CPU metrics (default value: 30 seconds) and KUX_PROCESS_SAMPLE_SECS for the CPU metrics per process (default value: 60 seconds). If these variables are set to 0, the sampling interval is variable: the samples are taken when the requests come to the agent (for example, at each workspace refresh), and the sampling interval is the difference in time between last two samples (with a minimum of 5 seconds).

  The CPU statistics measurements are provided by system API. Therefore, the KUX_IGNORE_MPSTAT, KBB_HPUX_SAR, and KBB_HPUX_VMSTAT environment variables are no longer required. Even if the variables are specified, they are ignored.

- The Summarization and Pruning agent automatically creates and maintains the shared dimensions tables. For instructions to enable this feature, see “Configuring the Summarization and Pruning agent to maintain the dimension tables” in the IBM Tivoli Monitoring Administrator’s Guide. To enhance this feature for the OS Agents Reports package, the installer now prompts you to provide JDBC connection details and credentials for the Tivoli Data Warehouse database. This RegisterPackage script execution step inserts data into the WAREHOUSETCRCONTROL table. After this step, the MANAGEDSYSTEM table and the TIME_DIMENSION table are kept up to date automatically by the Summarization and Pruning agent. However, if you opt not to use this feature and prefer, instead, to manually maintain the dimensions tables, skip this step.
For instructions to perform any required manual steps, see “Manually creating and maintaining the dimension tables” in the *IBM Tivoli Monitoring Administrator’s Guide*.

- The agent provides ComputerSystem and IPAddress resources for the Open Services for Lifecycle Collaboration Performance Monitoring (OSLC-PM) service provider. The service provider registers monitoring resources with the Registry Services. Registry Services is a Jazz for Service Management integration service that provides a shared data repository for products in an integrated service management environment.

- The IBM Tivoli Monitoring Infrastructure Management Dashboards for Servers is a web-based application that runs in the Dashboard Application Services Hub. The server dashboards give the overall status of the service areas in your managed network. Use the server dashboards to assess the event and system status of your managed network that is filtered by your area of responsibility. The information ranges from a high-level overview of all managed system groups and the situation events that are associated with them, to more detailed dashboards with key performance information about the selected group, managed system, or situation event.

**Components of the monitoring agent**

After you install and set up the Monitoring Agent for UNIX OS (product code: kux or ux), you have an environment with a client, server, and monitoring agent implementation for IBM Tivoli Monitoring.

This IBM Tivoli Monitoring environment contains the following components:

- Tivoli Enterprise Portal client with a Java-based user interface for viewing and monitoring your enterprise.

- Tivoli Enterprise Portal Server that is placed between the client and the Tivoli Enterprise Monitoring Server and enables retrieval, manipulation, and analysis of data from the monitoring agents.

- Tivoli Enterprise Monitoring Server, which acts as a collection and control point for alerts received from the monitoring agents, and collects their performance and availability data.

- Monitoring Agent for UNIX OS, which collects and distributes data to a Tivoli Enterprise Monitoring Server. This component also embeds the Agent Management Services function.

- Operating system agents and application agents installed on the systems or subsystems you want to monitor. These agents collect and 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 the *IBM Tivoli Monitoring Installation and Setup Guide*. 

Chapter 1. Overview of the agent  5
Agent Management Services

Two watchdog monitors run as part of the Monitoring Agent for UNIX. One monitor runs as part of the OS Monitoring Agent process, which is referred to as the Agent Watchdog. The other watchdog monitor runs as a separate process named 'kcawd'. The kcawd process is also called the Agent Management Services Watchdog. This watchdog monitor watches the OS Agent as long as its Availability Status displays 'Running' in the Agent's Runtime Status view of the Agent Management Services workspace. No setup or configuration is required.

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

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

You can temporarily disable the Agent Management Services Watchdog by using the `InstallDir/bin/itmcmd execute ux disarmWatchdog.sh` command. This command disables the Watchdog process for the OS Monitoring Agent and all Agent Management Services managed agents. If there is local administrative work to be performed, and you do not want the auto-restart of the agents to interfere with it, run the `InstallDir/bin/itmcmd execute ux disarmWatchdog.sh` command before proceeding. When the work is complete, recycle the OS Monitoring Agent to reenable Agent Management Services, or use the `InstallDir/bin/itmcmd execute ux rearmWatchdog.sh` command.

