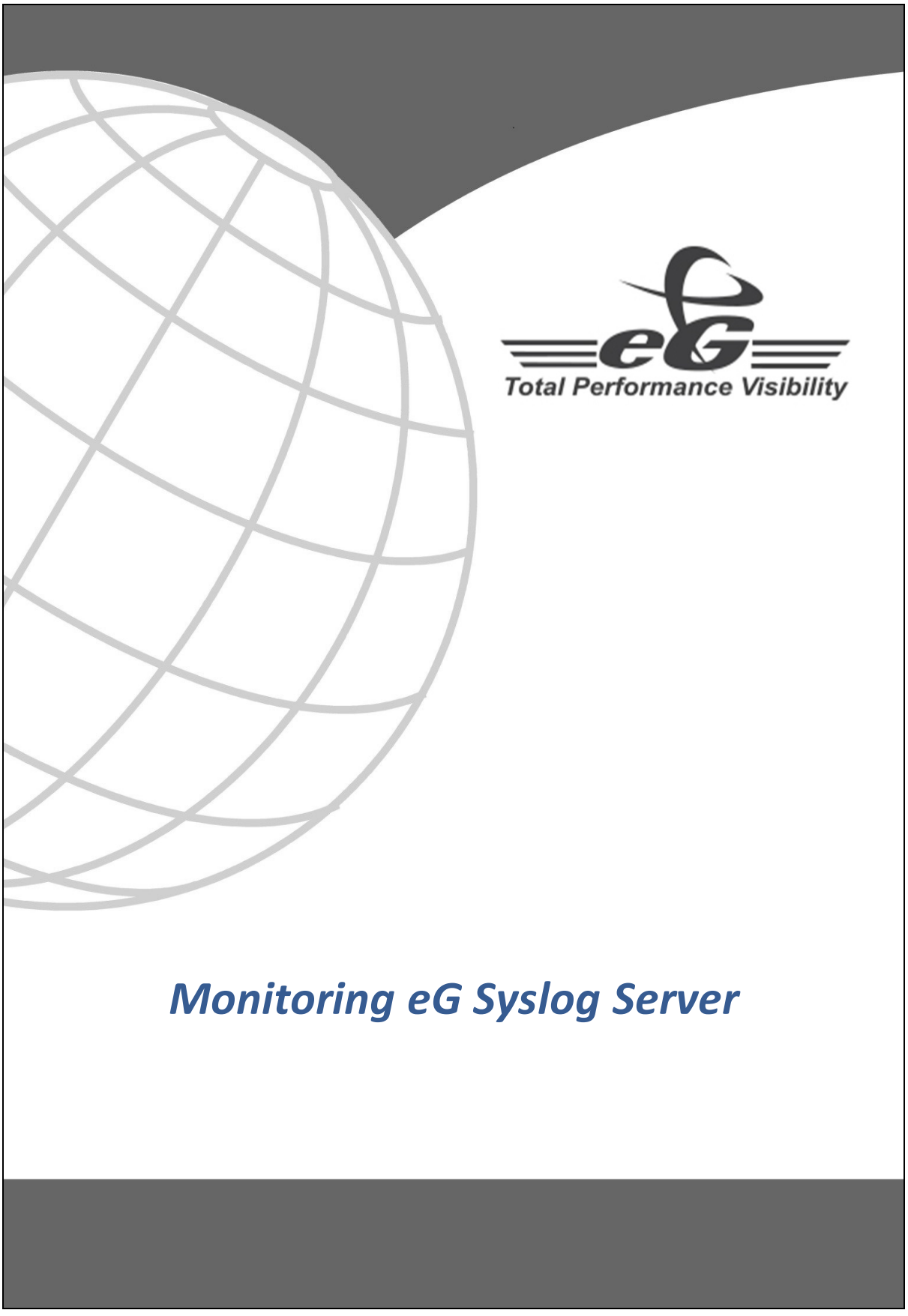


# *Monitoring eG Syslog Server*

**Restricted Rights Legend**

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

**Trademarks**

Microsoft Windows, Windows 2008, Windows 7, Windows 8, Windows 10, Windows 2012 and Windows 2016 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**Copyright**

©2016 eG Innovations Inc. All rights reserved.

