Monitoring GroupWise Internet Agent (GWIA)

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The GWIA allows communication between GroupWise users and users of other messaging systems who use the Internet to send e-mail. Problems in the GWIA, if not resolved in time, could close all doors of communication across messaging systems. To avoid this, the GWIA has to be continuously monitored.

Novell GroupWise 6.5 is a cross-platform collaboration product that enables users to work over any type of network. In addition to integrated e-mail and scheduling services, GroupWise offers task-, contact- and document-management services. It also delivers secure instant messaging tools and offers mobile-access capabilities.

Owing to its diverse capabilities, GroupWise components play a very crucial role in the delivery of many business-critical applications. Operational issues with any GroupWise component can thus have serious repercussions on service performance. Therefore, in order to ensure high availability and uninterrupted delivery of the service, continuous monitoring of the GWIA is essential. To achieve this purpose, eG Enterprise provides a specialized model for continuously monitoring the GWIA.

Chapter 2: How to Monitor GroupWise Internet Agent (GWIA) Using eG Enterprise?

eG Enterprise monitors the GroupWise component in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. This agent is capable of monitoring the GroupWise component via SNMP. Before attempting to monitor the GroupWise application, ensure that it is SNMP-enabled.

Once you SNMP-enable the components and feed the eG Enterprise system with the SNMP port and community string, the eG agent can easily contact the SNMP-MIB of GroupWise to extract the measures of interest. What more, these monitoring models do not even require an agent to be installed on the monitored system. If a target server/device supports the HOST-RESOURCES MIB, then eG Enterprise can provide in-depth insights into the performance of those targets in a non-intrusive, agentless manner. For more details related to agentless monitoring, refer to the *Administering eG Enterprise* document.

The eG Enterprise offers two different component types to monitor GroupWise running on Novell Netware and Windows operating systems. In the eG Enterprise system, the GWIA component should be managed either as “Groupwise Internet - Netware” or “Groupwise Internet - Win”, based on the OS (i.e. Netware or Windows) that it executes on.

The broad steps for monitoring the server using eG Enterprise are as follows:

- Managing the GroupWise Internet Agent (GWIA)
- Configuring the tests

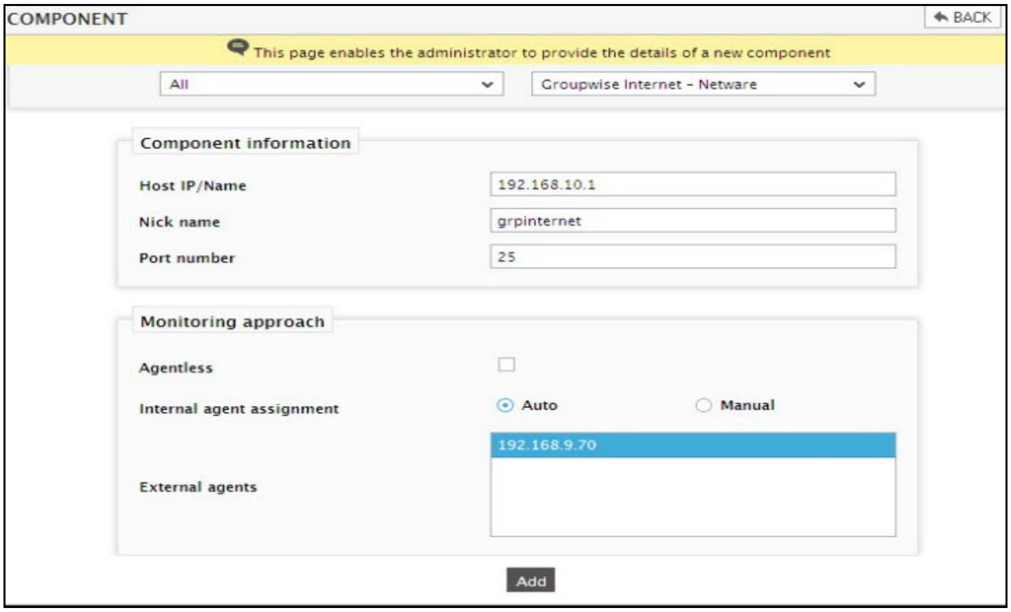
These steps have been discussed in following sections.

