Monitoring Novell Groupwise Components

eG Enterprise v6

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 NT, Windows 2000, Windows 2003 and Windows 2008 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

Table of Contents

Table of Figures

Chapter 1

Introduction

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 GroupWise components is essential.

eG Enterprise provides specialized models for monitoring each of the following key GroupWise components:

- GroupWise Internet Agent (GWIA)
- GroupWise Message Transfer Agent (MTA)
- GroupWise Post Office Agent (POA)
- GroupWise Web Access Agent (GwWeb)

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 by eG Enterprise*, refer to the *eG User Manual*.

This document will discuss each of the above-mentioned monitoring models in great detail.

Chapter 2

Monitoring the GroupWise Internet Agent (GWIA)

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.

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 2.1 below depicts the *Groupwise Internet Agent - Netware* model.

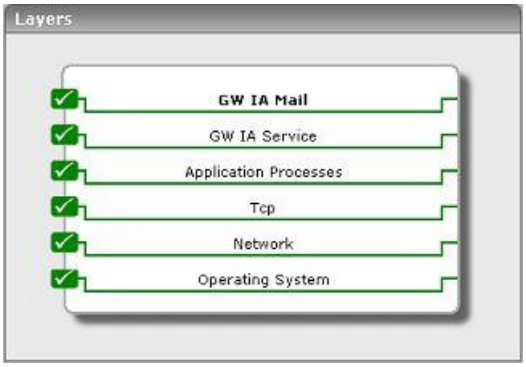

Figure 2.1: Layer model of GWIA

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 Figure 2.1. 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 Chapter 4 in the *Monitoring Applications that Support the Host Resources MIB* document.

Since the bottom layers of Figure 2.1 have all been dealt with in other documents, let us simply focus on the top 2 layers of Figure 2.1.

2.1 The GW IA Service Layer

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

Figure 2.2: The test associated with the GW IA Service layer

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

2.1.1 Gwla Test

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

Purpose	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

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. **port** – The port at which the server listens. By default, this is 25. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here. 15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
Outputs of the test	One set of results for every GWIA application being monitored.

Measurements made by the test	Measurement	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 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.
	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.

2.2 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

Figure 2.3: The tests associated with the GW IA Mail Layer

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

2.2.1 GwSmtp Test

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

Purpose	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

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. **port** – The port at which the server listens. By default, this is 25. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every GWIA application being monitored.		
Measurements made by the test	**Measurement**	**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.
	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	
	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 daemon. These messages will be available in the RECEIVE directory.	Number	If this value is consistently high, increase the number of SMTP receive threads available.
	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.

2.2.2 GWPop3 Test

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

Purpose	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	A remote agent

test	

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. **port** – The port at which the server listens. By default, this is 25. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every GWIA application being monitored.		
Measurements made by the test	**Measurement**	**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 errors: Indicates the rate at which errors occurred while retrieving messages from a 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.
	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	

2.2.3 GwLdap est

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

Purpose	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

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. **port** – The port at which the server listens. By default, this is 25. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every GWIA application being monitored.		
Measurements made by the test	**Measurement**	**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.
	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	

2.2.4 GwImap Test

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

Purpose	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

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. **port** – The port at which the server listens. By default, this is 25. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every GWIA application being monitored.		
Measurements made by the test	**Measurement**	**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 errors: Indicates the rate at which errors occurred while retrieving messages from a 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 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	

Chapter 3

Monitoring the GroupWise MTAs

A domain organizes post offices into a logical grouping for addressing, routing, and administration purposes in your GroupWise® system. Messages are transferred between post offices and domains by the Message Transfer Agent (MTA).

The Internet Agent picks up inbound e-mail messages from the Internet, converts them into the GroupWise message format, and then passes the converted messages to the GroupWise Message Transfer Agent (MTA). For outgoing messages transported by the Internet, the GroupWise MTA passes the message to the Internet Agent, which then converts the message to Internet messaging format, and then sends it to the designated Internet address.

Error-free functioning of the MTA is imperative to ensure the prompt delivery of messages to the post offices or domains. Non-availability of the MTA or long winding message queues at the MTA can significantly delay the delivery of critical messages. To prevent such problem situations, the MTA's performance needs to be brought under the scanner.

eG Enterprise prescribes two specialized monitoring models for the MTA – one for every operating system that is executes on. While the MTA on Netware can be monitored using the *Groupwise MTA - Netware* component-type, the one on Windows can be managed as *Groupwise MTA - Win*. Figure 3.1 depicts the *Groupwise MTA - Win* monitoring model.

