Monitoring Syslog Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

One of the first places to look for warning or error messages in UNIX operating system is Syslog file. Syslog is responsible for gathering and saving all the error and warning messages from the system. The error and warning messages are generated by programs and sometimes by the kernel itself. It is important to look and monitor at syslog log's on a regular and continual basis. eG Enterprise lends helping hands to administrators in achieving this task.

Chapter 2: How to Monitor Syslog Server using eG Enterprise?

eG Enterprise monitors the Syslog Server in an agent-based manner. The eG agent installed on the target host periodically monitors the Syslog file for specific patterns of errors/warning messages.

2.1 Managing the Syslog Server

The eG Enterprise cannot automatically discover the Syslog Server so that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a Syslog Server component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select Syslog as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

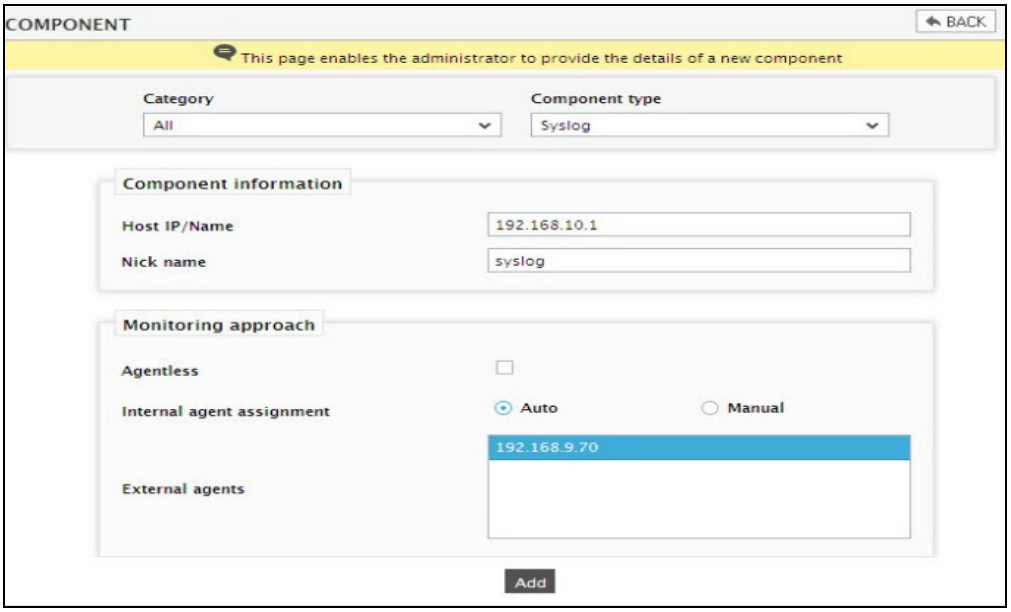

Figure 2.1: Adding a Syslog server

4. Specify the **Host IP/Name** and the **Nick name** of the Syslog server in Figure 2.1. Then, click the **Add** button to register the changes.

5. When you attempt to sign out, a list of unconfigured tests appears.

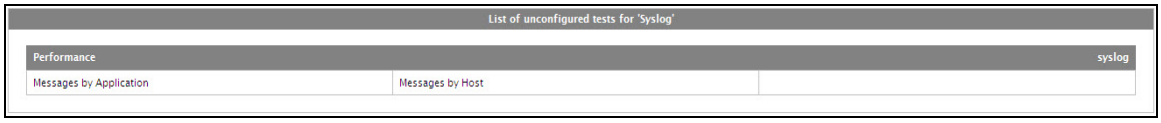

Figure 2.2: List of Unconfigured tests for the Syslog server

6. Configure the tests in the list of unconfigured tests one after another. To know the details on configuring these tests, refer to **Monitoring a Syslog** chapter.
7. Finally, signout of the administrative interface.

Chapter 3: Monitoring a Syslog

eG Enterprise provides a specialized Syslog monitoring model (see Figure 3.1) to periodically check the Syslog file for specific patterns of errors/warning messages. If messages that match the configured patterns are found, eG Enterprise alerts administrators to them, so that they can initiate the necessary remedial measures.

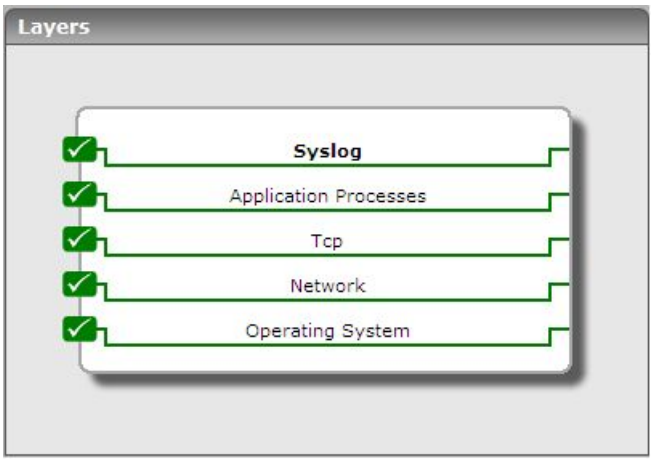

Figure 3.1: The layer model of a Syslog

Since the bottom 4 layers have been dealt with extensively in the *Monitoring Unix and Windows Servers* document, the sections to come will discuss the first layer of the layer model only.