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

User interface options

Installation of the base IBM Tivoli Monitoring software and other integrated applications provides a variety of interfaces that you can use to work with your resources and data.

The following interfaces are available:

**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.

**IBM Tivoli Enterprise Console**  
Event management application

**Manage Tivoli Enterprise Monitoring Services window**  
The window for the Manage Tivoli Enterprise Monitoring Services utility is used for configuring the agent and starting Tivoli services not already designated to start automatically.
Chapter 2. Agent installation and configuration

Agent installation and configuration requires the use of the IBM Tivoli Monitoring Installation and Setup Guide and agent-specific installation and configuration information.

To install and configure the monitoring agent, use the “Installing monitoring agents” procedures in the IBM Tivoli Monitoring Installation and Setup Guide.

If you are installing silently by using a response file, see “Performing a silent installation of IBM Tivoli Monitoring” in the IBM Tivoli Monitoring Installation and Setup Guide.

In addition to the installation and configuration information in the IBM Tivoli Monitoring Installation and Setup Guide, use this agent-specific installation and configuration information to install the monitoring agent.

Requirements for the monitoring agent

Consider the requirements for installing this monitoring agent.

In addition to the requirements described in the IBM Tivoli Monitoring Installation and Setup Guide, the Monitoring Agent for UNIX OS has the requirements listed in Table 1.

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

<table>
<thead>
<tr>
<th>Operating system</th>
<th>UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system versions</td>
<td></td>
</tr>
<tr>
<td>• AIX V6.1 (32 and 64 bit)</td>
<td></td>
</tr>
<tr>
<td>• AIX V7.1 (64 bit)</td>
<td></td>
</tr>
<tr>
<td>• HP-UX 11i v2 (64 bit) on PA-RISC</td>
<td></td>
</tr>
<tr>
<td>• HP-UX 11i v3 (64 bit) on PA-RISC</td>
<td></td>
</tr>
<tr>
<td>• HP-UX 11i v2 on Integrity (IA64)</td>
<td></td>
</tr>
<tr>
<td>• HP-UX 11i v3 on Integrity (IA64)</td>
<td></td>
</tr>
<tr>
<td>• Solaris V10 (SPARC) (32 and 64 bit)</td>
<td></td>
</tr>
<tr>
<td>• Solaris V10 (Intel x86-64) (64 bit)</td>
<td></td>
</tr>
<tr>
<td>• Solaris V11 (SPARC) (32 and 64 bit)</td>
<td></td>
</tr>
<tr>
<td>• Solaris V11 (Intel x86-64) (64 bit)</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>55 MB RAM for the Monitoring Agent for UNIX OS</td>
</tr>
</tbody>
</table>
Table 1. System requirements for the Monitoring Agent for UNIX OS (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>UNIX</th>
</tr>
</thead>
</table>
| Disk space       | The Monitoring Agent for UNIX OS needs 320 MB of disk space in the file system where it is to be installed through the local install method. It needs 200 MB of disk space in the /tmp file system and 320 MB of disk space in the file system where the agent is to be installed through the tacmd createNode command. It needs 510 MB of disk space when it is updated using the command tacmd updateAgent.

Historical data space varies, depending on the tables collected. Refer to general installation guidelines for disk space requirements in the IBM Tivoli Monitoring Installation and Setup Guide and “Disk capacity planning for historical data” in the IBM Tivoli Monitoring Unix OS Agent Reference.