# Table of contents

# Table of Figures

1

# Monitoring the eG Syslog server

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 can be analyzed and displayed in the eG Enterprise console.

With 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.

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.

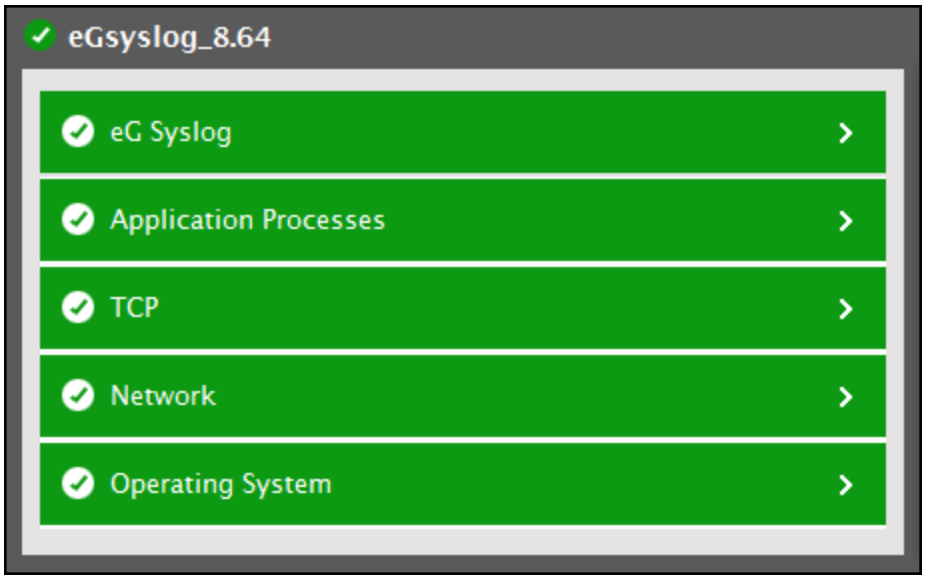


Figure 1.1: The layer model of eG Syslog

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 Pre-requisites for monitoring the eG Syslog server

## 1.1.1 Starting the eG syslog server service

Once the eG agent is installed on the Windows system, 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.

## 1.1.2 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 1.2 appears, provide the configuration details as shown in Figure 1.2.

