Goliath Log Management – EventLog Archives

This document will guide you through the multiple functions on the EventLog Archives page of the technology.

Table of Contents

I. Manage Archive Schedules

The 'Manage Archive Schedule' functionality provides the option to create one or more Archive Schedules to archive and optionally upload the selected archived Event Log files, from the selected servers/workstations, based on 1 of 4 conditions. Archived Event Log files are stored in a compressed GZIP format which achieves 20 to 1 and as much as 30 to 1 compression. The files are automatically uncompressed by Goliath when one chooses to 'View Archived Event Logs', but can also be manually decompressed by WinZip or any other Windows compression utility that supports the GZIP format. Archived Event Log files are named by appending the machine name where the file originated plus the date/time the archive file was created. For example, a standard "AppEvent.evt" file name for an Application Event Log would be named "AppEvent_MachineName_mmddyy_hhmmss.gz" after it was uploaded in the native EVT format and compressed.

A. Create a New Archive Schedule

1. Open Goliath Performance Monitor and click the **'Log Management'** tab, and then the **'EventLog Archives'** submenu
2. Click the first button for **'Manage Archive Schedules'**
3. The **'Manage Archive Schedules'** pane will appear, click the **'New'** button in the middle of the screen
4. At the top of the page, in the section **'Select Event Logs at Archive'**, check the boxes for the Event Logs that you would like to archive.
    a. For **'User Custom Log(s)'**, click the button labeled **'…'** to choose the custom log if it has already been defined in the technology. If you would like to monitor it a new custom log, click the **'new button'** and in the text box enter the Event log name and the full path of the EventLog separated by a coma. Enter each event log on a new line.
5. Under **'Specify Automatic Archive Schedules'** complete the following options:
    a. Give this archive schedule a unique name
    b. Choose one of the 4 options for how often the event logs are archived based on
        i. Specific dates and times
        ii. Log record count
        iii. Log File Size (KB)
        iv. Log File Size (%)
    c. Choose one of the archive actions:
        i. Clear the event logs when above condition is met
        ii. Archive the Event Logs locally on the machine
        iii. Archive the Event Logs Centrally
            1. The default location is in the install directory of the Goliath Server ("…\MonitorIT\Archive") where the archived files are stored in a subfolder based on machine name.
            2. You can override the default archive folder and specify an alternative folder that can be on the same machine as the Goliath Server, or reachable from the Goliath Server via a mapped drive, or via a UNC path by clicking the button labeled **'Specify Central Archive'**
    d. At the bottom of the page, use the **'Servers/Workstations Tree'** to select the machines in which you'd like to archive the Event Logs for.
    e. When finished, click the **'Save'** button in the middle of the page.

B. Modify/Remove an Archive Schedule

1. Open Goliath Performance Monitor and click the **'Log Management'** tab, and then the **'EventLog Archives'** submenu
2. Click the first button for **'Manage Archive Schedules'**
3. The **'Manage Archive Schedules'** pane will appear, use the dropdown menu in the middle of the pane to select the archive schedule that you would like to modify or remove.
4. Click the **'Edit'** or **'Remove'** button in the middle of the screen as appropriate.
5. If you are modifying the schedule, at the top of the page, in the section **'Select Event Logs at Archive'**, check the boxes for the Event Logs that you would like to add/remove from the archive.
    a. For **'User Custom Log(s)'**, click the button labeled **'…'** to choose the custom log if it has already been defined in the technology. If you would like to monitor it a new custom log, click the **'new button'** and in the text box enter the Event log name and the full path of the EventLog separated by a coma. Enter each event log on a new line.
6. Under **'Specify Automatic Archive Schedules'** modify the following options as appropriate:
    a. Modify the archive schedules name as appropriate
    b. Modify one of the 4 options for how often the event logs are archived based on as appropriate
        i. Specific dates and times
        ii. Log record count
        iii. Log File Size (KB)
        iv. Log File Size (%)
    c. Modify one of the archive actions:
        i. Clear the event logs when above condition is met
        ii. Archive the Event Logs locally on the machine
        iii. Archive the Event Logs Centrally
            1. The default location is in the install directory of the Goliath Server ("…\MonitorIT\Archive") where the archived files are stored in a subfolder based on machine name.
            2. You can override the default archive folder and specify an alternative folder that can be on the same machine as the Goliath Server, or reachable from the Goliath Server via a mapped drive, or via a UNC path by clicking the button labeled **'Specify Central Archive'**
    d. At the bottom of the page, use the **'Servers/Workstations Tree'** to select the machines in which you'd like to archive the Event Logs for.
    e. When finished, click the **'Save'** button in the middle of the page.

II. View Archived Event Logs

The **'View Archived Event Logs'** functionality allows one to view the Event Logs that have been configured with an archive schedule. One can specify specific Event Log conditions in which they'd like to see and Goliath will search through the archived logs and display the data within the technology.

