Agent Monitors

Overview

Agent monitors are service monitors that require an agent to be installed on the system being monitored. An agent is software that collects performance information from the system and transmits that information to the Monitoring Station. Using the information gathered by an agent, *up.time* can alert users to changes in an environment based on defined thresholds.

File System Capacity

The File System Capacity monitor checks the amount of total and used space, in kilobytes, on a disk. This monitor then compares the capacity to the specified warning and critical thresholds. On Windows servers, *up.time* looks at the capacity of all local drives; on UNIX and Linux servers, *up.time* looks at all local file systems (e.g., */var* , */export* , */usr*).

On UNIX and Linux systems, you can configure the monitor to check all of the mount points on a system, or just specific mount points.

Windows Volume Mount Points can be monitored when the host Element is monitored through WMI, not the *up.time* agent (see Working with Systems for more information). Note that the level of detail for mounted volumes on Windows XP and 2000, when reported through WMI, is limited: the mounted volume name and exact location are not always accurate, but other pertinent information, such as volume capacity and usage, are correct.

> *Note - This monitor does not check floppy drives, tapes drives, or CD-ROM drives.*

Configuring File System Capacity Monitors

To configure File System Capacity monitors, do the following:

1. Complete the monitor information fields.
   To learn how to configure monitor information fields, see Monitor Identification.
2. Complete the following fields:
   - Global Warning Threshold (Mandatory)
     Create a threshold that generates a warning. This threshold can be an actual amount (in MB, GB, or TB), or percentage of disk space that is used or is free.
   - Global Critical Threshold (Mandatory)
     Create a threshold that generates a critical alert, whether it is an actual amount, or percentage of disk space used or free.
3. Optionally, to exclude specific mount points on the disk from the capacity calculations enter the names of the mount points in any or all of the five the *Exclude Pattern* fields.
   For example, you can enter *D:* (for Windows) or */usr* (for Solaris, Linux, or AIX) to ignore that drive or directory. To, for example, ignore all mount points that start with */u* enter */u** .
4. Optionally, you can set thresholds for specific mount points by entering the following information in any or all of the five *Mount Point* fields:
   - The name of the mount point, for example */opt* .
     Case sensitivity is not taken into account when monitor-defined mount points are matched with those on the file system.
   - The *Warning* threshold, which is a percentage or amount of space used or free on the mount point that, when exceeded, generates a warning.
   - The *Critical* threshold, which is a percentage or actual amount of space used or free on the mount point that, when exceeded, generates a critical alert.
     The thresholds that you set for each mount point will be calculated separately from the thresholds that you specified in step 2.
5. Specify values for the Warning and Critical *Response Time* thresholds.
   For more information, see Response Time.
   To save the data from the thresholds for graphing or reporting, click the *Save for Graphing* checkbox beside each of the Response Time metrics.
6. Complete the following settings:
   - Timing Settings (see Adding Monitor Timing Settings Information for more information)
   - Alert Settings (see Monitor Alert Settings for more information)
   - Monitoring Period settings (see Monitor Timing Settings for more information)
   - Alert Profile settings (see Alert Profiles for more information)
   - Action Profile settings (see Action Profiles for more information)
7. Click *Finish*.

Performance Check

The Performance check monitor provides a wide variety of metrics with which to measure system performance:

- percentage of CPU time used (user, system, waiting for IO, or total)
- number of processes in the run queue, per CPU
- percentage of memory used
- percentage of available swap space
- disk I/O checks including percentage of time in a busy state, number of queued requests, transfers, or bytes per second, for individual disks or averaged across all disks
- network I/O rate checks including send and receive rates, for an individual interface or averaged across all interfaces
- network error counts including the number of collisions, retransmits, and inbound or outbound errors, for any individual interface or averaged across all interfaces
- process-specific CPU usage (reported by the ps utility)
- process-specific memory usage (reported by the ps utility)

Configuring Performance Check Monitors

To configure Performance Check monitors, do the following:

