Agent Monitors

Overview

Agent monitors are service monitors that require an agent to be installed on the monitored system. 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, Uptime Infrastructure Monitor can alert users to changes in an environment based on defined thresholds.

File and Directory

The *File and Directory* monitor can report the following Directory information:

- Number of files matching a certain regular expression
- Largest file size that matches that expression
- Age (in minutes) of the most recent file
- Most recent date of the latest file
- More recent time of the latest file
- File name that was most recently modified

Beginning with Uptime Infrastructure Monitor 7.7, this plugin is included within the product by default.

Configuring File Directory Monitor

Windows

1. Download the agent ZIP files.
2. Place the **filedircheck-win-agent.vbs** file in the Uptime agent directory in a subdirectory called "scripts". (`C:\Program Files\Uptime Software\Uptime agent\scripts`). Create the scripts directory, if needed.
3. Run as administrator, the Uptime Agent Console (**Start > Uptime Agent Console**).
4. Click **Advanced > Custom Scripts**.
5. Set up a command like this:
   ```
   Command Name: filedircheck
   Path to Script: cscript //nologo "C:\Program Files\Uptime Software\Uptime agent\scripts\filedircheck-win-agent.vbs"
   ```

POSIX

1. Place the needed **filedircheck-nix-agent.pl** file in the directory `/opt/uptime-agent/scripts`. Create the scripts directory, if needed.
2. Create/edit the following password file: `/opt/uptime-agent/bin/.uptmpasswd` and add the following line to it: `filedircheck /opt/uptime-agent/scripts/filedircheck-nix-agent.pl`
3. Run the following commands to change ownership and permission on `/opt/uptime-agent/scripts/filedircheck-nix-agent.pl`
   ```
   chown uptimeagent:uptimeagent /opt/uptime-agent/scripts/filedircheck-nix-agent.plchmod 770 /opt/uptime-agent/sctips/filedircheck-nix-agent.pl
   ```

File System Capacity

The *File System Capacity* monitor checks the amount of available space on a host's file system, and then compares the data to configured warning and critical thresholds. Thresholds can be based on percent free or used, or space free or used (in Megabytes, Gigabytes, or Terabytes).

By default, the service monitor uses global thresholds, which it applies to all local drives on Windows systems, or all local file systems on UNIX and Linux systems (for example, `/var`, `/export`, `/usr`). However, you can fine-tune how file systems are monitored using the following options:

- Use regular expressions to exclude one or more file systems from the list of default file systems.
- Use regular expressions to create special cases where the global thresholds are replaced with custom thresholds on one or more mount points.
- Exclude all file systems from capacity monitoring except for those locations listed as special cases.
- Disable global thresholds and alert on those defined for each special case.
- Use a combination of exclusions and special cases to augment the list of default file systems.

When using combinations to fine-tune file system monitoring, note that exclusions override the default file systems, and special cases override the default file systems and exclusions: if the same file system is added as a special case, and also matches a pattern to be excluded, it is still monitored for capacity.

You can monitor Windows Volume Mount Points when the host Element is monitored through WMI and not not the Uptime Infrastructure Monitor agent. for more information about this setup, see Working with Systems.

Configuring File System Capacity Monitor

Whether you want to set up a basic capacity monitor or create specific usage thresholds for 100 file systems, use the following common steps:

1. Complete the monitor information fields.
   To learn how to configure monitor information fields, see Monitor Identification.
2. 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.
3. 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** (see Monitor Timing Settings for more information)
   - **Alert Profile** (see Alert Profiles for more information)
   - **Action Profile** (see Action Profiles for more information)
4. Configure the options in the **File System Capacity Settings** section. Refer to the section that applies.

To set a common file system capacity check on local file systems, do the following:

1. In the **Global Settings** section, complete the following fields:
   - **Global Warning Threshold**
     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**
     Create a threshold that generates a critical alert, whether it is an actual amount, or percentage of disk space used or free.
2. Ensure the **Exclude None** option is selected.
   Using this option ensures global thresholds are used in conjunction with special cases.
3. Click **Finish**.

To create one or more exclusions from a common capacity check on local file systems, do the following:

1. In the **Global Settings** section, complete the following fields:
   - **Global Warning Threshold**
     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**
     Create a threshold that generates a critical alert, whether it is an actual amount, or percentage of disk space used or free.
2. Select the **Exclude File Systems Matching these Patterns** option.
3. In the New Pattern box, use a regular expression to exclude specific mount points on the disk from the capacity calculations.
   For example, enter `D:` (for Windows) or `/usr` (for Linux or UNIX) to ignore that drive or directory. Enter `^/u.*` to ignore all mount points that begin with `/u`.
4. Click the  icon to add the regular expression to the **Selected Patterns** list.
5. Optionally continue to add patterns until all file system exclusions are accounted for.
6. Click **Finish**.