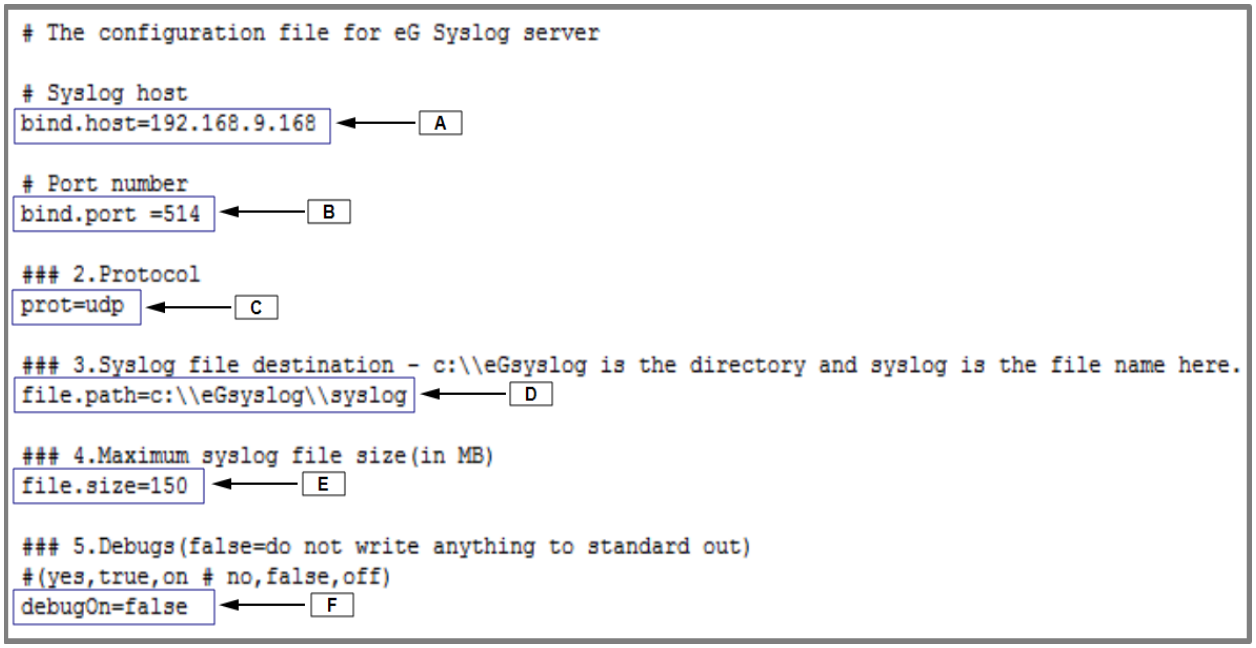


Figure 1.2: Specifying the configuration details in the syslog.properties file

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.

## 1.2 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.

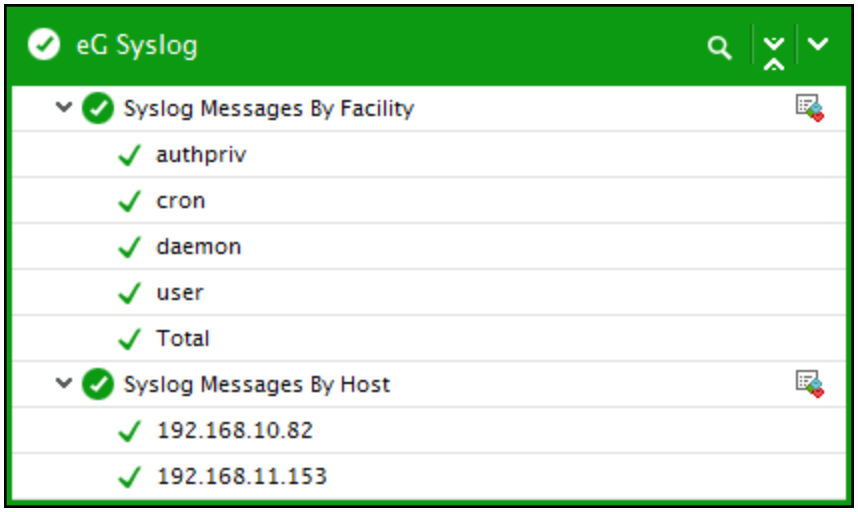


Figure 1.3: The tests mapped to the eG Syslog layer

### 1.2.1 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**

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The IP address of the host for which the test is being configured.
3. **PORT** – The port at which the specified host listens. By default, this is *NULL*.
4. **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.
5. **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.
6. **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*.
7. **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**.
8. **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**.
9. **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. |

## 1.2.2 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**

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The IP address of the host for which the test is being configured.
3. **PORT** – The port at which the specified host listens. By default, this is *NULL*.
4. **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.
5. **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.

6. **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*.
7. **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**.
8. **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**.
9. **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. |

## 1.2.3 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**

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The IP address of the host for which the test is being configured.
3. **PORT** – The port at which the specified host listens. By default, this is *NULL*.
4. **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. The format of your rule should be: *rule1: str1|str2|str3|str4|str5*, where *rule1* refers to the unique name that you assign to every rule, which will appear as the descriptor of this test, and *str1, str2, str3, str4* and *str5* refer to the strings to be searched in the syslog file. Using these strings, the information in the syslog file may be parsed and metrics may be collected. When you want to define more than one rule, you can do so by setting multiple rules in the following format: *rule1=str1|str2|str3|str4|str5^#^rule2=str1|str2|str3*. For example: *rule1:session closed|session close|session fail^#^rule2=logon fail|login failed|login failure*
5. **FACILITY** - This parameter is set to *all* indicating that all the facilities will be monitored by default for the rule specified in the **RULE NAME** text box. If you wish to filter the messages received from specific parts/processes of the host system, then, you can enter the facilities corresponding to those parts/processes against this parameter. For example: *rule1=UNKNOWN,MAIL*. When more than one rules are defined, you have to provide the facilities in the following format: *rule1=UNKNOWN,MAIL^#^rule2=all.*
6. **FILTER HOST** - Here, specify the IP addresses of the host systems for which the messages collected should be filtered from the syslog file. Multiple host systems can be given in a comma-separtated list.

