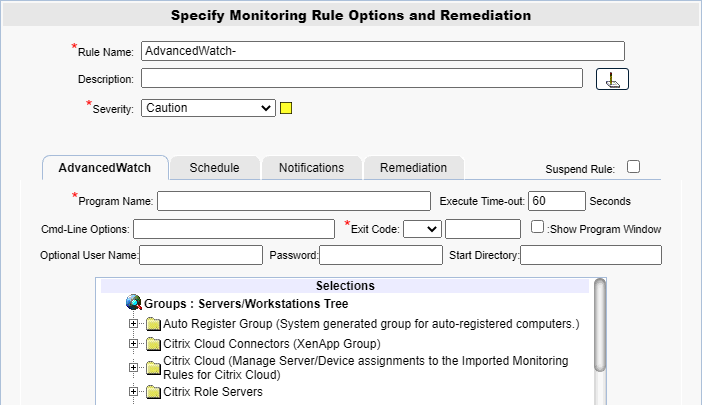
**Configure Advanced Watch Rules**

**This article was updated to support v12.0 of Goliath Performance Monitor.**

Goliath Performance Monitor (GPM) Advanced Watch monitors your Windows servers/workstations by executing any Windows program, command, script, or batch file executable that you provide. It runs the executable periodically on the monitored server/workstation according to a schedule that you specify.



**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 **Advanced 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, **AdvancedWatch** is where you will define what is to be configured.
5. In the **Program Name** field, define the name of the program that Goliath will run.
   1. For example, Windows Powershell, Command Line, etc.
   2. This must be a fully qualified program name path.
   3. In order to access the network share, the agent must have rights to the share
   4. Environment variable substitution is supported when bracketed with the percent character, for example, **%SystemRoot%**
   5. Examples:
      1. Windows Powershell

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

* + 1. Command Line

C:\Windows\system32\cmd.exe

\\1.1.1.1\c$\temp\test.bat

1. You can optionally specify an **Executable Time-Out** value and Goliath will terminate the executable if it does not complete on its own before the timeout expires.
2. In the **Cmd-Line Options** field, define an 'Argument' string that will be passed to the program named in the **Program Name** field
   1. Please note, the parameters are case sensitive and must be upper case.
   2. Environment variable substitution is supported when bracketed with the percent character; for example, **%SystemRoot%**.
   3. If you are returning an Exit code from your script for processing in Goliath, please see the next step for some options surrounding how you call the script.
   4. If referencing a file, the location will be based on the machine where the execution is taking place. If the file is not local, the agent must have rights to the network share/location.
   5. Examples:
      1. Windows Powershell:

"& 'C:\Program Files\MonitorIT\Scripts\test.ps1'"

$reg = ((GP -Path 'HKLM:\SOFTWARE\Citrix\VirtualDesktopAgent\State' -Name Registered).Registered); exit $reg

"& '\\10.20.20.20.\Scripts\test.ps1'"

* + 1. Command Line

net stop Spooler

1. In the **Exit Code** field, optionally define an exit code. When an exit code is defined, the Goliath Agent will make compare the script/programs exit code to what is defined in the rule. If the comparison fails, an alert will be generated.
   1. For example, if the Exit Code in the rule configuration is **=0** but the program/script returns an exit code of **5**, an alert will trigger.
   2. For Exit Codes coming back from a PowerShell script, there are two configuration options:
      1. Option 1 - define the Exit Code in your PowerShell using **[Environment]::Exit(###)** where **###** is the Exit Code number you want to pass back to Goliath.
      2. Option 2 - define the Exit Code using a powershell variable within the script, for example **$exitCode = #**. When using a variable for the exit code, you then want to call the variable in the **Cmd-Line Options** field with the following format:

"& 'c:\commands\ExitCodeTest.ps1'"; exit $exitCode

1. The **optional username and password** fields are where you would, if necessary, define a user that the Goliath Agent will use to run the executable in this user’s security context.
2. In the **Start Directory** field, optionally specify the location where the agent will create the process and run the executable from.
3. Set the **Show Program Window** check box to have the executable window GUI appear on the screen or uncheck to run the executable in the background; hidden.

**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.
* **Maximum Notification Interval**: Defines the maximum number of times you want to be notified during a continuous failure situation.
  + A value of 0 means no maximum is defined so you will continue to be notified according to your Alert Every Time and Minimal Notification Interval settings.
  + A non-zero value means that after you have been notified the number of times defined in the Maximum Alert Notifications, and according to your Alert Every Time and Minimal Notification Interval settings, you will not be notified again.
* **Notify On Restore**: Defines whether a 'Restore' alert is generated if you have previously been alerted due to a failure.
  + There is always a Notify on Restore for a ServerWatch for IP Service
* **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'.
* **Alert 1st Time After \_\_\_ Failures**: This field allows for the alert to only trigger if the event is happening continuously.
  + For example, if 5 is defined, the event will not trigger until it has occurred 5 times or more in a row. Events 1-4 will be ignored.
* **Run Program Every**: This is a required field where you would designate how frequently the program will execute
* **Start At Date/Time**: Defines the starting point for the executable. The Goliath Agent attempts to always run the executable at a periodic rate that is an even increment from the Start Date/Time plus the Run Program Every rate

**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)