Monitoring Printers

eG Enterprise v6

Restricted Rights Legend

Trademarks

Copyright

Table of Contents

Table of Figures

Chapter 1

Monitoring Printers

Of all peripheral devices that can be used in an IT infrastructure, printers are the most frequently used, and hence, the most important. If a printer goes offline, then critical reports and documents cannot be printed until such time that it is switched back online. Since network printers are typically placed in a central location and shared by users across multiple locations, it would be impractical for some users and a bit time-consuming for others, to manually check the printer status time and again. Instead, if the current status of the printer and its core components such as the tray, cover, output bins etc., is automatically reported to a centralized console at pre-configured intervals, then administrators will come to know of abnormalities in printer operations as soon as they occur, and can initiate corrective measures soon after. This is possible only if a monitoring solution is employed to monitor the printer status at pre-set frequencies.

eG Enterprise has designed a specialized *Printer* monitoring model (see Figure 1.1) that periodically runs status checks on the printer to determine its availability, monitors its key parts such as the printer cover, the tray, the output bin, the toner, the door, etc., for faults, and proactively alerts administrators to printer-related problems.

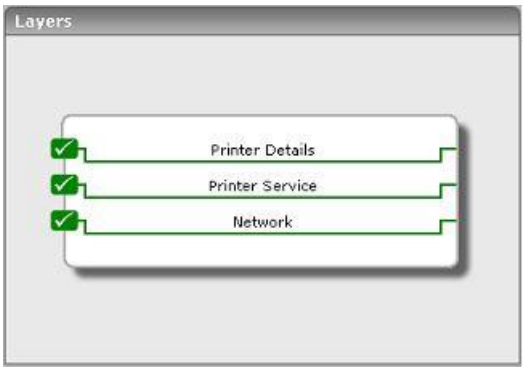

Figure 1.1: The layer model of a Printer

The **Network** layer depicted by Figure 1.1 has been discussed in the *Monitoring Unix and Windows Servers* document. The sections to come therefore, will discuss only the top 2 layers of Figure 1.1.

1.1 The Printer Service Layer

Using the tests associated with this layer, administrators can determine the following (see Figure 1.2):

- Is the printer cover closed?
- Are the input trays available?
- Has paper been fed into the input trays?
- Are the output bins available?

Figure 1.2: Tests that run on the Printer Service layer

1.1.1 PrinterCover Test

This test provides the status of every cover available in the printer.

Purpose	Provides the status of every cover available in the printer
Target of the test	A Printer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured 3. **Snmpport** – The port number on which the printer is exposing its SNMP MIB. The default port is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the printer. The default is public. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

	14. **TIMEOUT** - Here, specify the maximum duration (in seconds) for which the test will wait for a response from the server. The default **TIMEOUT** period is 10 seconds.		
Outputs of the test	One set of results for the printer being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Is cover closed: Critical warning Indicates whether a particular cover is closed	Boolean	A value of 0 indicates that the cover is open. If the value is 1, it means that the cover is closed.

Note:

This measure is available only for printers with covers.

1.1.2 PrinterInputs Test

This test reports statistics relating to a printer's input trays.

Purpose	Provides the status of each of the printer input trays
Target of the test	A Printer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured 3. **Snmpport** – The port number on which the printer is exposing its SNMP MIB. The default port is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the printer. The default is public. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

	14. **timEOUT** - Here, specify the maximum duration (in seconds) for which the test will wait for a response from the server. The default **TIMEOUT** period is 10 seconds.		
Outputs of the test	One set of results for the printer being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Input device availability: Critical warning Indicates whether a particular tray is available for printing	Boolean	A value of 0 indicates that the tray is not available for printing and the value 1 indicates that the tray is available for printing. Availability problems can be caused by various factors including paper unavailability, paper jam, etc.
	Is tray idle: Non Critical warning Indicates whether the tray is idle or busy	Boolean	While a value of 1 indicates that the tray is idle, value of 0 denotes that the tray is busy with some printing job
	Is paper available in tray: Critical warning Indicates whether the tray has paper or not	Boolean	A value of 0 indicates that the tray does not have paper to print. A value of 1, suggests that the tray has paper to print.

1.1.3 PrinterOutputs Test

This test reports statistics relating to each of the output bins of a printer.

Purpose	Indicates the status of the output bins
Target of the test	A Printer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured 3. **Snmpport** – The port number on which the printer is exposing its SNMP MIB. The default port is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the printer. The default is public. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

	14. **TIMEOUT** - Here, specify the maximum duration (in seconds) for which the test will wait for a response from the server. The default **TIMEOUT** period is 10 seconds.		
Outputs of the test	One set of results for the printer being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Output device availability: Non-critical warning Indicates whether the output bin is available or not.	Boolean	A value of 0 indicates that the output bin is not available and a value of 1 indicates that it is available.
	Is output bin idle: Non-critical warning Indicates whether the output bin is busy or idle	Boolean	A value of 0 indicates that the bin is busy and a value of 1 indicates that it is idle.

Note:

These measures are available only for printers that support output bins.

