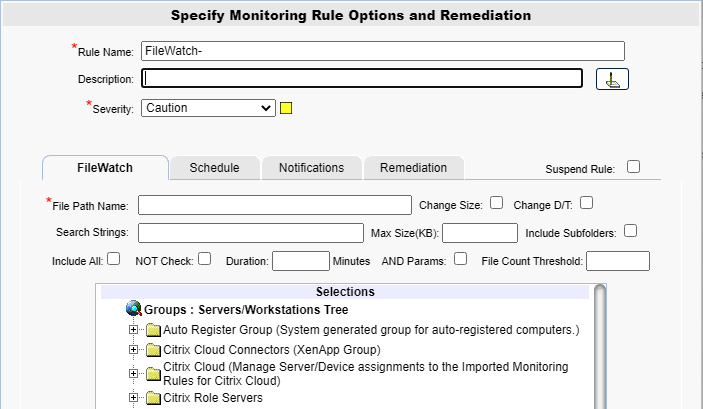
**File/Folder Monitoring**

 This article was updated to support v11.7.8 of Goliath Performance Monitor.

File Watch rules monitor your files and folders for keywords/files, changes, size, and or existence on your Windows servers/workstations using our Goliath Intelligent Agent to alert on specified conditions in real-time.



**Configure the Monitoring**

1. To create a new monitoring condition, navigate to the **Configure - Monitoring Rules** page and click the **New** button
2. A selection pane will appear, select the radio button option for **File Watch** and then click **OK**
3. Now the monitoring rule pane will appear. At the top of the pane name the Monitoring Rule via the **Rule Name** field, as well as define the description and the severity.
4. The first tab, **FileWatch** is where you will define the condition to be monitored.
5. In the **File Path Name** field, define the fully qualified path for the file to be checked in this Monitoring Rule. The path includes the driver letter but does NOT include the machine name. For example, "C:\MyApplication\MyLogFiles\Log.txt" is a correct specification.
   1. This parameter fully supports wild-cards for defining a Watch on a group of files matching the specification; this parameter also accepts a directory/folder name as a specification to monitor the entire folder for the specified conditions.
   2. If none of the other optional parameters below are defined then GPM watches for the creation and existence of the specified file(s).  If the ‘NOT Check’ checkbox is checked, GPM watches for the deletion of the file(s).
   3. You can exclude files from being part of a wild-card or folder check by following the ‘File Path Name’ spec with an exclamation point character (‘!’) and then the file to be excluded;  you can specify multiple exclusions, and you can use a wild-card in an exclusion name.  An example of a ‘File Path Name’ spec with multiple exclusions would look like this: C:\Log.\* ! tx1 ! log.tx2 !\*.tx3
6. The **Change Size** checkbox, when checked, the file's current size is determined, and any subsequent change to that size results in an alert condition.
7. The **Change D/T** checkbox, when checked, the file's current last-modified date/time is determined, and any subsequent change to that last-modified date/time results in an alert condition.
8. In the **Search String** field, if specified, the file is scanned for this sub-string, and if found, results in an alert condition.  The file scanning is optimized so that only new data added to the file is scanned on each check.
   1. This field supports Boolean AND search with multiple substrings using the plus sign, and Boolean OR using the comma, for example, s1+s2,s3+s4, meaning if substrings s1 AND s2 are found OR s3 AND s4 are found then there is a match.  Any combination of substrings using the plus and comma are accepted such as s1+s2+s3 or s1+s2,s3,s4, etc.  The comma has the highest precedence meaning combinations separated by comma are parsed 1st, and then within that, combinations with plus are parsed.
   2. This field also supports comparing and testing a numerical value as part of the search substring. The syntax for checking a numeric value as part of a search substring is as follows: <#GT nnnn>, <#LT nnnn> or <#EQnnnn>.  For example, you could specify your Search String as two substrings using the Boolean AND plus sign:  MEM:<#GT 1024000>+-<#LT 300000>
9. In the **Max Size(KB)** field, if specified, the file size in kilobytes (KB) is checked against this parameter and if it exceeds it, results in an alert condition.
10. The **Include Subfolders** checkbox, when checked and the File Path Name specified is a folder name, then all the 1st level subfolders are also included for monitoring using the same specified parameters.
11. The **Include All** checkbox, when checked and the File PathName specified uses a wild-card and the **Max Size** parameter is specified, then the total size of all files matching the wild-card is compared versus the ‘Maximum Size’; otherwise if not set, then each individual file’s size is compared versus the ‘Maximum Size’.
    1. When checked, and when the **NOT Check** checkbox is checked and the File Name specified uses a wild-card, then all files are included in the NOT check before the alert condition is triggered.  For example, all files matching the wild-card spec must change before a change alert notification occurs, or all files must be deleted before the file delete (file does NOT exist) alert notification occurs.
    2. When checked and the **Include Subfolders** is checked, and the File Name specified is a folder name, then the Max Size and File Count Threshold parameters apply to the total size of the folder and its 1st level subfolders or the total count of the files in the folder and its 1st level subfolders.
12. The **NOT Check** checkbox, when checked, that all the defined parameters are tested in the NOT condition. The simple example is the specified file does not exist (perhaps it has been deleted).
    1. For the Size Change, D/T Change, Max Size,and Search String parameters, if specified imply, the NOT of the parameter.  For example, the Size and/or D/T have NOT changed, the File is less than the specified Maximum Size, or the File does NOT contain the specified Search String.
13. The **Duration** field, optional parameter, if specified, defines the Duration in Minutes that the File conditions must exist in the 'matched' (that is, the Alert state) before the Alert notification is actually triggered.
14. The **AND Params** checkbox, when checked, specifies that a match must occur on all of the parameter fields above that have been specified (Boolean AND); otherwise, if not set, a match can occur on any of the parameter fields above that have been specified (Boolean OR).
15. The **File Count Threshold** optional field, if specified, the count of the files in the specified directory exceeds the specified threshold, results in an alert condition.
16. In the **Selections** Tree, select the machines that you want to monitor with this rule.

**Configure the Schedule**

The **Schedule** tab of a monitoring rule allows users to define how frequently the rule will alert. This can be done by adjusting the following fields:

* **Alert Every Time**: Defines whether an alert is generated every time the conditions are on the previous tab are met.
  + When checked the alert is generated every time the conditions are met.
  + When unchecked, the alert is only generated if the alert conditions are met, and the Minimal Notification Interval is exceeded since the last alert for this type.
* **Minimal Notification Interval**: Defines the minimal interval that must elapse between events for this alert before another alert will be generated.
  + The Alert Every Time checkbox must be unchecked in order to use this option.
  + For ServerWatch IP Services, this also defines the minimum elapsed time since a service is first detected as down or failed before an alert is generated.
* **Active Only if Server 'Owns".... This Cluster Group**: This option is for monitoring machines that are apart of a cluster. If the checkbox is checked, then the rule is monitoring and will alert only if the server is a member of a cluster, 'owns' the specified Cluster Group and the specified Cluster Group is 'Online'.

**Additional Configuration**

For additional configuration options please see the following articles:

* Enabling Notifications:
  + [Configure Email and Text Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024446933)
  + [Configure SNMP Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024726913)
  + [Configure Syslog Alert Notifications](https://support.goliathtechnologies.com/hc/en-us/articles/360024346594)
* [Configure Custom Remediation](https://support.goliathtechnologies.com/hc/en-us/articles/360024446633)