GFI White Paper

How to configure SharePoint event collection with LOGbinder SP and GFI EventsManager™

Contents

Overview 3

Prerequisites 3

Configuration 3

- Adding new SharePoint servers as event source 3
- Additional event processing rules 3
- Additional event browser queries 4

Technical difficulties and support 4

Overview

This document explains how to configure and use GFI EventsManager to collect Microsoft SharePoint audit events which have been processed by LOGbinder SP in order to make the information more readable and manageable.

The features which are referred to in this document add the following extra functionality to GFI EventsManager:

- Custom log to collect LOGbinder SP audit events
- Additional rules to process SharePoint events
- Additional queries to view SharePoint events in the events browser

Prerequisites

This procedure assumes that a functional installation of Microsoft SharePoint Server or SharePoint Services is already in place.

Further we assume that LOGbinder SP has been installed and configured on the SharePoint server. For more information on LOGbinder SP please follow these links:

- Download: http://www.logbinder.com/form.aspx?action=download
- Requirements: http://www.logbinder.com/products/logbindersp/resources/requirements.aspx
- Support: support@logbinder.com (866-749-2048)

GFI EventsManager does not include a license for LogBinder. You need to purchase a LogBinder license. You can find out more information about LogBinder licenses and pricing here: http://www.logbinder.com/products/logbindersp/pricing.aspx

Once LOGbinder SP is installed on the SharePoint Server it will start writing events either in the security event log or in a custom log called 'LOGbinder SP' depending on the configuration. This setting is very important, however, in order to configure GFI EventsManager appropriately. For more information click on this link: http://www.logbinder.com/products/logbindersp/agent.aspx

An installation of GFI EventsManager version 2011 (build 20110407) and the GFI EventsManager ReportPack 2011 (build 20110401) is also required.

NOTE: All further references to 'SharePoint events' in this document assumes that these are events which have been processed by LOGbinder SP and saved in a Windows event log in the usual LOGbinder SP format.

Configuration

Adding new SharePoint servers as event source

New SharePoint servers can be added as an event source to the GFI EventsManager configuration by right-clicking into the 'SharePoint servers' group section and selecting 'Add new event source' – Events from these sources will then be collected for the first time as soon as they are added.

The properties of this group can be customized further to meet individual requirements.

Additional event processing rules

The default rules to process and evaluate SharePoint events can be found in the GFI EventsManager configuration under Configuration > Event Processing Rules > Windows Event Logs > SharePoint Audit. Currently there are three rule sets which contain various rules to evaluate different event types plus one additional rule called 'Archive SharePoint Audit Events' which will capture and archive any event which has not matched any other rule with low priority. This is done to prevent any loss of data at the initial time of setup. However, once additional processing rules have been configured and all events of interest are being captured by other rules this 'catch-all' rule can be disabled.

There are multiple ways to create new custom processing rules for SharePoint events which do not match any of the default rules. The easiest way is described in the steps below:

1. Open the GFI EventsManager UI and select the Events Browser tab.
2. Make sure the Windows Events Browser is active and select 'Other Events' > 'LOGbndSP'. This will display all SharePoint events currently in the database.
3. Select any event which has been captured by the generic 'Archive SharePoint Audit Events' rule and for which a new processing rule needs to be created.
4. Right click the event and select 'New rule from selected event'.
5. Accept the default conditions for the newly created event and click OK.
6. The new rule will be created in the 'Custom Rules' folder but can be moved to any rule set in the 'SharePoint Audit' folder per drag-and-drop.

Additional event browser queries

Creating additional queries in the events browser is described in the GFI EventsManager user manual, section 4.2. (http://support.gfi.com/manuals/en/esm2011/esm2011manual.1.21.html)

Technical difficulties and support

In case of technical difficulties with any of the components involved in the process described in this document, it is important to first evaluate which part of the process is failing in order to contact the appropriate support personnel.

1. No default SharePoint logs (*.log files) are being generated or the SharePoint audit settings don't seem to work as expected.
   » This part of the process is related only to SharePoint itself and should be handled through Microsoft's support team or technical forums.
2. LOGbinder SP does not seem to process any events or does not generate any events in the Windows event logs.
   » This part of the process is related to LOGbinder SP and will be handled by the LOGbinder support team which can be contacted via email (support@logbinder.com) or phone (866-749-2048).
3. Events are being generated on the SharePoint server but GFI EventsManager is unable to collect them or does not process them according to the configured processing rules.
   » This part of the process is related to GFI EventsManager and will be handled by our own support team which can be contacted via http://support.gfi.com.

GFI 2321 oct11

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit http://www.gfi.com/contactus

Disclaimer

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.