2.1 Managing the Groupwise Internet Application (GWIA)

eG Enterprise can automatically discover the Groupwise Internet Application (GWIA) in the environment and also lets you to add the GWIA component if the server is not auto-discovered. The following steps explain you how to manually add the GWIA component using the eG administrative interface.

1. Log into the eG administrative interface.
2. If a GWIA is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page.

3. However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or add the component manually using the **COMPONENTS**page (Infrastructure -> Components -> Add/Modify). Remember that components manually added are managed automatically. Figure 2.1 clearly illustrates the process of adding a GWIA application.



COMPONENT

This page enables the administrator to provide the details of a new component

All | Groupwise Internet - Netware

Component information

Host IP/Name: 192.168.10.1

Nick name: grpinternet

Port number: 25

Monitoring approach

Agentless: □

Internal agent assignment: ● Auto ○ Manual

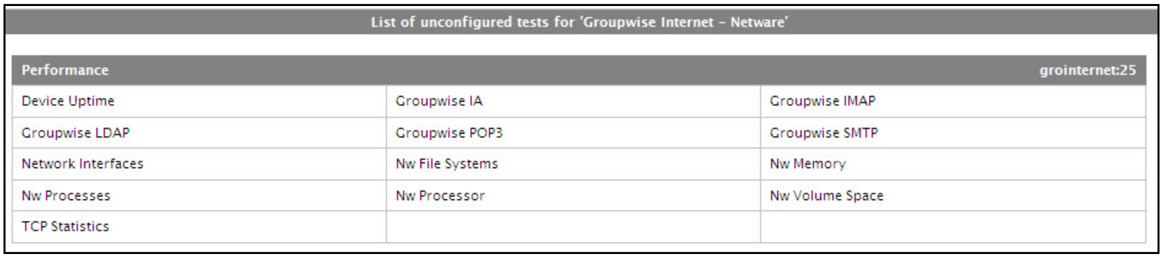
External agents: 192.168.9.70

Figure 2.1: Adding a new Groupwise Internet Application

4. Specify the **Host IP**, the **Nick name** and **Port Number** for the GWIA in 2.1. Then, click the **Add** button to register the changes.

2.2 Configuring the tests

1. When try to sign out of the eG administrative interface. A list of unconfiugured tests page will appear listing the tests that require manual configuration as shown in Figure 2.2.



List of unconfigured tests for 'Groupwise Internet - Netware'

Performance		grointernet:25
Device Uptime	Groupwise IA	Groupwise IMAP
Groupwise LDAP	Groupwise POP3	Groupwise SMTP
Network Interfaces	Nw File Systems	Nw Memory
Nw Processes	Nw Processor	Nw Volume Space
TCP Statistics		

Figure 2.2: The list of unconfigured tests that need to be configured

2. Upon doing so, a **LIST OF UNCONFIGURED TESTS** listing the GWIA-specific tests requiring manual configuration, will appear. Click on the test names to configure. To know how to configure the tests, refer to **Monitoring the GroupWise Internet Agent (GWIA)** chapter.
3. Then, try to sign out one more time. This time again, the list of unconfigured tests will appear. Click on the **Network Interfaces** test to configure it. To know the details on configuring this test, refer to the *Monitoring Cisco Routers* document.
4. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the GroupWise Internet Agent (GWIA)

eG Enterprise provides out-of-the-box, not one, but two specialized monitoring models for the GWIA component – i.e., one for every operating system on which the component executes. While the GWIA component on Netware can be managed as Groupwise Internet Agent - Netware, the one on Windows can be managed as Groupwise Internet Agent - Win. Figure 3.1 below depicts the Groupwise Internet Agent - Netware model.

