



Windows Event Log



Windows Event Log

Our Foglight Windows Event Log integration will provide:

Enhanced data collection

Enhanced Alerting

- More control
- Extended throttling capabilities



Windows Event Log – Solution

Simplify
Management
of
Incoming
Events



Alarming

- One alarm per unique event
- One email per unique event
- Sends summary emails per incoming events



Specify how long an alarm remains active before it is auto-cleared for specific event(s).

Java Regular Expressions Supported



Event throttling - an event may be generated 'x' amount of times during a specified period.

Java Regular Expressions Supported

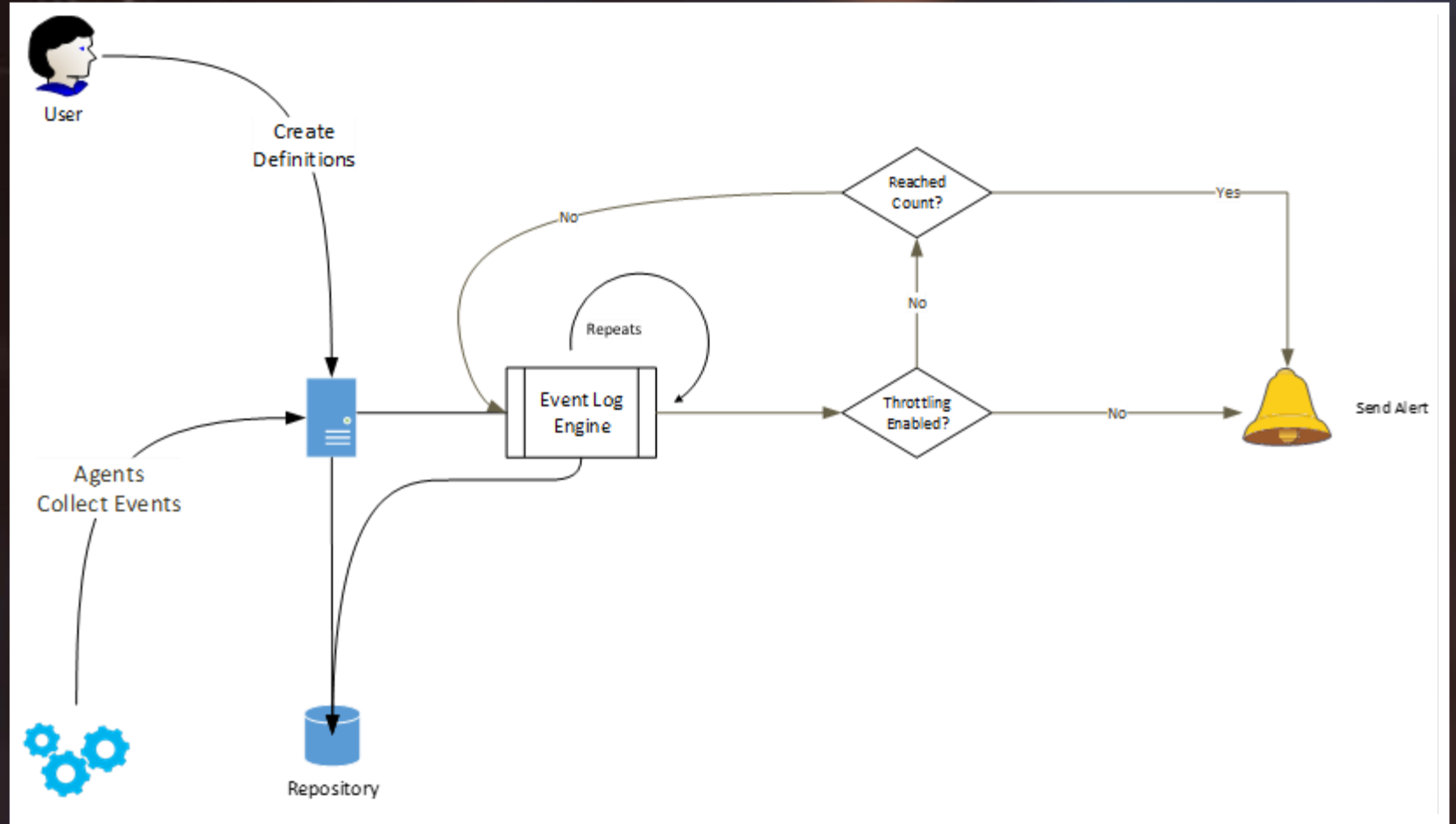


The ability not to alert on specific event(s).