To create custom threshold special cases for a common capacity check on local file systems, do the following:

1. In the **Global Settings** section, complete the following fields:
   - **Global Warning Threshold**
     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**
     Create a threshold that generates a critical alert, whether it is an actual amount, or percentage of disk space used or free.
2. Ensure the **Exclude None** option is selected.
   Using this option ensures global thresholds are used in conjunction with special cases.
3. For **Special Case File Systems**, indicate mount points among the local file systems, then create custom thresholds for them:
   - Use a regular expression to indicate the **Mount Point** among the local file systems.
   - Create a **Warning Level** threshold for a **Warning Type**: a percentage or amount of space used or free on the mount point that, when exceeded, generates a warning.
   - Create a **Critical Level** threshold for a **Critical Type**: a percentage or actual amount of space used or free on the mount point that, when exceeded, generates a critical alert.

   Any thresholds defined as special cases replace any **Global Settings** thresholds, should they apply.
4. Optionally click the icon to add mount points until all file systems you wish to add are accounted for.
5. Click **Finish**.

To monitor only specific file systems for capacity, do the following:

1. Select the **Exclude All Except Special Cases** option.
   Using this option ignores the default list of local file systems from capacity monitoring.
2. For **Special Case File Systems**, include specific mount points you would like to monitor:
   - Use a regular expression to indicate the Mount Point among the local file systems.
   - Create a **Warning Level** threshold for a **Warning Type**: a percentage or amount of space used or free on the mount point that, when exceeded, generates a warning.
   - Create a **Critical Level** threshold for a **Critical Type**: a percentage or actual amount of space used or free on the mount point that, when exceeded, generates a critical alert.
3. Optionally click the  icon to add mount points until all file systems you wish to add are accounted for.
4. Click **Finish**.

To monitor local file systems for capacity with some exceptions and special cases, do the following:

1. In the **Global Settings** section, complete the following fields:
   - **Global Warning Threshold**
     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**
     Create a threshold that generates a critical alert, whether it is an actual amount, or percentage of disk space used or free.
2. Select the **Exclude File Systems Matching these Patterns** option.
3. In the **New Pattern** box, use a regular expression to exclude specific mount points on the disk from the capacity calculations.
   For example, enter `D:` (for Windows) or `/usr` (for Linux or UNIX) to ignore that drive or directory. Enter `^/u.*` to ignore all mount points that begin with `/u`.
4. Click the icon to add the regular expression to the **Selected Patterns** list.
5. Optionally continue to add patterns until all file system exclusions are accounted for.
6. For **Special Case File Systems**, indicate mount points among the local file systems, then create custom thresholds for them:
   - Use a regular expression to indicate the Mount Point among the local file systems.
   - Create a **Warning Level** threshold for a **Warning Type**: a percentage or amount of space used or free on the mount point that, when exceeded, generates a warning.
   - Create a **Critical Level** threshold for a **Critical Type**: a percentage or actual amount of space used or free on the mount point that, when exceeded, generates a critical alert.

   Any thresholds defined as special cases replace any **Global Settings** thresholds, should they apply.
7. Optionally click the icon to add mount points until all file systems you wish to add are accounted for.
8. 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

> When the Disk I/O Check threshold is exceeded, the Performance Check monitor status displays a message such as, "Disk I/O Check: % Busy >= 95 for 0 (100.0)." The "for 0" section of the message refers to the specific disk name or ID that exceeded the threshold and appears only when the **Individual Disks** option is selected for the Disk I/O Check portion of the monitor. When **Average across all disks** is selected, the threshold is compared against the average Disk I/O for all disks, and therefore the "for 0" section of the message does not appear.

- 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 is 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 runable process requires to perform an I/O operation.
     - **Total**
       The total of all CPU time that is 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 received through the interface.
        - **Send Rate**
          The average rate at which data is transmitted through the interface.
        - **Send or Receive Rate**
          The average rate at which data is 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 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 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** (see Monitor Timing Settings for more information).
    - **Alert Profile** (see Alert Profiles for more information)
    - **Action Profile** (see Action Profiles for more information)
13. Click **Finish**.

Process Count Check

The Process Count Check 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.

If your monitor includes a space in the Process Name field, you may experience an error in monitor operation. The Process Count Check monitor uses regular expressions, which means that you must use the proper notation for a space. To match a space, use an escape with the space notation, i.e. \s. For example:

```
/usr/local/uptime/apache/bin/httpd -k start
```

should be

```
/usr/local/uptime/apache/bin/httpd\s-k\sstart
```

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** (see Monitor Timing Settings for more information).
    - **Alert Profile** (see Alert Profiles for more information)
    - **Action Profile** (see Action Profiles for more information)
5. Click **Finish**.