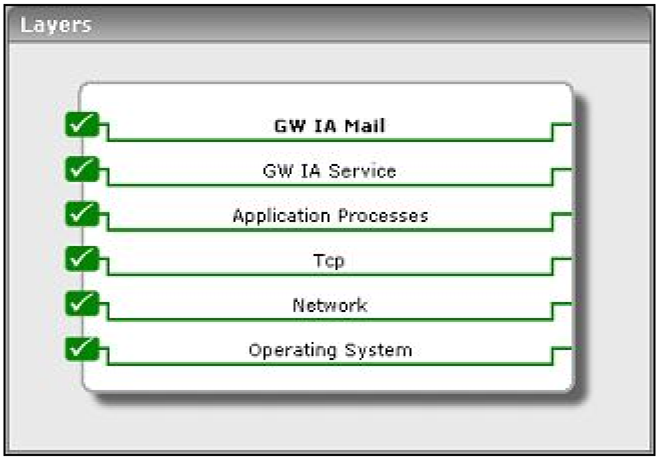


Figure 3.1: Layer model of GWIA

Though both the Groupwise Internet Agent - Win and Groupwise Internet Agent - Netware models share the same set of layers, the difference lies in the tests mapped to the operating system-specific layers – in other words, the bottom 4 layers of the layer model. To know the details of tests mapped to these 4 layers on Windows environments, refer to the *Monitoring Unix and Windows Servers* document. Similarly, to know which tests are associated with these 4 layers on Netware, refer to *Monitoring Netware* document.

Since the bottom layers of Figure 3.1 have all been dealt with in other documents, let us simply focus on the top 2 layers of the layer model.

3.1 The GW IA Service Layer

Using the test associated with this layer, an administrator can determine how well the GWIA processes messages.

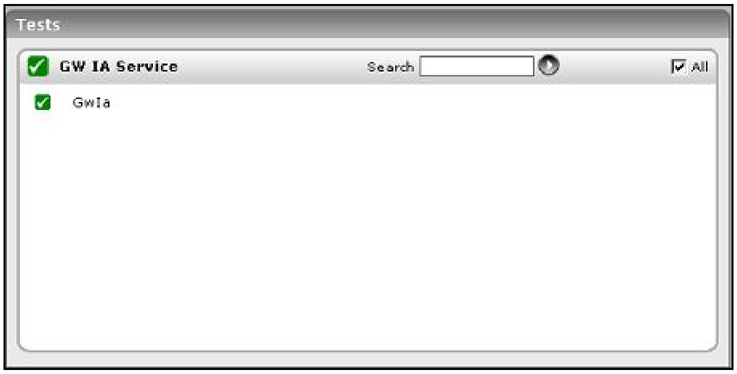


Figure 3.2: The test associated with the GW IA Service layer

This test is common to both the Netware and Windows environments.

3.1.1 Groupwise IA Test

This test reports performance statistics pertaining to a GWIA application on Netware/Windows.

Target of the test : A GWIA application

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every GWIA application being monitored.

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 this test is to be configured.
Port	The port at which the server listens. By default, this is 25.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.

Parameter	Description
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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:

Parameter	Description
	- **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

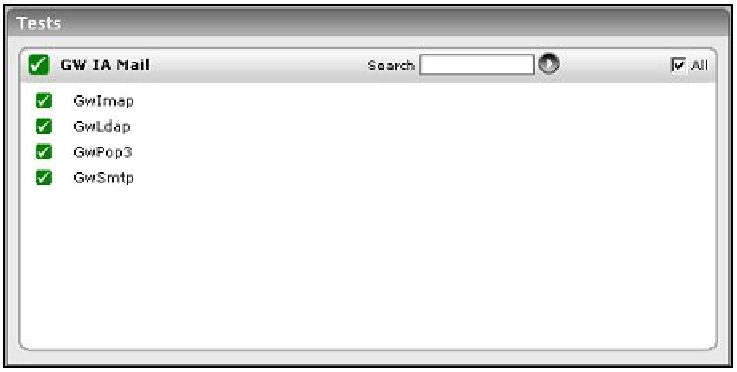
Measurement	Description	Measurement Unit	Interpretation
Data transmit rate	The rate at which message bytes were sent to the GWIA.	Bytes/Sec	This measure is indicative of the throughput of the GWIA. If this rate is high, it means that the GWIA is processing a high volume of data. A low value indicates a lower throughput.
Data receive rate	Indicates the rate at which message bytes were received from GWIA.	Bytes/Sec	This measure is indicative of the throughput of the GWIA. If this rate is high, it means that the GWIA is processing a high volume of data. A low value indicates a lower throughput.
Messages sent	Indicates the number of messages sent to the GWIA per second.	Msgs/Sec	This measure is indicative of the throughput of the GWIA. If this rate is high, it means that the GWIA is processing a high volume of data. A low value indicates a lower throughput.
Messages received	Indicates the number of messages received from	Msgs/Sec	This measure is indicative of the throughput of the GWIA. If this rate is

Measurement	Description	Measurement Unit	Interpretation
	the GWIA per second.		high, it means that the GWIA is processing a high volume of data. A low value indicates a lower throughput.
Message send errors	The number of failed transfers to the GWIA per second.	Msgs/Sec	This value should be low or preferably zero. A high value indicates poor performance of the server or incorrect addresses.
Message receive errors	Indicates the number of failed transfers from the GWIA per second.	Msgs/Sec	This value should be low or preferably zero. A high value indicates poor performance of the server or incorrect addresses.
Messages in output queue	Indicates the number of messages to be processed by the GWIA. The WPCSOUT directory stores these messages.	Number	A consistently high value indicates a problem in sending mails. This value should be preferably low. A high value of this measure over a period of time may lead to dead mails and poor performance of the server.
Messages in input queue	Indicates the number of messages to be processed by the GWIA. The WPCSIN directory stores these messages.	Number	A consistently high value may be indicative of MTA domain link failure. Check whether all MTAs are running and their link configurations are correct.
Messages in hold queue	Indicates the number of messages in the GWHOLD directory that are scheduled for delayed delivery.	Number	A consistently high value indicates a problem in processing the withheld mails.
Messages in problem directory	Indicates the number messages in the GWIA's problem directory (GWPROB). These are usually messages that have been corrupted during transmission or that have the wrong Internet address.	Number	If this value is too large, recover messages from the GWPROB directory. To perform this recovery, copy the message files from the GWPROB directory into the RECEIVE directory with a new file extension.

3.2 The GW IA Mail Layer

This layer enables you to assess the effectiveness of each of the following services that are offered by the GWIA:

- SMTP
- IMAP
- LDAP
- POP3



Tests

☑ GW IA Mail

Search ☑ All

☑ GwImap

☑ GwLdap

☑ GwPop3

☑ GwSmtp

Figure 3.3: The tests associated with the GW IA Mail Layer

These tests are common to both the Netware and Windows environments.

3.2.1 Groupwise SMTP Test

This test reports performance statistics pertaining to a GWIA application's SMTP service.

Target of the test : A GWIA application

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every GWIA application being monitored.

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 this test is to be configured.

Parameter	**Description**
Port	The port at which the server listens. By default, this is 25.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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

Parameter	Description
	• **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Available send threads	Indicates the number of SMTP daemon send threads available.	Number	If this value remains as 0 for a considerable period of time, you might want to increase the total number of send threads.
Available receive threads	Indicates the number of SMTP daemon receive threads available.	Number	If this value remains as 0 for a considerable period of time, you might want to increase the total number of receive threads.