Java Regular Expressions Supported



Windows Event Log — Flow



Windows Event Log – Changing Settings

Remote Administration of the solution across servers

File Event Log Registry Settings - Local FMS

Save | Undo | Filter

| Name ▲ | Value | Scoping | | | |
|---|------------------------|---------|---|---|---|
| | | | | | |
| Debug | | | | | |
| PSO.FileEventLog.Debug | true | | | | Whether or not to enable debug mode in the File Event Log |
| Error Log | | | | | |
| Alarm | | | | | |
| PSO.FileEventLog.Alarm.GenerationSeverity | Warning,Critical,Fatal | + | + | - | Defines the Foglight severity levels that will cause an alarm |
| Individual Notification | | | | | |
| PSO.FileEventLog.Email.NotificationSeverity | Warning,Critical,Fatal | + | + | - | Defines the Foglight severity levels that will trigger an email notification |
| PSO.FileEventLog.Email.Recipient.Critical | | + | + | - | Comma separated list of email addresses to which to send critical notifications |
| PSO.FileEventLog.Email.Recipient.Fatal | | + | + | - | Comma separated list of email addresses to which to send fatal notifications |
| PSO.FileEventLog.Email.Recipient.Warning | | + | + | - | Comma separated list of email addresses to which to send warning notifications |
| Summary Notification | | | | | |
| PSO.FileEventLog.Email.NotificationSeverity.Summary | Warning,Critical,Fatal | + | + | - | Defines the Foglight severity levels that will trigger a summary notification |
| PSO.FileEventLog.Email.Recipient.Summary | | + | + | - | Comma separated list of email addresses to which to send summary notifications |



Windows Event Log – Rule Management

Remote Administration of the solution across servers

The screenshot displays the 'Windows Event Log Rule Management - Local FMS' interface. On the left is a navigation pane with 'Expert View' selected and a list of 'Foglight Servers' including 'Local FMS' and 'fms-5756 8080'. The main area shows a table of rules with columns for 'Category / Title', 'Enabled', and a description. The rules are grouped into 'Alerting', 'Clean Up', and 'FMS' categories.

| Category / Title | Enabled | Description |
|---|---------|--|
| Alerting | | |
| <input type="checkbox"/> Windows Event Log | | Generates alarms for event logs based on the Throttle definitions. |
| <input type="checkbox"/> Windows Event Log Record | | Generates alarms for event logs based on the Throttle definitions. |
| Clean Up | | |
| <input type="checkbox"/> Auto Clear Alarms | | Handles auto clearing of the various generated event log alarms based on the def |
| FMS | | |
| <input type="checkbox"/> Ping | | Handles updating the FMS Ping Time |



Windows Event Log – Throttling Definition

The image shows a screenshot of the Windows Event Log console. A dialog box titled "Add Throttle Definition" is open, allowing the user to configure throttling settings for a specific service. The dialog box contains the following fields and options:

- Service Name:** A dropdown menu.
- Host Name:** A text box containing the wildcard character `.*`.
- Log File:** A text box containing the wildcard character `.*`.
- Category:** A text box containing the wildcard character `.*`.
- Source:** A text box containing the wildcard character `.*`.
- Event ID:** A text box containing the wildcard character `.*`.
- User:** A text box containing the wildcard character `.*`.
- Message:** A text box containing the wildcard character `.*`.
- Duration (Seconds):** A text box containing the value `300`.
- Count in Duration:** A text box containing the value `5`.
- Merge:** A checked checkbox followed by a dropdown menu. The dropdown menu is open, showing three options: `PER_DEFINITION` (highlighted in blue), `PER_DEFINITION`, and `PER_HOST`.

At the bottom right of the dialog box, there are two buttons: "Add" and "Cancel".

Windows Event Log – Auto Clear Definition

The screenshot displays the Windows Event Log application interface. At the top, there is a menu bar with options: Add, Save, Undo, Delete, and Edit Time. A search bar is located on the right side of the menu bar. Below the menu bar is a table with the following columns: Service Name, Host Name, Log File, Category, Source, Event ID, User, Message, and Time (Minutes). The table is currently empty, and the message "There Is No Data To Display" is centered below the column headers.

An "Add Auto Clear Definition" dialog box is open in the foreground. It contains the following fields:

- Service Name: [Dropdown menu]
- Host Name: *.*
- Log File: *.*
- Category: *.*
- Source: *.*
- Event ID: *.*
- User: *.*
- Message: *.*
- Time (Minutes): 15

At the bottom right of the dialog box, there are two buttons: "Add" and "Cancel".



Windows Event Log

System Requirements



Minimum required
FMS version

5.9.3



Supported
Database
Minimum
Version

| | |
|------------|------------------------------|
| MS SQL | 2008 v 10.0.1600 or later |
| Oracle | 9i R2 |
| MySQL | 5.1.45 |
| PostgreSQL | 9.4.0 |





Performance Monitoring customized to your unique environment

Ten plus years of providing Professional Services to Quest customers revealed these enhancements to be most requested modifications.

Let us take Foglight's out of the box capabilities and enhance for your unique environment.

Contact: Sales@LightSpeedPM.com

