Monitoring eG Syslog Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

In large IT environments that installed with multiple network devices/applications, a dedicated Syslog server is configured for gathering and saving all the error and warning messages from the network devices/applications. The error and warning messages that logged in the syslog server, 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 to locate and fix the issues quickly. Some environments may not be configured with the dedicated syslog server to collect the syslog messages. In such environments, an eG agent installed on the Windows system can be configured as a syslog service to collect syslog messages from multiple network devices/applications. These messages are displayed in the eG Enterprise console.

Using the syslog messages displayed in the eG Enterprise console, administrators can easily detect and troubleshoot hardware and software issues as well as application and host configuration errors. In addition, these messages also play a vital role in security auditing and incident response. If the messages are not addressed in time, it may cause serious uncertainties in the environment, thus severely impacting the performance. To avoid such adversities, the messages logged in the syslog file should be continuously monitored. The eG Enterprise Suite helps administrators in this task!

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

eG Enterprise monitors the eG 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. To enable the eG agent to monitor the eG Syslog server, the following pre-requisites should be fulfilled.

2.1 Pre-requisites for monitoring the eG Syslog server

The following requirements should be kept in place before starting to monitor the eG Syslog server:

- Starting the eG syslog server service
- Configuring the eG Syslog server

2.1.1 Starting the eG syslog server service

Once the eG agent is installed on the Windows host, first you need to create the syslog server service in it. To create the syslog server service, do the following:

1. Go to the **eGurkha/syslog/bin** folder.
2. Then, run the *CreateSyslogService.bat* file for starting the service.

When the syslog server service is created, the eG Syslog server will run as a Windows service on the system and, will be ready to collect error/warning messages through a port.

2.1.2 Configuring the eG Syslog server

To configure the eG Syslog server to collect the syslog messages, you need to do the following:

1. Go to the **eGurkha/syslog/config** file folder and open the *syslog.properties* file to edit.
2. When Figure 2.1 appears, provide the configuration details as shown in Figure 2.1.