Measurement	Description	Measurement Unit	Interpretation
Active send threads	Indicates the number of SMTP daemon send threads that are currently active.	Number	
Active receive threads	Indicates the number of SMTP daemon receive threads that are currently active.	Numbers	
MX lookup errors	Indicates the rate at which the SMTP daemon queries the Domain Name Server (DNS) for the address of the destination host and receives a SERVER FAIL code message back from the DNS. These messages will be deferred and automatically re-queued according to the Retry Schedule.	Errors/Sec	If the number of messages is very high, you might want to check the DNS to make sure the tables are not corrupted. If you are using a remote DNS, you might consider setting up a local DNS server. It could also mean that your file server TCP/IP is not correctly configured.
Host unknown errors	Indicates the rate at which the SMTP daemon attempted to do a lookup on a destination host and the host name did not exist in either the DNS records or in the host table.	Errors/Sec	
Host down errors	Indicates the rate at which the SMTP daemon tried to open a connection with the destination host and received a connection refused status. This is a temporary error. These messages will be deferred and automatically re-queued according to the Retry Schedule.	Errors/Sec	

Measurement	Description	Measurement Unit	Interpretation
Tcp read errors	Indicates the rate at which TCP/IP read errors indicating some communication problem occurred. This is a temporary error. These messages will be deferred and automatically re-queued according to the retry schedule.	Errors/Sec	If this value is consistently high, you might want to contact your Internet service provider to check for anything that could hinder communication, such as network problems or line noise. You might also want to adjust the timeout switches, particularly the /te and the /tr switches.
Tcp write errors	Indicates the rate at which TCP/IP write errors indicating some communication problem occurred. This is a temporary error. These messages will be deferred and automatically re-queued according to the retry schedule.	Errors/Sec	If this value is consistently high, you might want to contact your Internet service provider to check for anything that could hinder communication, such as network problems or line noise. You might also want to adjust the timeout switches, particularly the /te and the /tr switches.
Messages sent	Indicates the number of SMTP daemon messages sent per second.	Msgs/Sec	If this rate is high, it indicates that the SMTP daemon is processing high volume of mail. A low value indicates a lower throughput.
Messages received	Indicates the number of SMTP daemon messages received per second.	Msgs/Sec	If this rate is high, it indicates that the SMTP daemon is processing high volume of mail. A low value indicates a lower throughput.
Messages in send queue	Indicates the number of messages queued to the daemon from GWIA. These messages will be available in the SEND directory.	Number	If this value is consistently high, increase the number of SMTP send threads available.
Messages in receive queue	Indicates the number of messages queued to the GWIA from the SMTP	Number	If this value is consistently high, increase the number of SMTP receive threads available.

Measurement	Description	Measurement Unit	Interpretation
	daemon. These messages will be available in the RECEIVE directory.		
Messages in retry queue	Indicates the number of messages queued to retry for SMTP daemon on the GWIA. Such messages will be available in the DEFER directory.	Number	A very high value can impact the performance of the GWIA. Therefore, increase the number of available SMTP send threads to handle retry queue messages effectively.

3.2.2 Groupwise POP3 Test

This test reports the performance metrics pertaining to the POP3 service provided by the GroupWise Internet Agent (GWIA).

Target of the test : A GWIA application

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every GWIA application being monitored.

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 this test is to be configured.
Port	The port at which the server listens. By default, this is 25.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.

Parameter	Description
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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:

Parameter	Description
	• **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Available sessions	Indicates the number of POP3 server sessions currently available.	Number	If this value is 0 over a period of time, then increase the total number of POP3 threads.
Active sessions	Indicates the number of POP3 server sessions currently active.	Number	
Messages downloaded	Indicates the number of POP3 messages downloaded per second.	Msgs/Sec	This measure is indicative of the throughput of the POP3 service. If this rate is high, it means that the POP3 service is processing high volume of mail. A low value indicates a lower throughput.
Login errors	Indicates the rate at which errors occurred while logging into the GroupWise Post Office.	Errors/Sec	If this value is consistently high, check the availability of the Post Office Agent (POA) and the Internet Agent (IA) link to the post office.
Message retrieval	Indicates the rate at which	Errors/Sec	If this value is consistently high, check