1. Complete the monitor information fields.
   To learn how to configure monitor information fields, see Monitor Identification.
2. If desired, change the default *Time Interval* , indicating the number of minutes' worth of collected data that will be averaged then compared to configured thresholds.
3. In the *CPU Check* section, do the following:
   - Select one of the following *CPU Value* options:
     - User
       Time that the CPU spends processing application threads or threads that support tasks which are specific to applications.
     - System
       Time that the kernel spends processing system calls. If all the CPU time is spent in system time, there could be a problem with the system kernel, or the system is spending too much time processing I/O interrupts.
     - Waiting on I/O
       Time that a runnable process requires to perform an I/O operation.
     - Total
       The total of all CPU time that is being used.
   - Enter values, expressed as percentages, in the *CPU Warning Threshold* and *CPU Critical Threshold* fields.
4. In the *Run Queue Check* section, enter warning- and critical-level thresholds for the number of processes in the run queue, per CPU.
5. In the *Memory Check* section, enter warning- and critical-level thresholds for the percentage of used memory.
6. In the *Swap Check* section, enter warning- and critical-level thresholds for the percentage of used swap space.
7. In the *Disk I/O Check* section, do the following:
   - Indicate whether to check thresholds against values for individual disks on the system, or an average value for all disks on the system.
   - Select one of the following *Disk Value* options:
     - % Busy
       The amount of disk capacity in use.
     - Queued Requests
       The number of processes that are waiting to access the disk.
     - Transfers/sec
       The number of disk transfer requests processed per second.
     - Bytes/sec
       The amount of disk traffic flowing to and from a disk.
   - Enter warning- and critical-level thresholds for the selected disk performance metric.
8. In the *Network I/O Check* section, do the following:
   - Indicate whether to check thresholds against values for individual NICs, or an average value for all NICs on the system.
   - Select one of the following *Network Value* options:
     - Receive Rate
       The average rate, in Kbps, at which data is being received through the interface.
     - Send Rate
       The average rate at which data is being transmitted through the interface.
     - Send or Receive Rate
       The average rate at which data is being received or transmitted through the interface.
   - Enter warning- and critical-level thresholds for the selected network I/O metric.
9. In the *Network Error Check* section, do the following:
   - Indicate whether to check thresholds against values for individual NICs, or an average value for all NICs on the system.
   - Select one of the following *Network Value* options:
     - Collisions
       The simultaneous presence of signals from two nodes on the network, which can occur when two nodes start transmitting over a network at the same time. During a collision, both packets involved in a collision are broken into fragments and must be retransmitted.
     - Retransmits
       The number of retransmits required due to lost or broken packets.
     - In Errors
       Data packets that were received but could not be decoded because either their headers or trailers were not available.
     - Out Errors
       Data packets that could not be sent due to problems formatting the packets for transmission, or transmitting the packets.
     - In or Out Errors
       Data packets that were either received but not decodable, or unable to be sent.
   - Enter warning- and critical-level thresholds for the selected network error metric.
10. In the *Process CPU Check* area, complete the following fields:
    - Process to Check
      The name of process that you want this monitor to check. This monitor uses the *ps* utility on UNIX to collect information about active processes. For example, to check the status of the email
      process enter *sendmail* in this field.
    - Enter values, expressed as percentages, in the *Process Warning Threshold* and *Process Critical Threshold* fields.
11. In the *Process Memory Check* area, complete the following fields:
    - Process to Check
      The name of process that you want this monitor to check. This monitor uses the *ps* utility on UNIX to collect information about active processes. For example, to check the status of the email process enter *sendmail* in this field.
    - Select the desired *Process Value* option:
      - Private Memory / RSS
        The amount of physical memory being used by the process. (On Windows systems, the Run Set Size or RSS is Working Set.)
      - Total Memory / Virtual Memory
        The amount of the page file and virtual memory being used by the process.
    - Enter values, expressed as percentages, in the *Process Warning Threshold* and *Process Critical Threshold* fields.
12. Complete the following settings:
    - Timing Settings (see Adding Monitor Timing Settings Information for more information).
    - Alert Settings (see Monitor Alert Settings for more information)
    - Monitoring Period settings (see Monitor Timing Settings for more information).
    - Alert Profile settings (see Alert Profiles for more information)
    - Action Profile settings (see Action Profiles for more information)

13. Click *Finish* .

Process Count Check

The Process Count monitor measures the number of identical processes that are running on a system. If there is more than one instance of a process running, the check returns an OK status. If the process is not running, the check returns a Critical status.

Configuring Process Count Check Monitors

To configure Process Count Check monitors, do the following:

1. In the Process Count Check monitor template, complete the monitor information fields.
   To learn how to configure monitor information fields, see Monitor Identification.
2. Complete the following fields:
   - Process Name (Mandatory)
     The exact name of the process that you want to monitor.
     The name is the absolute name of the process, without its path, file extension, or any parameters.
     For example, on UNIX systems, the process " */usr/bin/vmstat -p* " is checked as " *vmstat* ", and on Windows systems, " *process.exe* " should be entered as " *process* ".
   - Process Occurrences
     Enter the number of process occurrences for which you want to set Warning and Critical thresholds. For more information, see Configuring Warning and Critical Thresholds.
   - Response Time
     Enter the Warning and Critical Response Time thresholds. For more information, see Configuring Warning and Critical Thresholds.
3. To save the data from the thresholds for graphing or reporting, click the *Save for Graphing* checkbox beside each of the metrics that you selected in step 3.
4. Complete the following settings:
   - Timing Settings (see Adding Monitor Timing Settings Information for more information).
   - Alert Settings (see Monitor Alert Settings for more information)
   - Monitoring Period settings (see Monitor Timing Settings for more information).
   - Alert Profile settings (see Alert Profiles for more information)
   - Action Profile settings (see Action Profiles for more information)
5. Click *Finish*.