

NT/2K/XP Server Event Log Reporting

Gravity Square Inc. – Windows NT/2K Server Event
Log Gatherer Database Application

White Paper

Abstract

Gravity Square's Windows NT and 2000 Event Log Gatherer Database Application is a web-based database application that allows system administrators to view event log entries on multiple servers from a single console, based on criteria administrators can define, even if a server is off line or unresponsive. Gravity Square's Event Log Gatherer (GSELG) decreases the amount of time administrators must spend to view all event log messages from all servers, and allows administrators to view all servers' events from a single web interface. This application also allows administrators to view only those events that are relevant at any given time, and only from specific servers, further reducing the time spent researching issues on servers.

This paper provides general information on the Event Log Gatherer application, how it allows administrators to review all server event logs from a single console, how it allows administrators to research server issues, even from unresponsive servers, how to set up this application, and where to go for further information on the Event Log Gatherer and Gravity Square, Inc.

CONTENTS

INTRODUCTION2

EVENT LOG GATHERER.....3

INSTALLING EVENT LOG GATHERER DATABASE AND APPLICATION.....4

Event Log Gatherer Database and Application 4

Installation Details 4

Pricing and Packaging Information 4

MORE INFORMATION.....5

Contact Information 5

APPENDIX A: SYSTEM REQUIREMENTS6

APPENDIX B: SUPPORT DETAILS.....7

INTRODUCTION

Administrators should continuously audit the event logs on each Windows NT and Windows 2000 systems that they manage. As the number of servers managed increases, this task requires more time and can become a burden. The Event Log Gatherer database application pulls the event log entries from each designated server into a single database, and provides a web-based interface from which administrators can view all or selected event log entries from their servers. This single interface reduces the number of logons required to audit the event logs on each server, and as events are pulled from the server into a database, administrators can view events even from servers that have gone off line.

Administrators can view server events based on the following criteria:

- All designated servers, selected servers, or a single server
- Range of dates/times or specific time period
- All events, selected types of events, selected source of events, or any number of selected event IDs

The GSI Event Log Gatherer significantly reduces the amount of time required to audit and review all server events, or to find a specific event on a single server. Daily administration of servers is simplified and administrators may not even have to visit the server room for long periods of time, and can administer their servers from the desktop. The Event Log Gatherer permanently clears all designated event types from the server, further reducing the administrator's workload and reducing the risk of losing important log entries if a log fills up completely; administrators do not have to periodically purge event logs when they reach their storage limits. Finally, administrators do not need to repair a server that has halted, locked or experienced a Blue Screen Stop before the event log can be viewed, as event logs will be pulled from the server as long as it is responsive and on line, based on a refresh interval that the administrator defines. This allows administrators to view the events that may have led to the specific server experiencing a Blue Screen, whereas normally this information would not be available immediately.

EVENT LOG GATHERER

The Event Log Gatherer database application allows administrators to collect server event log entries automatically, enter them into a database, and view entries based on criteria that the administrator defines. Administrators will never have to log onto any production and test server and manually audit the event logs again - the GSI Event Log Gatherer Application provides a single interface for all event log entries.

The GSI Event Log Gatherer offers:

- A single repository for all event log data
- An easy to use, web-based interface that administrators can access from anywhere on the network
- The ability to search for a specific event based on its ID, type, or source, or to see all events for a user-defined period of time

The Event Log Gatherer database application runs as a Windows NT\2000 service, accesses locally or remotely a SQL or MSDE database, has no client agents, and consumes virtually no system resources on the targeted servers. The Event Log Gatherer Interface allows administrators to define exactly which servers, what timeframe, and which events to view. Administrators never have to log onto managed servers in order to view event log entries again.

INSTALLING EVENT LOG GATHERER DATABASE AND APPLICATION

Event Log Gatherer Database and Application

The Event Log Gatherer Database and Application operate as a client-server application. The components include an application that runs as a service on a Windows NT\2000 system, database server software such as Microsoft SQL Server 7.0, SQL Server 2000 server, or Microsoft Data Engine (MSDE), and a web-based interface with COM+ components. The three components may run on the same server or on separate servers altogether.

Installation Details

GSI Event Log Gatherer database and application are installed by executing simple batch files. These batch files create the database, install the server service, create the COM+ components, and create the web server virtual directories. Once those components are created, administrators simply log onto the application, designate servers that are to be targeted by the application, and create and save reports that can be used to view event log entries at any time.

- GSI Event Log Gatherer uses SQL or Integrated NT security and, properly managed, takes up very little disk space on the database server
- GSI Event Log Gatherer allows administrator-level and user-level access via the web interface, allowing non-administrative staff to view event log entries, but not to change any settings or add or remove servers
- GSI Event Log Gatherer's server service only targets the servers that are specified by administrators; servers may be included or excluded at the administrator's discretion

Pricing and Packaging Information

Gravity Square offers a 30-day evaluation copy of the Event Log Gatherer available for download at <http://www.gravitysquare.com/products/gatherer.htm>. The evaluation copy, which is a time-limited full version of the product, can be upgraded to a licensed product via the security key. The evaluation software package includes all of the latest pricing information for this product.

Pricing information can be also obtained at:

mail: elg@gravitysquare.com
fax: 206.524.4159

Packaging

The Event Log Gatherer is distributed by Web download and CD-ROM.

If an order requires additional services have your reseller contact us directly at 206.669.8341.

MORE INFORMATION

Gravity Square is the leader in planning, designing, and implementing desktop management solutions. These management solutions, including the GSI Advanced Scheduler, the Software Distribution Load Balancer for SMS 2.0, and the Event Log Gatherer Database Application, have been successfully deployed to over 25,000 machines – and these management solutions have already paid for themselves.

President and CTO Ian Turek, has written the book on Microsoft System Management Server 2.0 – MCSE SMS 2 EXAM CRAM, and his expertise and innovation enable Gravity Square to deliver products and services that are second to none.

Contact Information

For more information on our products and services visit Gravity Square's website at <http://www.gravitysquare.com>, e-mail info@gravitysquare.com, or write, phone or fax Gravity Square Inc. at

Gravity Square
5041 46th Ave. NE
Seattle, WA 98105

Phone: 206.669.8341
Fax: 206.524.4159

**APPENDIX A: SYSTEM
REQUIREMENTS**

Event Log Gatherer contains three components that can be installed on one, two, or three Windows NT/2000 systems. The current version of the Event Log Gatherer is available only for x86 based computers. Windows NT/2000 administrative privileges are required for the installation.

Event Log Gatherer Service	<ul style="list-style-type: none">Any (x86) Windows NT or Windows 2000 systemMDAC 2.6 SP2 or higherAdministrative privileges required for the installation
Event Log Gatherer Database	<ul style="list-style-type: none">MS SQL Server 7.0, SQL Server 2000, or MSDE database systemMDAC 2.6 SP2 or higherPermissions to create database are required
Event Log Gatherer Web Component	<ul style="list-style-type: none">IIS 5.0 or above running on Windows 2000 systemMDAC 2.6 SP2 or higher

APPENDIX B: SUPPORT DETAILS

Gravity Square is available for consultation and follow-up services as stated by a contractual agreement between all parties involved.