1.2 The Printer Details Layer

This layer promptly notifies administrators when printer errors occur, or when the printer suddenly goes offline. The layer also helps administrators judge how effectively the printer was utilized by reporting the number of pages that have been printed using the printer.

Figure 1.3: Tests executing on the Printer Details layer

1.2.1 PrinterErrors Test

The PrinterErrors test indicates whether a particular measure generates a Critical warning or a Non-critical warning. A Critical warning is indicative of a problem so severe, that the printer is rendered unavailable until the warning is attended to. A Non-critical warning is one wherein the printer will continue to remain available despite the warning.

Purpose	Indicates whether a particular measure generates a Critical warning or a Non-critical warning.
Target of the test	A Printer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The variable name of the host for which the test is to be configured 3. **Snmpport** – The port number on which the printer is exposing its SNMP MIB. The default port is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the printer. The default is public. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. TIMEOUT - Here, specify the maximum duration (in seconds) for which the test will wait for a response from the server. The default TIMEOUT period is 10 seconds.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the printer being monitored</td></tr>
<tr><td rowspan="6">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Is paper available:
Critical warning
Indicates the availability of papers in all trays</td><td>Boolean</td><td>A value of 0 indicates that there are no papers in any of the trays. If the value is 1, it means that papers are available in at least one tray.</td></tr>
<tr><td>Toner capacity:
Non-critical warning
Indicates the status of the toner with respect to its capacity</td><td>Boolean</td><td>A value of 0 indicates that the toner capacity is low. However, if the value is 1 it indicates that there is adequate toner in the printer.</td></tr>
<tr><td>Is toner available:
Critical warning
Indicates whether a toner is available for printing or not</td><td>Boolean</td><td>A value of 0 is indicative of either of the following scenarios:
➢ The toner cartridge is not physically present in the printer
➢ The printer is out of toner
A value of 1, on the other hand, confirms the physical presence of the toner cartridge and its availability for printing.</td></tr>
<tr><td>Paper flow status:
Critical warning
Indicates whether the flow of paper into and out of the printer is smooth</td><td>Boolean</td><td>A value of 0 indicates that there is a paper jam and a value of 1 indicates that the paper flow is smooth</td></tr>
<tr><td>Is online:
Critical warning
Indicates whether the printer is on line or off line.</td><td>Boolean</td><td>A value of 0 indicates that the printer is off line. If the value is 1, it denotes that the printer is on line</td></tr>
</table>

	Is door closed: Critical warning Indicates the overall status of the doors/covers present in the printer Note: This measure is available only for printers with doors / covers.	Boolean	While a value of 0 indicates that the door is open, 1 indicates that it is closed.

1.2.2 PrinterPageCount Test

This test monitors the usage of a printer.

Purpose	The PrinterPageCount gives the number of pages that were printed during the set test frequency.
Target of the test	A Printer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured 3. **Snmpport** – The port number on which the printer is exposing its SNMP MIB. The default port is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the printer. The default is public. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

	14. **TIMEOUT** - Here, specify the maximum duration (in seconds) for which the test will wait for a response from the server. The default **TIMEOUT** period is 10 seconds.		
Outputs of the test	One set of results for the printer being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Pages printed Indicates the number of pages printed during the set test frequency For example, assume that the PrinterPageCount is set to execute every 60 seconds. During this time interval, if 3 pages are printed, then the *Pages printed* measure will return 3.	Pages	The value " –1" indicates that the test is not able to generate measures. Any other value indicates the number of pages printed during the pre-defined time interval.

1.2.3 PrinterTest

This test monitors the availability of a network printer.

Purpose	Indicates the availability of the printer for printing
Target of the test	A Printer
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **Host** - The host for which the test is to be configured 3. **Snmpport** – The port number on which the printer is exposing its SNMP MIB. The default port is 161. 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **snmpversion** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the printer. The default is public. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **username** – This parameter appears only when **v3** is selected as the **snmpversion**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **username** parameter. 7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **confirm password** – Confirm the **authpass** by retyping it here. 9. **authtype** – This parameter too appears only if **v3** is selected as the **snmpversion**. From the **authtype** list box, choose the authentication algorithm using which SNMP v3 converts the specified **username** and **password** into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **encryptflag** – This flag appears only when **v3** is selected as the **snmpversion**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **encryptflag** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **encrypttype** – If the **encryptflag** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **encrypttype** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **encryptpassword** – Specify the encryption password here. 13. **confirm password** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. TIMEOUT - Here, specify the maximum duration (in seconds) for which the test will wait for a response from the server. The default TIMEOUT period is 10 seconds.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the printer being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Is the printer service available:
This shows whether the printer is available for printing or not</td><td>Boolean</td><td>A value of 0 indicates that the printer is not available for printing. A value of 1 indicates that the printer is available for printing.
A printer could be rendered unavailable if its off the network. This could be due to the following reasons:
➢ A Power shut-down
➢ Failure of the network connection
Similarly, a printer on the network can also become unavailable for printing. This could be owing to either of the following reasons:
➢ The printer does not support snmp
➢ The printer is in an "unknown" state</td></tr>
</table>

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 **Event Logs**. 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.