Disk space requirements can be as high as 1 GB for log files, remote deploys and historical data. |
| Other requirements | • IBM Tivoli Monitoring OS agents require that the hub monitoring server and portal server be at the same version or at a later version relative to the OS agent version. |
|                    | • A POSIX-compliant threads package must be installed on the monitored machine. |
|                    | • Ethernet or token ring LAN capability. |
|                    | • Native X-term monitor for UNIX or Hummingbird Exceed X-windows emulators for PCs only. |
|                    | • For AIX: A compatible version of libperfstat. Upgrade to the latest version of libperfstat for the latest memory fixes. |
|                    | • Version 11.1 of the AIX XL C/C++ runtime must be installed. To determine the current level, run the following AIX command: |
|                    | ls1pp -l | grep -i xlc |
|                    | • On Solaris, the posix standard utilities package, SUNWxscu4, is required. To check if the package is installed, run the following Solaris command: |
|                    | pkginfo -1 SUNWxscu4 |
|                    | • The monitoring agent must have the permissions necessary to perform requested actions. For example, if the user ID you used to log onto the system to install the monitoring agent (locally or remotely) does not have the permission to perform a particular action being monitored by the monitoring agent (such as running a particular command), the monitoring agent will be unable to perform the requested action. |
|                    | • Solaris versions require the latest version of SUNWlibC (libC.so.5). |
|                    | • Veritas VxFS (type 32) is a supported file system for the AIX platform. |
Table 1. System requirements for the Monitoring Agent for UNIX OS (continued)

<table>
<thead>
<tr>
<th>Operating system</th>
<th>UNIX</th>
</tr>
</thead>
</table>

**Note:**

1. On AIX 7.1 TL1, SP 2 (or later) is required. If you cannot upgrade to SP 2, you can download the fix for APAR V09585. For more information, see the IBM Tivoli Monitoring Troubleshooting Guide.

2. The ITM Unix OS Agent on HP-UX 11.21 might crash if the following HP-UX patch is installed on the machine: PHSS_31855 1.0 aC++ Runtime (IA®: A.05.61, PAA.03.61). If so, the message "aCC runtime: Use of "-mt" must be consistent during both compilation and linking." is added to the log file. To remedy this situation, either downgrade aC++ runtime to HP-UX patch PHSS_31852 or upgrade to HP-UX patch PHSS_33350.

3. For Solaris, the minimum software group required to run this monitoring agent is the 'End User' group.

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

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

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

**Enabling the monitoring agent to run as a nonroot user**

The “Post-installation steps for nonroot installations” section of the IBM Tivoli Monitoring Installation and Setup Guide describes the post-installation setup process required to enable a nonroot user. Those instructions result in the availability of root authority to the underlying IBM Tivoli Monitoring processes. These instructions, in contrast, remove root authority from the underlying processes.

**Securing your IBM Tivoli Monitoring installation**

On UNIX operating systems, the product installation process creates the majority of directories and files with world write permissions. This configuration creates a security situation that is not acceptable in many enterprises. The secureMain utility helps you bring the monitoring environment into compliance with the security standards of your company. Run the secureMain utility on all installations, especially those installations that include the UNIX OS Agent, to prevent privilege escalation.

For information about the secureMain utility and usage examples, see the “Securing your IBM Tivoli Monitoring installation on Linux or UNIX” appendix in the IBM Tivoli Monitoring Installation and Setup Guide.

**Setting overall file ownership and permissions for nonroot users**

The Monitoring Agent for UNIX OS is capable of running with nonroot user privileges, with some limitations, by changing some agent file permissions and assuring that the desired running user ID has write access to the necessary directories.
The Monitoring Agent for UNIX OS must run with root user privileges to assure correct remote deployment, and collection of some attributes on the Solaris platform. To ensure root privileges, the IBM Tivoli Monitoring installation sets the owner to root and the Set User-ID bit on the primary agent binary, kuxagent, to ensure the agent starts up as the root regardless of which user ID starts the agent.

If you want to start the Monitoring Agent for UNIX OS with permissions of another user ID, use the `chmod` command to turn off the Set User-ID (SUID) bits of the kuxagent binaries to enable running the agent as nonroot. The relevant binary for the Monitoring Agent for UNIX OS in the directory `CANDLEHOME/platform/ux/bin` directory is kuxagent (HPUX - User SUID, Solaris - User SUID, AIX).

**Setting kuxagent binary permissions**

Changing the permissions requires running systems commands locally on the target system:

```
find CANDLEHOME/* -name kuxagent -exec chmod 755 {} \;
```

The bit setting above (755) unsets the SUID bit and ensures that the other bits are set correctly. Note that the bit setting for kuxagent is not persistent. If you ever run secureMain, SetPerm, or install.sh, you need to unset the SUID bit for kuxagent again.