For instance: *rule1=192.168.10.1,192.168.10.2,192.168.10.5^#^rule2=all*. By default, this parameter is set to *all* which indicates that all the hosts systems will be monitored.

7. **LEVEL** - The error/warning messages logged in the syslog file have various degrees of criticality. Here, indicate the **LEVEL** to check the error/warning messages with particular degree of criticality in the syslog file. This parameter is set to *all*, which indicates that all messages in the syslog file will be monitored, by default. Multiple levels can be included as a comma-separated list in the following format: *rule1=Error, critical*.
8. **FILTER LOGIC** - Provide the logic based on which this test should monitor the messages from the syslog file. This logic is derived based on the strings provided in the **RULE NAME** text box. The logic can be provided as follows: *rule1=(str1 and str2) or str3^#^rule2=str1 or (str2 and str3).*
9. **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.
10. **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*.
11. **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**.
12. **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**.
13. **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 Mes-** | Indicates the number of | Number | The detailed diagnosis of this measure |

| Measurement | Description | Measurement Unit | Interpretation |
|---|---|---|---|
| **sages:** | messages in the specified Syslog file that matched this rule. | | reveals the host IP, the time stamp and the log message. |

## 1.2.4 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**

1. **TEST PERIOD** – How often should the test be executed
2. **HOST** – The IP address of the host for which the test is being configured.
3. **PORT** – The port at which the specified host listens. By default, this is *NULL*.
4. **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.
5. **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. The format of your rules should be: *rule1: str1|str2|str3|str4|str5*, where *rule1* refers to the unique name that you assign to every rule, which will appear as the descriptor of this test, and *str1, str2, str3, str4* and *str5* refer to the strings to be searched in the syslog file. Using these strings, the information in the syslog file may be parsed and metrics may be collected. When you want to define more than one rule, you can do so by setting multiple rules in the following format: *rule1=str1|str2|str3|str4|str5^#^rule2=str1|str2|str3*. For example: *rule1:session closed|session close|session fail^#^rule2=logon fail|login failed|login failure*
6. **FACILITY** - This parameter is set to *all* indicating that all the facilities will be monitored by default for the

rule specified in the **RULE NAME** text box. If you wish to filter the messages received from specific parts/processes of the host system, then, you can enter the facilities corresponding to those parts/processes against this parameter. For example: *rule1=UNKNOWN,MAIL*. When more than one rules are defined, you have to provide the facilities in the following format: *rule1=UNKNOWN,MAIL^#^rule2=all.*

7. **FILTER HOST** - Here, specify the IP addresses of the host systems for which the messages collected should be filtered from the syslog file. Multiple host systems can be given in a comma-separtated list. For instance: *rule1=192.168.10.1,192.168.10.2,192.168.10.5^#^rule2=all*. By default, this parameter is set to *all* which indicates that all the hosts systems will be monitored.
8. **LEVEL** - The error/warning messages logged in the syslog file have various degrees of criticality. Here, indicate the **LEVEL** to check the error/warning messages with particular degree of criticality in the syslog file. This parameter is set to *all*, which indicates that all messages in the syslog file will be monitored, by default. Multiple levels can be included as a comma-separated list in the following format: *rule1=Error, critical*.
9. **FILTER LOGIC** - Provide the logic based on which this test should monitor the messages from the syslog file. This logic is derived based on the strings provided in the **RULE NAME** text box. The logic can be provided as follows: *rule1=(str1 and str2) or str3^#^rule2=str1 or (str2 and str3).*
10. **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*.
11. **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**.
12. **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**.
13. **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. |

2

# Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **Syslog** file. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.