1. Open Goliath Performance Monitor and click the **'Log Management'** tab, and then the **'EventLog Archives'** submenu
2. Click the button for **'View Archived Event Logs'**
3. The **'View Archived Event Logs'** pane will appear, use the following options to search for specific condition:
    a. **Select Archived Event Logs to View** – use the check box options to choose the logs you'd like to see
    b. **Select View filters** – configure filters based on type, event id, source, user/group, and description
        i. The **'Event ID'** field also accepts ranges (e.g. 532-550, 560-590) and you can also enter multiple event ids delimited by a coma.
        ii. 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.
        iii. In the **'Description'** field, you can optionally specify a description substring. 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.
        iv. The **'AND Params'** check box will look to see 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).
        v. When the **'Summary Counts'** checkbox is selected, it will roll up all like events and display a number count for how many times the event occurred. If unselected, it will show each individual entry.
        vi. When **'Exclude Desc/Catg'** is selected the technology will not display the description field text
    c. Click the **'Specify Archive'** button to choose the archive location
    d. Set the date and time for which you'd like to view
    e. At the bottom of the page, use the **'Servers/Workstations Tree'** to select the machines in which you'd like view the archived Event Logs for.
4. Please note, you can save your search specifications for later use by clicking **'Save Filter'** and giving it a unique name. The next time you come into the screen you'd then be able to select **'Load Filter'**
5. When ready click **'View'.**
    a. Please note, depending on the number of events that took place it may take a few minutes to load. You will be able to see the progress in the bottom left hand corner.

III. View Monitored Event Logs

The **'View Monitored Events'** functionality allows one to view the Event Logs that have been configured for monitoring and are saved in the Goliath database. One can specify specific Event Log conditions in which they'd like to see and Goliath will search through the database and display the data within the technology.

1. Open Goliath Performance Monitor and click the **'Log Management'** tab, and then the **'EventLog Archives'** submenu
2. Click the button for **'View Monitored Events'**
3. The **'View Monitored Events'** pane will appear, use the following options to search for specific condition:
    a. **Select Monitored Events to View** – use the check box options to choose the logs you'd like to see
    b. **Select View filters** – configure filters based on type, event id, source, user/group, and description
        i. The **'Event ID'** field also accepts ranges (e.g. 532-550, 560-590) and you can also enter multiple event ids delimited by a coma.
        ii. 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.
        iii. In the **'Description'** field, you can optionally specify a description substring. 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.
        iv. The **'AND Params'** check box will look to see 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).
        v. When the **'Summary Counts'** checkbox is selected, it will roll up all like events and display a number count for how many times the event occurred. If unselected, it will show each individual entry.
    c. Set the date and time for which you'd like to view
    d. At the bottom of the page, use the **'Servers/Workstations Tree'** to select the machines in which you'd like view the archived Event Logs for.
4. Please note, you can save your search specifications for later use by clicking **'Save Filter'** and giving it a unique name. The next time you come into the screen you'd then be able to select **'Load Filter'**
5. When ready click **'View'.**
    a. Please note, depending on the number of events that took place it may take a few minutes to load. You will be able to see the progress in the bottom left hand corner.

IV. View Current Event Logs

The **'View Current Event Logs'** functionality allows one to view the Event Logs that are currently on a given machine, regardless if they are configured for monitoring within Goliath. One can specify specific Event Log conditions in which they'd like to see and Goliath will connect to the machine and display the data within the technology.

1. Open Goliath Performance Monitor and click the **'Log Management'** tab, and then the **'EventLog Archives'** submenu
2. Click the button for **'View Current Event Logs'**
3. The **'View Current Event Logs'** pane will appear, use the following options to search for specific condition:
    a. **Select Current Event Logs to View** – use the check box options to choose the logs you'd like to see
    b. **Select View filters** – configure filters based on type, event id, source, user/group, and description
        i. The **'Event ID'** field also accepts ranges (e.g. 532-550, 560-590) and you can also enter multiple event ids delimited by a coma.
        ii. 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.
        iii. In the **'Description'** field, you can optionally specify a description substring. 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.
        iv. The **'AND Params'** check box will look to see 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).
        v. When the **'Summary Counts'** checkbox is selected, it will roll up all like events and display a number count for how many times the event occurred. If unselected, it will show each individual entry.
    c. Set the date and time for which you'd like to view
    d. At the bottom of the page, use the **'Servers/Workstations Tree'** to select the machines in which you'd like view the archived Event Logs for.
4. Please note, you can save your search specifications for later use by clicking **'Save Filter'** and giving it a unique name. The next time you come into the screen you'd then be able to select **'Load Filter'**
5. When ready click **'View'.**
    a. Please note, depending on the number of events that took place it may take a few minutes to load. You will be able to see the progress in the bottom left hand corner.

V. Set Maximum File Size

The '**Set Maximum File Size'** functionality provides the option to set the maximum log file size for selected Event Log files on selected servers/workstations. The size is in KB and is rounded to the nearest 64KB increment following the Windows behavior for these.