**Limitations of starting the agent as a nonroot user**

On installation of any other agent by a nonroot user, the permissions on the agent are reset to run the agent with root requirements. You must manually reset the permissions as described above.

Metrics belonging to the WPAR attribute groups:

All of the metrics belonging to the WPAR attribute groups are collected by using the `lswpars` command. However, only the root user can run this command. Therefore, to collect metrics for the WPAR attribute groups, you must be logged into the system as the root user.

Metrics belonging to the Defined Users attributes group:

All of the metrics belonging to the Defined Users attribute group are collected by using the `lsuser -c ALL` command. To collect metrics for the Defined Users attribute group as a nonroot user, you must belong to the security group. If not, the Defined Users view of the Users workspace lists “Not Collected” for each of its fields. In addition, even if the user belongs to the security group, the Roles and Login Retries attributes of the Defined Users group might be incorrectly reported as Not Collected.

Remote Deployment:

Remote deployment might not complete or work at all on certain agents that require root privileges to install the desired application. Install the agents locally or configure the agent manually after installation.
Setting up the monitoring agent in a cluster environment

You can install and set up the monitoring agent in as HACMP clustered environment by following these instructions.

The IBM Tivoli Monitoring Installation and Setup Guide contains an overview of clustering. The Monitoring Agent for UNIX OS is set up and works as it does in a non-clustered environment. There is a unique cluster configuration prompt for the Monitoring Agent for UNIX OS:

Are you installing this product into a clustered environment (Default is: NO):

You should accept the default (NO).

Note: The NO or YES response is case-sensitive.

The shared disks attributes are displayed in all cluster nodes workspace views that use the disk-related queries. However, the disk metrics are zero for the nodes that are not controlling the shared disk because they do not have access to the shared disk. The highly available IP addresses are not displayed in the network table since the highly available IP address is bound to an alias interface. Alias interface IP addresses are reported in the IP Address attribute group. The relevant statistics for those IP addresses are reported in the base Interface name in the Network attribute group since all aliases share one set of statistics for a particular network interface. The base interface can usually be found by removing the colon and number at the end of the aliased interface (for example, Alias = en0:3 Base: en0).

Filtering capabilities on the names of processes

You can distinguish process names that are longer than 768 characters, so that situations can be defined on the relevant part of the name. You can also use this enhancement for filtering processes of any length.

To improve filtering on the processes, a Process Filter attribute has been added to the UNIX Process attribute group. Its content, a regular expression, is sent to the agent as a filter object and is intended to only act on the Process Command (Unicode) attribute. For example, the agent uses the value provided in the Process Filter attribute to match the process name, and then fills the Process Command (Unicode) attribute.

In a Tivoli Enterprise Portal workspace view, you see only the processes whose names match the specified regular expression. The Process Command (Unicode) column is filled with the matching patterns separated by blanks, as defined in the regular expression. The Process Filter column is filled with the regular expression that matches it. Situations can be defined mixing the Process Command (Unicode) column and other conditions (for example, CPU usage).

To use this enhancement, create queries and situations on the UNIX Process attribute group containing the Process Filter attribute and define a regular expression in it. More rows and more regular expressions are allowed. Use the query in a workspace view or distribute the situation to the target managed systems.

There are a few predefined regular expressions for the Process Filter attribute when you use it in the query or situation editor:

- Java processes (*.java.*)
Complying with FIPS requirements

The monitoring agent complies with the Federal Information Processing Standard (FIPS) 140-2. This computer security standard requires stronger checksum algorithms (for example, SHA-256 and SHA-512) when you define situations for checking file changes.

To enforce compliance at the agent, specify checksum algorithms with the KDEBE_FIPS_MODE_ENABLED environment variable in the ux.ini file. Table 2 lists the supported algorithms for each setting of the environment variable.

