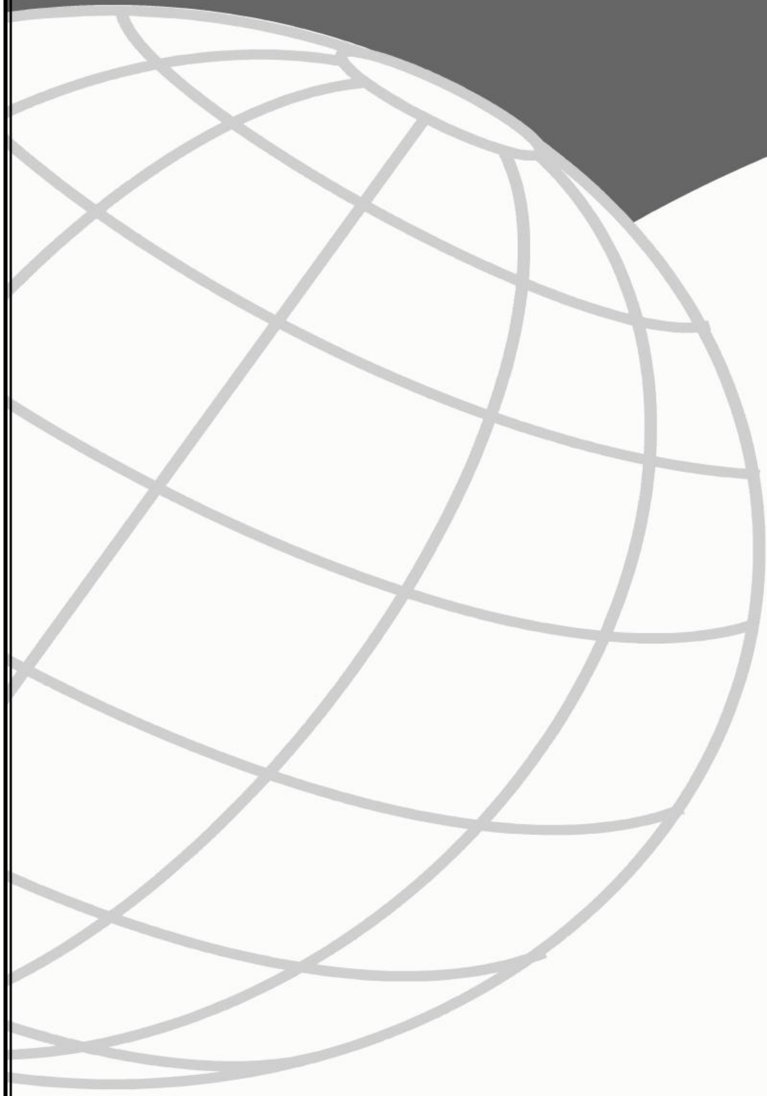


Enabling Service Excellence

Monitoring a Syslog

eG Enterprise v6

Restricted Rights Legend

Trademarks

Copyright

Table of Contents

Table of Figures

Chapter

1

Monitoring a Syslog

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 provides a specialized *Syslog* monitoring model (see Figure 1.1) 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.