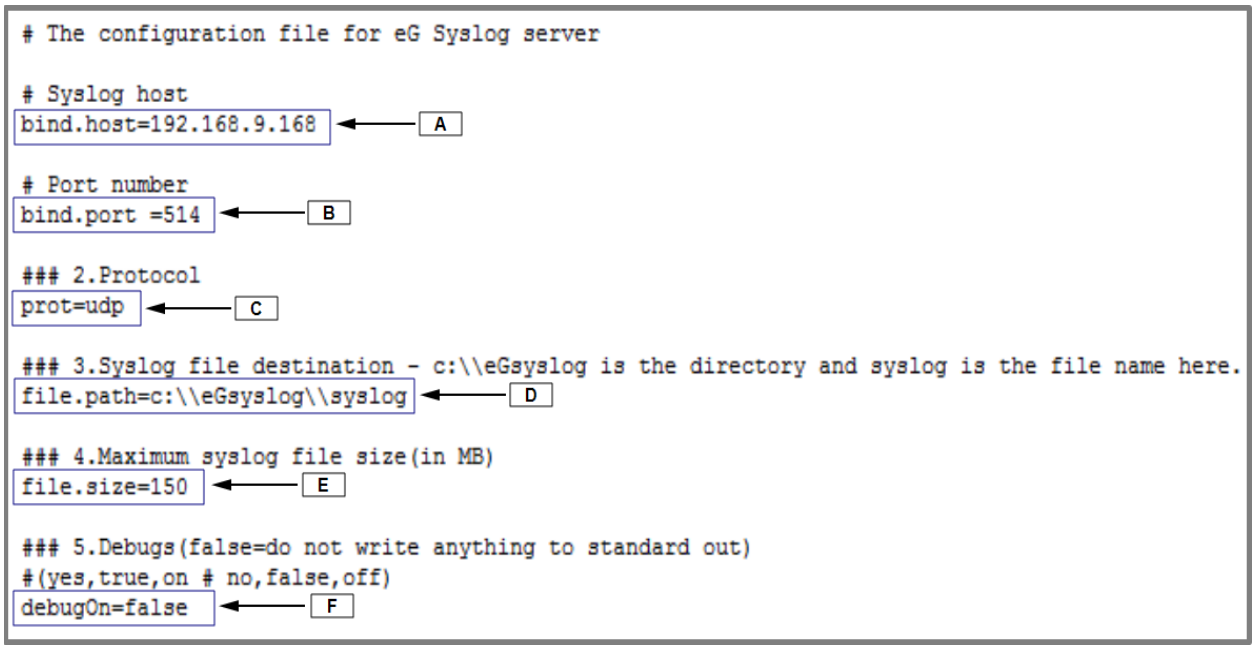

Figure 2.1: Specifying the configuration details in the syslog.properties file

3. The details to be configured in the *syslog.properties* file include the following:

   - **A** - Specify the IP address of the eG Syslog server
   - **B** - Provide the UDP port number at which the eG syslog server listens. By default, this is 514.
   - **C** - By default, User Datagram Protocol (UDP) is used for communication. If you wish to use any other protocol for communication, you can mention it here.
   - **D** - Specify the location and name of the syslog file.
   - **E**- Size limit (in MB) of the syslog file. When the syslog file reaches this limit, a new syslog file named syslog.1 will be created in the same folder. The content of the syslog file will be copied to the syslog.1 file each time syslog file reaches its size limit. At any point in time, the destination folder will contain only two files – syslog and syslog.1 for storing syslog messages.
   - **F** - Indicate whether the eG syslog server should run in debug mode or not. If you wish to run the eG syslog server in the debug mode, this flag should be set to **true**. Otherwise set this flag to **false**.

4. Likewise, the host systems should also be configured with the IP address and port of the eG Syslog server to stream the error/warning messages.

Once the above-said requirements are set in place, manage the eG Syslog component using eG administrative interface to start monitoring eG Syslog server. The steps for achieving this are explained in the following section.

2.2 Managing the eG Syslog Server

The eG Enterprise cannot automatically discover the eG Syslog Server. This implies 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 eG 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 eG Syslog as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.2.

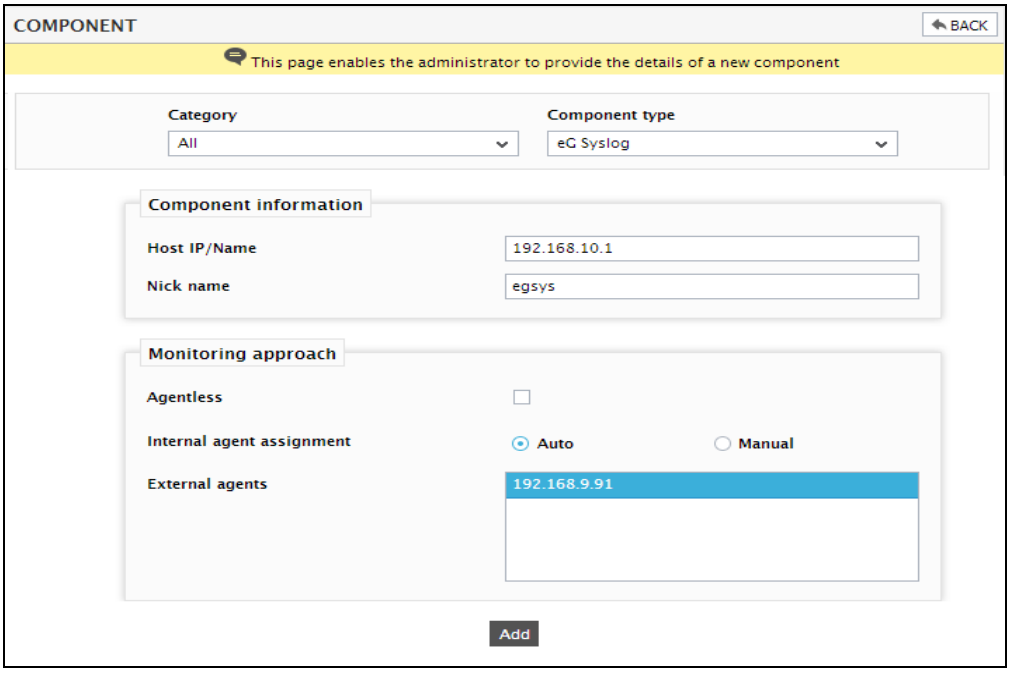

Figure 2.2: Adding a eG Syslog component

4. Specify the **Host IP/Name** and the **Nick name** of the eG Syslog server in Figure 2.2. Then, click the **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests appears.