<table>
<thead>
<tr>
<th>Environment variable setting</th>
<th>CRC32</th>
<th>MD5</th>
<th>SHA - 1</th>
<th>SHA - 256</th>
<th>SHA - 512</th>
</tr>
</thead>
<tbody>
<tr>
<td>KDEBE_FIPS_MODE_ENABLED not set</td>
<td>default</td>
<td>allowed</td>
<td>allowed</td>
<td>allowed</td>
<td>allowed (“Long Checksum” attribute)</td>
</tr>
<tr>
<td>KDEBE_FIPS_MODE_ENABLED=yes</td>
<td>N/A</td>
<td>N/A</td>
<td>default</td>
<td>allowed</td>
<td>allowed (“Long Checksum” attribute)</td>
</tr>
<tr>
<td>KDEBE_FIPS_MODE_ENABLED=sp800-131a</td>
<td>N/A</td>
<td>N/A</td>
<td>default</td>
<td>allowed</td>
<td>allowed (“Long Checksum” attribute)</td>
</tr>
<tr>
<td>KDEBE_FIPS_MODE_ENABLED=sp800-131a</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>default</td>
<td>allowed (“Long Checksum” attribute)</td>
</tr>
<tr>
<td>KDEBE_FIPS_MODE_ENABLED=suiteb192</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>default</td>
<td>allowed (“Long Checksum” attribute)</td>
</tr>
</tbody>
</table>

Create a situation on the File Information group that specifies a File Name, a Path, and File Content Changed = YES. Optionally, add a checksum algorithm-specific value to the situation definition to change the defaults. The situation fires when the file content is changed. The value of the computed file checksum is reported in the situation details. This value is in the “Checksum” attribute or “Long Checksum” attribute. The “Long Checksum” attribute also supports the longer checksum value of the SHA-512 algorithm.
Documentation library

This appendix contains information about the publications related to IBM Tivoli Monitoring and to the commonly shared components of Tivoli Management Services.

These publications are listed in the following categories:
- IBM Tivoli Monitoring library
- Related publications

For information about accessing and using the publications, select Using the publications in the Contents pane of the IBM Tivoli Monitoring and OMEGAMON® XE Information Center at http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp.

To find a list of new and changed publications, click What's new on the Welcome page of the IBM Tivoli Monitoring and OMEGAMON XE Information Center. To find publications from the previous version of a product, click Previous versions under the name of the product in the Contents pane.

IBM Tivoli Monitoring library

The following publications provide information about IBM Tivoli Monitoring and about the commonly shared components of Tivoli Management Services:
- Quick Start Guide
  Introduces the components of IBM Tivoli Monitoring.
- Installation and Setup Guide, SC22-5445
  Provides instructions for installing and configuring IBM Tivoli Monitoring components on Windows, Linux, and UNIX systems.
- Program Directory for IBM Tivoli Management Services on z/OS, GI11-4105
  Gives instructions for the SMP/E installation of the Tivoli Management Services components on z/OS.
- High Availability Guide for Distributed Systems, SC22-5455
  Gives instructions for several methods of ensuring the availability of the IBM Tivoli Monitoring components.
- IBM Tivoli zEnterprise Monitoring Agent Installation and Configuration Guide, SC14-7358
  Provides instructions for installing and configuring Tivoli zEnterprise monitoring agent components on Windows, Linux, and UNIX systems. Also includes migration and backup information, Enterprise Common Collector troubleshooting, Hardware Management Console configuration, and use of the command line interface or APIs to customize the collector. This guide complements the Tivoli zEnterprise Monitoring Agent User’s Guide.
- Administrator’s Guide, SC22-5446
  Describes the support tasks and functions required for the Tivoli Enterprise Portal Server and clients, including Tivoli Enterprise Portal user administration.
- Command Reference, SC22-5448
  Provides detailed syntax and parameter information, as well as examples, for the commands you can use in IBM Tivoli Monitoring.
• **Messages, SC22-5450**
  Lists and explains messages generated by all IBM Tivoli Monitoring components and by z/OS-based Tivoli Management Services components (such as Tivoli Enterprise Monitoring Server on z/OS and TMS:Engine).

• **Troubleshooting Guide, GC22-5449**
  Provides information to help you troubleshoot problems with the software.

• **Tivoli Enterprise Portal online help**
  Provides context-sensitive reference information about all features and customization options of the Tivoli Enterprise Portal. Also gives instructions for using and administering the Tivoli Enterprise Portal.