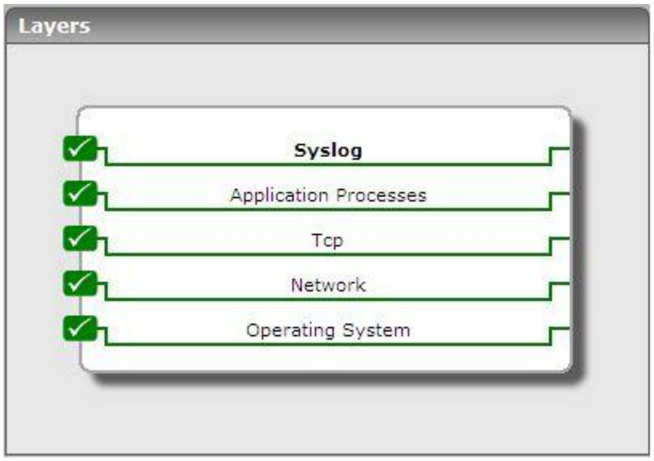
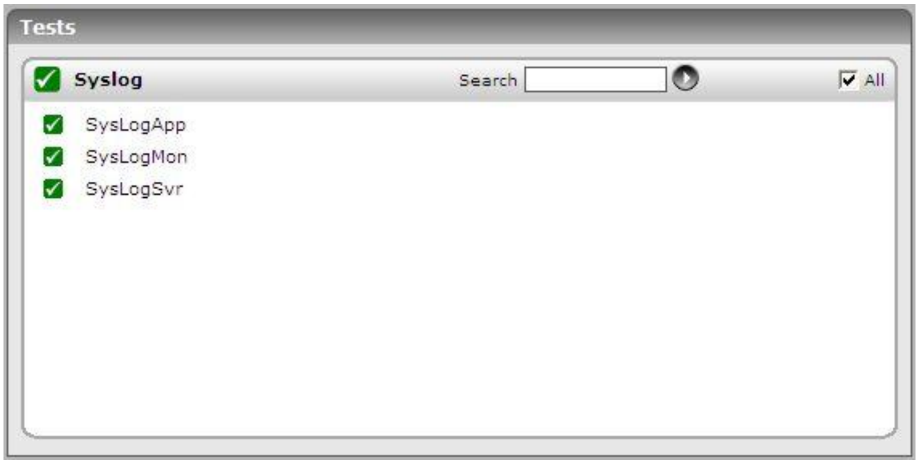


Figure 1.1: The layer model of a Syslog

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 Figure 1.1 only.

1.1 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.



Tests

☑ Syslog

Search

☑ All

☑ SysLogApp

☑ SysLogMon

☑ SysLogSvr

Figure 1.2: The tests mapped to the Syslog layer

1.1.1 SysLogMon Test

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

Purpose	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

<table>
<tr><td><b>Configurable parameters for the test</b></td><td colspan="3">1. <b>Testperiod</b> – How often should the test be executed
2. <b>Host</b> – The IP address of the host for which the test is being configured.
3. <b>port</b> – The port at which the specified <b>host</b> listens. By default, this is NULL.
4. <b>exclude patterns</b> – 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: <i>*error</i> or <i>warning messages*</i>. This parameter is set to <i>none</i> by default, which indicates that no message will be excluded from monitoring.
5. <b>include patterns</b>- Here, specify a comma-separated list of error or warning message patterns to be monitored. The format of your specification should be: <i>patternName:Pattern</i>, where <i>patternName</i> refers to the unique name that you assign to every pattern configuration, which will appear as the descriptor of this test, and <i>Pattern</i> refers to any message pattern of the form <i>*error</i> or <i>warning messages*</i>. Multiple pattern specifications can be provided as: <i>patternName1:Pattern1,patternName2:pattern2</i>. This parameter is set to <i>all:all</i> by default, which indicates that all error/warning messages will be monitored by default.
6. <b>syslogfile</b> – Specify the full path to the syslog file to be monitored.
7. <b>rotatingfile</b> - By default, the <b>ROTATINGFILE</b> parameter is set to <b>FALSE</b>. To instruct the eG Enterprise system to monitor newer log files also, set this parameter to <b>TRUE</b>. Otherwise, set it to <b>FALSE</b>.
8. <b>DETAILED DIAGNOSIS</b> - 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 <b>On</b> option. To disable the capability, click on the <b>Off</b> 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.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for every <i>patternName</i> configured in the <b>include patterns</b> text box</td></tr>
<tr><td rowspan="2"><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td><b>Number of messages:</b>
Indicates the number of messages in the specified Syslog file that matched the configured pattern.</td><td>Number</td><td>The detailed diagnosis of this measure, if enabled, will provide the details of the error/warning messages logged in the log file.</td></tr>
</table>

1.1.2 SysLogSvr Test

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

Purpose	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
Configurable parameters for the test	1. **Testperiod** – 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** – Specify the full path to the syslog file to be monitored. 7. **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**. 8. **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.
Outputs of the test	One set of results for the every *patternName* configured in the **include patterns** text box

Measurements made by the test	Measurement	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.

1.1.3 SysLogApp Test

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

Purpose	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

Configurable parameters for the test	1. **Testperiod** – 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** – Specify the full path to the syslog file to be monitored. 7. **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**. 8. **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.
Outputs of the test	One set of results for the every *patternName* configured in the **include patterns** text box

Measurements made by the test	Measurement	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.

Chapter

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.