

Configure File Watch Rule for Goliath Performance Monitor

Goliath Performance Monitor's (GPM) File Watch monitors your files and folders on your Windows servers/workstations using our Goliath Intelligent Agent to alert on specified conditions in real-time.

Instructions on how to configure a File Watch rule:

1. Name the Monitoring Rule in the 'Rule Name', as well as define the description and the severity.
2. In the "File Path Name" field, define the "fully qualified path" name 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.
 - a. 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.
 - b. 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).
 - c. 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.* !log.tx1 !log.tx2 !*.tx3
3. The "Change ID" checkbox, when checked, the file's current size is determined, and any subsequent change to that size results in an alert condition.
4. The "Change DT" 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.
5. 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.
 - a. The 'Search String' 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.

- b. The 'Search String' field 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>
6. 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.
7. 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.
8. The "Include All" checkbox, when checked and the File PathName specified uses a wild-card and the 'Maximum 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'.
 - a. 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.
 - b. When checked and the Include Subfolders is checked, and the File Name specified is a folder name, then the Max Size and FileCount 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.
9. 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).
 - a. 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.
10. 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.
11. 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).
12. 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.
13. In the "Selections" Tree, select the machines that you want to monitor with this rule.