• **Tivoli Enterprise Portal User’s Guide, SC22-5447**
  Complements the Tivoli Enterprise Portal online help. The guide provides hands-on lessons and detailed instructions for all Tivoli Enterprise Portal features.

• **Agent Builder User’s Guide, SC32-1921**
  Explains how to use the Agent Builder for creating monitoring agents and their installation packages, and for adding functions to existing agents.

• **Performance Analyzer User’s Guide, SC27-4004**
  Explains how to use the Performance Analyzer to understand resource consumption trends, identify problems, resolve problems more quickly, and predict and avoid future problems.

• **IBM Tivoli zEnterprise Monitoring Agent User’s Guide, SC14-7359**
  Complements the Tivoli zEnterprise monitoring agent online help. The guide provides reference information about the interface, usage scenarios, agent troubleshooting information, and information about Tivoli Common Reporting reports. This guide complements the **Tivoli zEnterprise Monitoring Agent Installation and Configuration Guide**.

**Documentation for the base agents**

If you purchased IBM Tivoli Monitoring as a product, you received a set of base monitoring agents as part of the product. If you purchased a monitoring agent product (for example, an OMEGAMON XE product) that includes the commonly shared components of Tivoli Management Services, you did not receive the base agents.

The following publications provide information about using the base agents.

• Operating system agents:
  – **Windows OS Agent User’s Guide, SC22-5451**
  – **UNIX OS Agent User’s Guide, SC22-5452**
  – **Linux OS Agent User’s Guide, SC22-5453**
  – **IBM i Agent User’s Guide, SC22-5454**

• Agentless operating system monitors:

• Warehouse agents:
  – **Warehouse Summarization and Pruning Agent User’s Guide, SC22-5457**

• System P agents:

• Other base agents:

Related publications

For information about related products and publications select OMEGAMON XE shared publications or other entries in the Contents pane of the IBM Tivoli Monitoring and OMEGAMON XE Information Center at [http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp](http://pic.dhe.ibm.com/infocenter/tivihelp/v61r1/index.jsp).

Other sources of documentation

You can also obtain technical documentation about IBM Tivoli Monitoring and related products from the following sources:

• Service Management Connect (SMC)
  For introductory information about SMC, see [IBM Service Management Connect](http://www.ibm.com/developerworks/servicemanagement).
  For information about Tivoli products, see the Application Performance Management community on SMC at [IBM Service Management Connect > Application Performance Management](http://www.ibm.com/developerworks/servicemanagement/apm).
  Connect, learn, and share with Service Management professionals. Get access to developers and product support technical experts who provide their perspectives and expertise. Using SMC, you can:
  – Become involved with transparent development, an ongoing, open engagement between external users and developers of Tivoli products where you can access early designs, sprint demos, product roadmaps, and pre-release code.
  – Connect one-on-one with the experts to collaborate and network about Tivoli and Integrated Service Management.
  – Benefit from the expertise and experience of others using blogs.
  – Collaborate with the broader user community using wikis and forums.

• Tivoli wikis
  [IBM Service Management Connect > Application Performance Management](http://www.ibm.com/developerworks/servicemanagement/apm) includes a list of relevant Tivoli wikis that offer best practices and scenarios for using Tivoli products, white papers contributed by IBM employees, and content created by customers and business partners.
  Two of these wikis are of particular relevance to IBM Tivoli Monitoring:

**• IBM Integrated Service Management Library**


IBM Integrated Service Management Library is an online catalog that contains integration documentation and other downloadable product extensions.

**• Redbooks®**


IBM Redbooks and Redpapers include information about products from platform and solution perspectives.

**• Technotes**

Technotes provide the latest information about known product limitations and workarounds. You can find Technotes through the IBM Software Support Web site at [http://www.ibm.com/software/support/](http://www.ibm.com/software/support/)
Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides ways for you to obtain the support you need.

Online

The following sites contain troubleshooting information:

- Go to the IBM Support Portal (http://www.ibm.com/support/entry/portal/software) and follow the instructions.
- Go to IBM Service Management Connect > Application Performance Management (http://www.ibm.com/developerworks/servicemanagement/apm) and select the appropriate wiki.

IBM Support Assistant

The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, go to IBM Support Assistant (http://www-01.ibm.com/software/support/isa).