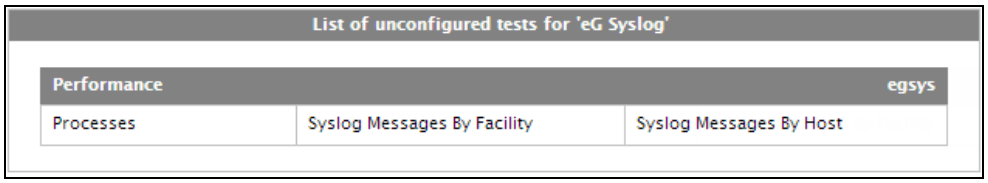

Figure 2.3: List of Unconfigured tests for the eG Syslog component

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

Chapter 1: Monitoring the eG Syslog server

eG Enterprise provides a specialized *eG Syslog* monitoring model (see Figure 1.1) to periodically check the Syslog file for specific patterns of the 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.

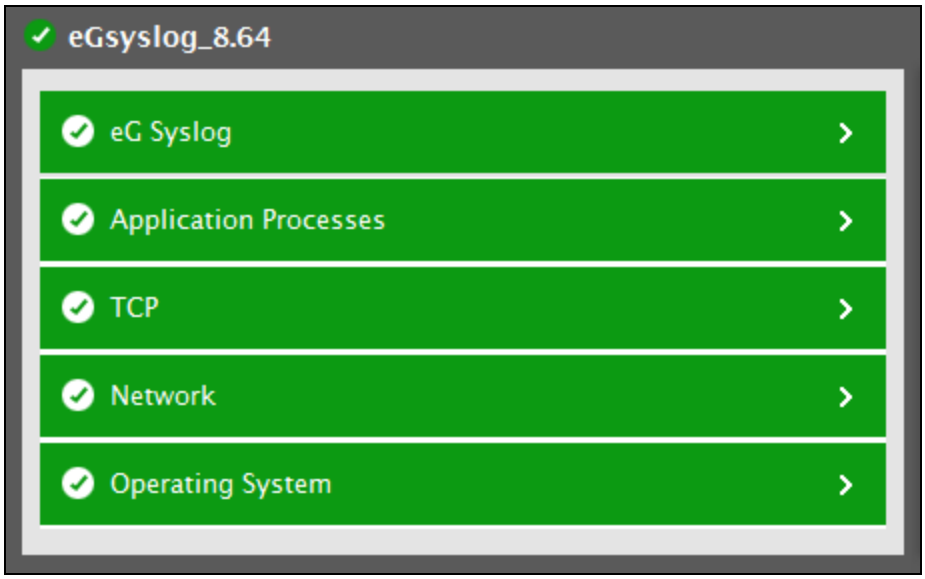

Figure 1.1: The layer model of eG Syslog

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 Figure 1.1 only.