3.1 The Syslog Layer

Using the tests mapped to this layer, you can scan the syslog file for specific error/warning message patterns related to hosts/applications/general.

Figure 3.2: The tests mapped to the Syslog layer

3.1.1 SysLogMon Test

This test mines the syslog file and reports the number of general error/warning events logged in the log file.

Target of the test : A Syslog file

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every *patternName* configured in the Include Patterns text box.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens. By default, this is NULL.
Exclude Patterns	Here, specify a comma-separated list of error or warning message patterns to exclude from monitoring. Your pattern specification can be of any of the following formats: **error* or *warning messages**. This parameter is set to *none* by default, which indicates that no message will be excluded from monitoring.
Include Patterns	Here, specify a comma-separated list of error or warning message patterns to be

Parameter	Description
	monitored. The format of your specification should be: *patternName:Pattern*, where *patternName* refers to the unique name that you assign to every pattern configuration, which will appear as the descriptor of this test, and *Pattern* refers to any message pattern of the form **error* or *warning messages**. Multiple pattern specifications can be provided as: *patternName1:Pattern1,patternName2:pattern2*. This parameter is set to *all:all* by default, which indicates that all error/warning messages will be monitored by default.
SyslogFile	Specify the full path to the syslog file to be monitored.
RotatingFile	By default, the RotatingFile parameter is set to **False**. To instruct the eG Enterprise system to monitor newer log files also, set this parameter to **True**. Otherwise, set it to **False**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of messages	Indicates the number of messages in the specified Syslog file that matched the configured pattern.	Number	The detailed diagnosis of this measure, if enabled, will provide the details of the error/warning messages logged in the log file.

3.1.2 Messages by Host Test

This test mines the syslog file and reports the number of host-related error/warning events logged in the log file.

Target of the test : A Syslog file

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the every *patternName* configured in the Include Patterns text box.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens. By default, this is NULL.
Exclude Patterns	Here, specify a comma-separated list of error or warning message patterns to exclude from monitoring. Your pattern specification can be of any of the following formats: **error* or *warning messages**. This parameter is set to *none* by default, which indicates that no message will be excluded from monitoring.
Include Patterns	Here, specify a comma-separated list of error or warning message patterns to be monitored. The format of your specification should be: *patternName:Pattern*, where *patternName* refers to the unique name that you assign to every pattern configuration, which will appear as the descriptor of this test, and *Pattern* refers to any message pattern of the form **error* or *warning messages**. Multiple pattern specifications can be provided as: *patternName1:Pattern1,patternName2:pattern2*. This parameter is set to *all:all* by default, which indicates that all error/warning messages will be monitored by default.
SyslogFile	Specify the full path to the syslog file to be monitored.
RotatingFile	By default, the RotatingFile parameter is set to **False**. To instruct the eG Enterprise system to monitor newer log files also, set this parameter to **True**. Otherwise, set it to **False**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability

Parameter	Description
	• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of messages	Indicates the number of messages in the specified Syslog file that matched the configured pattern.	Number	The detailed diagnosis of this measure, if enabled, will provide the details of the error/warning messages logged in the log file.

3.1.3 Messages by Application Test

This test mines the syslog file and reports the number of application-related error/warning events logged in the log file.

Target of the test : A Syslog file

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the every *patternName* configured in the Include Patterns text box.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens. By default, this is NULL.
Exclude Patterns	Here, specify a comma-separated list of error or warning message patterns to exclude from monitoring. Your pattern specification can be of any of the following formats: **error* or *warning messages**. This parameter is set to *none* by default, which indicates that no message will be excluded from monitoring.
Include Patterns	Here, specify a comma-separated list of error or warning message patterns to be monitored. The format of your specification should be: *patternName:Pattern*, where *patternName* refers to the unique name that you assign to every pattern configuration,

Parameter	Description
	which will appear as the descriptor of this test, and *Pattern* refers to any message pattern of the form **error* or *warning messages**. Multiple pattern specifications can be provided as: *patternName1:Pattern1,patternName2:pattern2*. This parameter is set to *all:all* by default, which indicates that all error/warning messages will be monitored by default.
SyslogFile	Specify the full path to the syslog file to be monitored.
RotatingFile	By default, the RotatingFile parameter is set to **False**. To instruct the eG Enterprise system to monitor newer log files also, set this parameter to **True**. Otherwise, set it to **False**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of messages	Indicates the number of messages in the specified Syslog file that matched the configured pattern.	Number	The detailed diagnosis of this measure, if enabled, will provide the details of the error/warning messages logged in the log file.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.