Troubleshooting Guide

For more information about resolving problems, see the product’s Troubleshooting Guide.

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, 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 your Tivoli product:

1. Start the IBM Support Assistant application.
2. Select Updater on the Welcome page.
3. Select New Properties and Tools or select the New Plug-ins tab (depending on the version of IBM Support Assistant installed).
4. Under Tivoli, select your product, and then click Install. Be sure to read the license and description.
If your product is not included on the list under Tivoli, no plug-in is available yet for the product.

5. Read the license and description, and click I agree.
6. 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:

2. Under Select a brand and/or product, select Tivoli.
   If you click Go, the Search within all of Tivoli support section is displayed. If you don't click Go, you see the Select a product section.
3. Select your product and click Go.
4. Under Download, click the name of a fix to read its description and, optionally, to download it.
   If there is no Download heading for your product, supply a search term, error code, or APAR number in the field provided under Search Support (this product), and click Search.


### Receiving weekly support updates

To receive weekly e-mail notifications about fixes and other software support news, follow these steps:

2. Click My support in the far upper-right corner of the page under Personalized support.
3. If you have already registered for My support, sign in and skip to the next step. If you have not registered, click register now. Complete the registration form using your e-mail address as your IBM ID and click Submit.
4. The Edit profile tab is displayed.
5. In the first list under Products, select Software. In the second list, select a product category (for example, Systems and Asset Management). In the third list, select a product sub-category (for example, Application Performance & Availability or Systems Performance). A list of applicable products is displayed.
6. Select the products for which you want to receive updates.
7. Click Add products.
8. After selecting all products that are of interest to you, click Subscribe to email on the Edit profile tab.
9. In the Documents list, select Software.
10. Select Please send these documents by weekly email.
11. Update your e-mail address as needed.
12. Select the types of documents you want to receive.
13. Click Update.
If you experience problems with the **My support** feature, you can obtain help in one of the following ways:

**Online**
Send an e-mail message to erchelp@ca.ibm.com, describing your problem.

**By phone**
Call 1-800-IBM-4You (1-800-426-4968).

---

**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.

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**
  - **By telephone**
    For the telephone number to call in your country, go to the IBM Software Support website at [http://techsupport.services.ibm.com/guides/contacts.html](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 website at [https://techsupport.services.ibm.com/ssr/login](https://techsupport.services.ibm.com/ssr/login).


- 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 website at [http://www.ibm.com/servers/eserver/techsupport.html](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://www14.software.ibm.com/webapp/set2/sas/1/handbook/home.html](http://www14.software.ibm.com/webapp/set2/sas/1/handbook/home.html) and click the name of your geographic region for telephone numbers of people who provide support for your location.
Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.
IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to
IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2013. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.
Index

C
cluster environment  13
code, product  5
components  5
configuration
agent  9
configuring the monitoring agent  9
copyright  23
customer support  21

D
developerWorks  17
disk space requirements  10

E
evironment
features  1

F
features, Monitoring Agent for UNIX OS  1
fixes, obtaining  20

I
IBM Redbooks  19
IBM Support Assistant  19
IBM Tivoli Enterprise Console
optional product  5
IBM Tivoli Monitoring for UNIX
benefits of  1
definition of  1
types of information collected by  1
installation
agent  9
installation requirements  9
installing the monitoring agent  9
Integrated Service Management Library  17
interface, user  6
ISA  19

M
memory requirements  9
Monitoring Agent for UNIX OS
components  5
features  1

N
nonroot users  11
notices  23

O
operating systems  9
other requirements  10

P
problem resolution  19
product code  5

R
Redbooks  17, 19
requirements  9
disk space  10
memory  9
operating system  9
other  10
requirements, installation  9

S
security  11
Service Management Connect  17, 19
SMC  17, 19
Software Support  19
contacting  21
receiving weekly updates  20
support assistant  19
Support Assistant  19

T
Technotes  17
Tivoli Data Warehouse  5
Tivoli Enterprise Console  5
Tivoli Enterprise Monitoring Server  5
Tivoli Enterprise Portal
component  5

U
user interfaces options  6

W
Warehouse Proxy agent  5
Warehouse Summarization and Pruning agent  5