1.1 The eG 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.

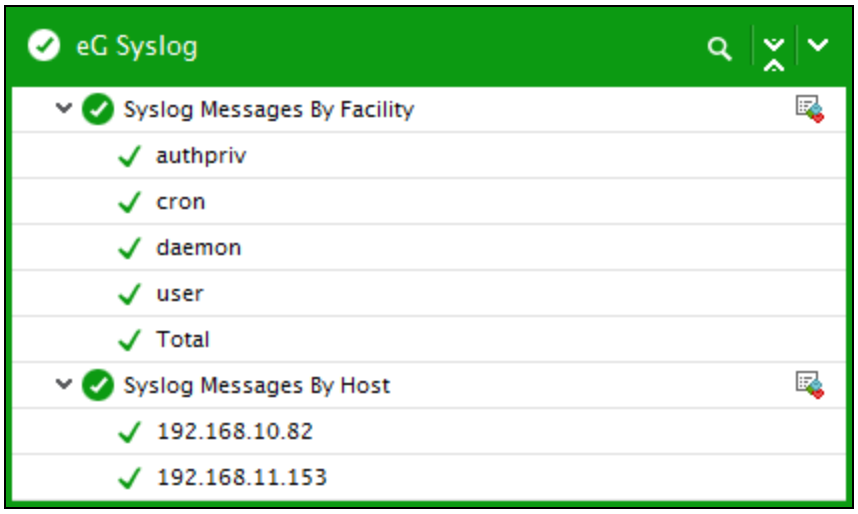

Figure 1.2: The tests mapped to the eG Syslog layer

1.1.1 Syslog Messages by Facility Test

eG Syslog server consolidates error/warning messages that are received from multiple systems in your environment into a single location. These error/warning messages are generated by any part/process of the system and are logged in the syslog file. The error/warning messages are broadly categorized on the basis of which process/part of the system generated the messages. This categorization is done using the concept called *Facilities* that are components of the systems and are represented by decimal integers. By referring to the values corresponding to these facilities, administrator can easily determine the part/process of the system that created the error/warning messages. Sometimes, administrator may only want to receive the messages from certain parts/processes of the system that are critical for the purpose of tracking performance of the system and for troubleshooting. In such cases, administrator can use the **Syslog Messages by Facility** test to filter out the messages of his/her interest. For that purpose, this test enables administrator to configure specific patterns of the error or warning messages based on which the messages should be filtered.

This test periodically mines the Syslog file for specific patterns of error/warning messages configured by administrator and reports the number of messages that match each configured pattern. This way, administrator is alerted to the errors/warnings at the systems and enabled to initiate the necessary remedial actions swiftly.

Target of the test : eG Syslog

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 IP address of the host for which the test is being configured.
Port	The port 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	This test reports metrics by parsing a Syslog file. Specify the full path to the Syslog file here. For instance: *C:\eGurkha\agent\syslog\syslog*.
RotatingFile	By default, the RotatingFile parameter is set to **No**. To instruct the eG Enterprise system to monitor newer log files also, set this parameter to **Yes**. Otherwise, set it to **No**.
DD frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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,

Parameter	Description
	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 this pattern.	Number	The detailed diagnosis of this measure reveals the host IP, the time stamp and the log message.

1.1.2 Syslog Messages by Host Test

This test periodically checks the Syslog file for specific patterns of error/warning messages configured by administrator and reports the number of messages that match each configured pattern. This way, administrator is alerted to the specific errors/warnings of his/her interest and enabled to initiate the necessary remedial actions swiftly.

Target of the test : eG Syslog server

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 IP address of the host for which the test is being configured.
Port	The port at which the specified host listens. By default, this is *NULL*.

Parameter	Description
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	This test reports metrics by parsing a Syslog file. Specify the full path to the Syslog file here. For instance: *C:\eGurkha\agent\syslog\syslog*.
RotatingFile	By default, the RotatingFile parameter is set to **No**. To instruct the eG Enterprise system to monitor newer log files also, set this parameter to **Yes**. Otherwise, set it to **No**.
DD frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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 this pattern.	Number	The detailed diagnosis of this measure reveals the host IP, the time stamp and the log message.

1.1.3 Specific Messages by Facility Test

eG Syslog server consolidates error/warning messages that are received from multiple systems in your environment into a single location. The error/warning messages are generated by any part/process of the system and are logged in the syslog file. The error/warning messages are broadly categorized on the basis of which process/part of the system generated the messages. In the Syslog server, this categorization is done using the concept called Facilities. These facilities are components of the systems and are represented by decimal integers. By referring to the values corresponding to these facilities, administrator can easily determine the part/process of the system that created the error/warning messages. Sometimes, administrator may only want to receive the messages from certain parts/processes of the system that are critical for the purpose of tracking performance of the system and for troubleshooting. In such cases, administrator can use the **Specific Messages by Facility** test to filter out the messages of his/her interest. This test enables administrator to specify a set of rules based on which the error/warning messages should be filtered.

