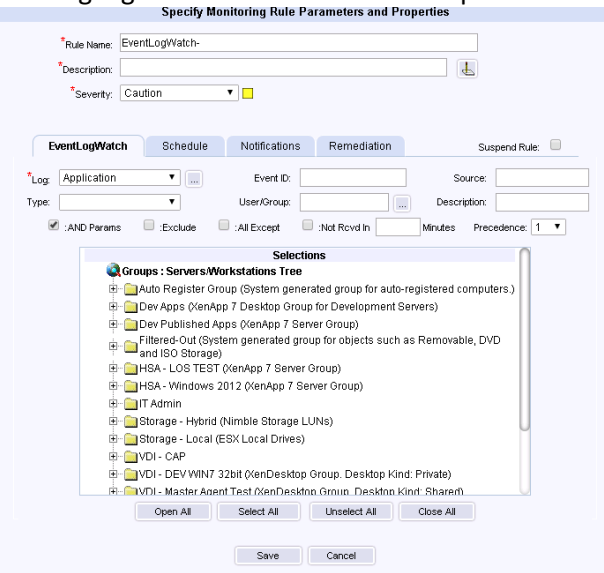
# Configure EventLog Watch Rule for Goliath Performance Monitor

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




## Instructions on how to configure an EventLog Watch rule:

### EventLogWatch Tab

1. Name the Monitoring Rule in the 'Rule Name', as well as define the description and the severity. If you would like to view events under the 'Log Management' tab, but not actually alert on them then you want to set the severity to be 'Normal'.

2. In the "Log" field, define the Event Log name that you would like to monitor. This field is required. If you select the "…" after the "log" field you can define a custom EventLog to monitor.

3. In the "Event ID" field, you can optionally specify an Event ID to monitor.

4. In the "Source" field, you can optionally specify a log source to monitor.

5. In the "Type" field, you can optionally specify a log type to monitor. If there are other optional parameters defined, then an empty or blank Event Log Type is ignored. If there are NOT any other optional parameters defined, then the "empty" Type is interpreted to mean "all" types, and every event for the given Event Log will cause an alert.

6. In the "User/Group" field, you can optionally specify a username to monitor. You can specify more than one user or group my separating them with a comma. This field is not case sensitive. You can also enter an Active Directory Group Name so that any user that is a member of the Group would be considered a match. You can specify multiple Group Name parameters by separating with a comma. You can also mix User and Group names. Click the "…" button to the right of the field to access the Active Directory options.

7. In the "Description" field, you can optionally specify a description substring to monitor. If separated by a comma, they are treated as a Boolean OR; if separated by a plus sign (+), they are treated as a Boolean AND. You CANNOT mix substrings with a comma and a plus.

8. The “AND Params” check box will cause an Event Log alert if any of the parameter fields match (Boolean "Or" check) when the box is NOT checked. When checked, it requires all the defined parameter fields to match (Boolean "And" check).

9. The “Exclude” checkbox, when checked, EXCLUDES any Event matching the criteria defined by the various parameter fields above, and no alert condition occurs.

10. The “All Except” checkbox, when checked, All Events Except those matching the criteria defined by the various parameter fields above, cause an alert condition to occur.

11. The “Not Recvd In __ Minutes” checkbox, when checked, to generate an alert when any of the events matching the specified criteria do NOT occur within the minutes specified. Any of the events that match criteria will reset the timer.

12. The “Precendence Field” specifies how this rule is handled if the received Event Log event satisfies the criteria of multiple Monitoring Rules. A higher-precedence (1 is higher than 2, etc.) trumps Monitoring Rules with a lower precedence.

13. In the “Selections” Tree, select the machines that you want to monitor with this rule

## Schedule Tab

In this tab you will define how often you would like the alerts to trigger.

**Required Options** *(one of the below must be selected)*:

- Alert Every Time Checkbox
    - When this option is selected, you will receive the alert every time the specified condition is met.

- Minimal Notification Interval
    - When selected, it defines the minimal interval that must elapse between events for this alert before another alert will be generated. For example, if the interval is 15 minutes and the condition is being met, you will receive 1 alert every 15 minutes instead of being alerted at each occurrence. However, each alert occurrence is considered unique based on the details. For example, an Event Log alert is considered the same based on being the same Event Type and ID, from the same server/workstation.

**Additional Option**:

- When Any Single Event Occurs ____ Times In _____ Seconds
    - This field acts as an additional filter so that if an alert condition exists only after a specific event occurs the defined amount of times within the specified time frame.
    - Each event that matches the criteria is treated discretely when counting. For example, if you have a rule that is monitoring for multiple events, an event with ID 500 is counted separately from ID 501, even though both match the rule.
        - If the ‘Combine All’ checkbox is checked, then matching events are not treated discretely and are combined together when counting.
        - The ‘Include Description’ checkbox when checked causes the Event Description to be included as part of the set of parameters that are checked for a match on the same event; if unchecked the Event Description is not included in the check.

- When the Log Only When Criteria Met checkbox is checked the Event is written to the database, otherwise the Event is filtered and not written to the database.