Measurement	Description	Measurement Unit	Interpretation
errors	errors occurred while retrieving messages from a GroupWise Post Office.		the availability of the Post Office Agent (POA) and the Internet Agent (IA) link to the post office.
POP3 conversion errors	Indicates the rate at which errors occurred while converting messages for POP3 download.	Errors/Sec	
Unknown user errors	Indicates the rate at which unknown user errors occurred while logging into the POP3 server.	Errors/Sec	
Bad password errors	Indicates the rate at which bad password errors occurred while logging into the POP3 server.	Errors/Sec	
Access denied errors	Indicates the rate at which errors denying access to the POP3 server occurred.	Errors/Sec	
TCP read errors	Indicates the rate of POP3 Server TCP/IP read errors.	Errors/Sec	
TCP write errors	Indicates the rate of POP3 Server TCP/IP write errors.	Errors/Sec	

3.2.3 Groupwise LDAP est

This test reports the performance metrics pertaining to the LDAP service provided by the GroupWise Internet Agent (GWIA).

Target of the test : A GWIA application

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every GWIA application being monitored.

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 this test is to be configured.
Port	The port at which the server listens. By default, this is 25.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the

Parameter	Description
	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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Available sessions	Indicates the number of LDAP server sessions currently available.	Number	If this value is 0 over a period of time, then increase the total number of POP3 threads.

Measurement	Description	Measurement Unit	Interpretation
Active sessions	Indicates the number of LDAP server sessions currently active.	Number	
Search rate	Indicates the rate of LDAP queries against the GroupWise Address Book.	Reqs/Sec	
Search entries	Indicates the number of address book entries returned for the search requests.	Number	

3.2.4 Groupwise IMAP Test

This test reports the performance metrics pertaining to the IMAP service provided by the GroupWise Internet Agent (GWIA).

Target of the test : A GWIA application

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every GWIA application being monitored.

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 this test is to be configured.
Port	The port at which the server listens. By default, this is 25.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen

Parameter	Description
	is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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:

Parameter	Description
	- **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Available sessions	Indicates the number of IMAP server sessions currently available.	Number	If this value is 0 over a period of time, then increase the total number of IMAP threads.
Active sessions	Indicates the number of IMAP server sessions currently active.	Number	
Messages downloaded	Indicates the number of IMAP messages downloaded per second.	Msgs/Sec	This measure is indicative of the throughput of the IMAP service. If this rate is high, it means that the IMAP service is processing high volume of mail. A low value indicates a lower throughput.
Login errors	Indicates the rate at which errors occurred while logging into the GroupWise Post Office.	Errors/Sec	If this value is consistently high, check the availability of the Post Office Agent (POA) and the Internet Agent (IA) link to the post office.
Message retrieval	Indicates the rate at which	Errors/Sec	If this value is consistently high, check

Measurement	Description	Measurement Unit	Interpretation
errors	errors occurred while retrieving messages from a GroupWise Post Office.		the availability of the Post Office Agent (POA) and the Internet Agent (IA) link to the post office.
Message conversion errors	Indicates the rate at which errors occurred while converting messages for IMAP download.	Errors/Sec	
Unknown user errors	Indicates the rate at which unknown user errors occurred while logging into the IMAP server.	Errors/Sec	
Bad password errors	Indicates the rate at which bad password errors occurred while logging into the IMAP server.	Errors/Sec	
Access denied errors	Indicates the rate at which errors denying access to the IMAP server occurred.	Errors/Sec	
TCP read errors	Indicates the rate of IMAP Server TCP/IP read errors.	Errors/Sec	
TCP write errors	Indicates the rate of IMAP Server TCP/IP write errors.	Errors/Sec	

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.