This test periodically mines the syslog file according to the specific rules set by administrator and reports the number of messages that match each rule. This way, administrator is alerted to the errors/warnings triggered at any level of the system, and enabled to initiate the remedial measures before anything untoward happens.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *eG Syslog* as the **Component type**, set *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : eG Syslog Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each rule set by administrator

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The IP address of the host for which the test is being configured.
Port	The port at which the specified host listens. By default, this is NULL.
Rule Name	By default, the syslog file contains logs relating to multiple of host systems that are installed in your environment. In order to obtain the log information of your interest, you can define a set of rules according to which the messages should be read from the syslog file. To create a rule of your choice, click on the  icon. The window that appears will provide you the options for creating the rule. To know how to configure the rules refer to Section **1.1.3.1**.
SyslogFile	This test reports metrics by parsing the syslog file. Specify the full path to the syslog file here. For instance: *C:\eGurkha\agent\syslog\syslog*.
RotatingFile	By default, this parameter is set to **No**. To instruct the eG Enterprise system to monitor newer log files also, set this parameter to **Yes**. Otherwise, set it to **No**.
DD frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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 this rule.	Number	The detailed diagnosis of this measure reveals the host IP, the time stamp and the log message.

1.1.3.1 Configuring Rules for Monitoring

To configure the rules, do the following:

1. Click on the  icon in the Figure 1.3.

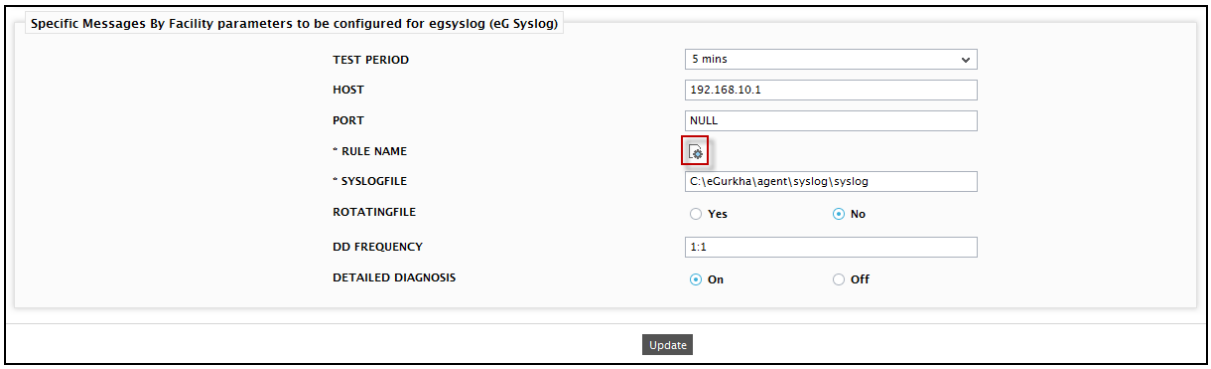

Figure 1.3: Configuring the Specific Messages By Facility test

2. In the popup window that appears, specify the values as shown in Figure 1.4.

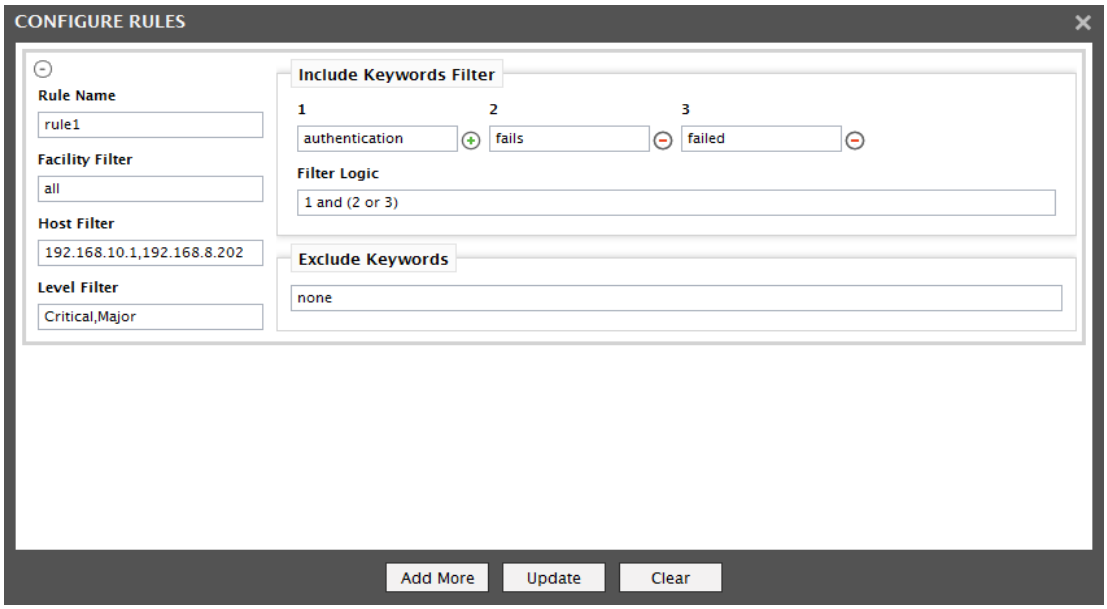

Figure 1.4: Configuring the rules

- **Rule Name :** Specify a name for the rule which will appear as the descriptor in the test.
- **Facility Filter :** By default, this is set to *all* indicating that all the facilities will be monitored by default. If you wish to filter the messages from any particular facility, then, specify the name of that particular facility in this text box. For example: *kern*. In this case, the messages belong to the kernal level will only be monitored. Besides, you can also filter the messages from multiple facilities of your choice by specifying the names of those facilities in a comma-separated list. For example, *kern,user,mail*.
- **Host Filter :** Here, specify the IP address of the host system for which the messages collected should be filtered from the syslog file. By default, this is set to *all* indicating that messages from all the host systems will be tracked. Multiple host systems of your choice can also be given in a comma- separtated list. Your specification should be of the following format: *192.168.10.1,192.168.8.202*
- **Level Filter :** The error/warning messages logged in the syslog file have various degrees of severity. In this text box, indicate a severity level to check for the error/warning messages with particular degree of severity in the syslog file. By default, this is set to *all* indicating that all the messages will be monitored regardless of their degree of severity. You can also specify multiple severity levels as a comma-separated list in the following format: *Critical,Major*.
- **Include Keywords Filter :** Specify one or more keywords to be monitored from the syslog file in this section. By default, this section would be provided with one field wherein you will have to

specify a keyword to be monitored. However, to add more keywords, click on the ⊕ button and add the keywords in the fields that are added. For instance, if you want to search for the authentication failure related messages, then you can specify the keywords as shown in Figure 1.4. Using the ⊖ button, you can remove the keywords that you added.

- **Filter logic** - Here, you can define a logic on how to filter out messages in the syslog file. This logic is derived based on the keywords that you provided in the **Include Keywords Filter** section. For instance, assume that the **Filter Logic** is 1 and (2 or 3) as shown in Figure 1.4. Here, the messages will be filtered only if the messages contain the keyword 1 and either of the keyword 2 or keyword 3. Likewise, you can define any filter logic according to your need.
- **Exclude Keywords** : Here, specify a comma-separated list of keywords to be excluded from monitoring. The format of your specification should be: *error,warning*. By default, this is set to *none* indicating that no messages will be excluded from monitoring.

Once you clicked the **Update** button after defining all the values, you will return to the test configuration page. To add more rules, click on the **Add More** button in Figure 1.4. If you want to clear the values that you entered and define the new values, you can do so by using the **Clear** button. You can also remove a specific rule that you added, using the ⊖ button.

1.1.4 Specific Messages by Host Test

This test periodically checks the Syslog file for a specific rule set by administrator and reports the number of messages that match each rule. This way, administrator is alerted to the errors/warnings triggered at any level of the system, and enabled to initiate the remedial measures before anything untoward happens.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *eG Syslog* as the **Component type**, set *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : eG Syslog server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each *rule* set by administrator.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The IP address of the host for which the test is being configured.
Port	The port at which the specified host listens. By default, this is NULL.
Rule Name	By default, the syslog file contains logs relating to multiple of host systems that are installed in your environment. In order to obtain the log information of your interest, you can define a set of rules according to which the messages should be read from the syslog file. To create a rule of your choice, click on the  icon. The window that appears will provide you the below options for creating the rule. To know how to configure the rules refer to Section **1.1.3.1**.
Syslogfile	This test reports metrics by parsing the syslog file. Specify the full path to the syslog file here. For instance: *C:\eGurkha\agent\syslog\syslog*.
Rotatingfile	By default, this parameter is set to **No**. To instruct the eG Enterprise system to monitor newer log files also, set this parameter to **Yes**. Otherwise, set it to **No**.
DD frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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 this rule.	Number	The detailed diagnosis of this measure reveals the host IP, the time stamp and the log message.

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.