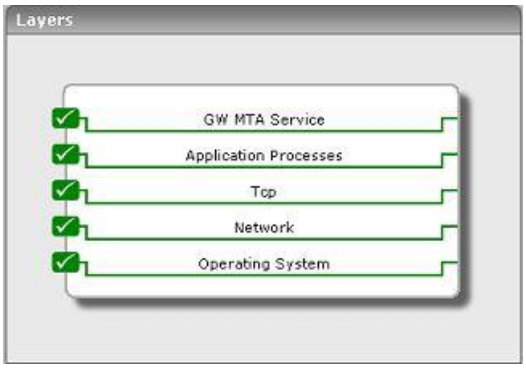

Figure 3.1: The layer model of a GroupWise MTA application

Though both the *Groupwise MTA - Netware* and *Groupwise MTA - Win* 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 Figure 3.1. 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 Chapter 4 in the *Monitoring Applications that Support the Host Resources MIB* document.

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

3.1 The GW MTA Service Layer

This layer monitors the GWMTA in and out to reveal the following:

- Availability and responsiveness of the MTA
- Overall MTA health in terms of the throughput seen by the MTA, outstanding messages to the MTA, error-filled messages, etc.
- The health of the MTA's Admin thread
- The type and length of the message queues on the MTA

Figure 3.2: The tests associated with the GW MTA Service layer

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

3.1.1 MtaPort Test

The MtaPort test reports the availability and responsiveness of the GroupWise Message Transfer Agent (MTA).

Purpose	Reports the availability and responsiveness of the GroupWise Message Transfer Agent (MTA)
Target of the test	A GWMTA application
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **targetports** – The port number of the MTA component to be monitored. By default, the value in the **PORT** text box will be displayed here.

Outputs of the test	One set of results for the GWMTA port specified		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Availability: Indicates whether the TCP connection is available or not.	Percent	An availability problem can be caused by different factors – e.g., the server process may not be up, a network problem may exist, or there could be a configuration problem with the DNS server.
	Response time: Indicates the time taken (in seconds) by the server to respond to a request.	Secs	An increase in response time can be caused by several factors such as a server bottleneck, a configuration problem with the DNS server, a network problem, etc.

3.1.2 Mta Test

This test measures the health of the GroupWise Message Transfer Agent (MTA).

Purpose	Measures the health of the GroupWise Message Transfer Agent (MTA)
Target of the test	A GWMTA application
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **mtadomainname** - The name of the domain on which the MTA has been installed. 16. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every domain specified.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total domains: Indicates the number of domains serviced by this MTA.	Number	
	Closed domains: Indicates the number of closed domains serviced by this MTA.	Number	If the value is greater than 0, identify the closed domains and determine the reason for their non-availability. Domain closure could occur due to the following reasons: ➢ Improper domain link configuration: If the domain link of the closed domain is found to be improperly configured, then configure it correctly. ➢ Threads executing on the MTA stop functioning: In this case, restart the MTA to ensure that the threads start executing. ➢ MTA crash: Here again, revive the MTA by restarting it.
	Total postoffices: Indicates the number of post offices serviced by this MTA.	Number	
	Closed postoffices: Indicates the number of closed post offices serviced by this MTA.	Number	If the value is greater than 0, identify the closed post offices and determine the reason for their non-availability. Post office closure could occur due to the following reasons: ➢ Improper POA (Post Office Agent) link configuration: If the POA link of the closed POA is found to be improperly configured, then configure it correctly. ➢ POA crash: Here again, revive the POA by restarting it.

<table>
<tr><td></td><td>Total gateways:
Indicates the number of gateways serviced by this MTA.</td><td>Number</td><td colspan="2"></td></tr>
<tr><td></td><td>Closed gateways:
Indicates the number of closed gateways serviced by this MTA.</td><td>Number</td><td colspan="2">If the value is greater than 0, identify the closed gateways and determine the reason for their non-availability. Gateway closure could occur due to the following reasons:
➢ Improper gateway link configuration: If the link to the closed gateway is found to be improperly configured, then configure it correctly.
➢ Gateway crash: In this case, revive the POA by restarting it.</td></tr>
<tr><td></td><td>Messages tranferred:
Indicates the number of messages routed by this MTA during the last measurement period.</td><td>Msgs/Sec</td><td colspan="2">This measure is an indicative of the throughput of the MTA. If this rate is high, the MTA is processing high volume of messages. A low value indicates a lower throughput.</td></tr>
<tr><td rowspan="4"></td><td rowspan="4">Undeliverable messages:
Indicates the number of messages that were not delivered by this MTA during the last measurement period.</td><td rowspan="4">Number</td><td>Possible Cause</td><td>Action</td></tr>
<tr><td>The sender typed the recipient's address incorrectly.</td><td>Have the sender select the recipient in the GroupWise Address Book so the address is provided automatically, then resend the message.</td></tr>
<tr><td>The recipient's mailbox might be damaged so the message cannot be delivered.</td><td>In ConsoleOne perform maintenance to correct any problems with the recipient's mailbox.</td></tr>
<tr><td>If the recipient is a brand new user, the sender might have sent the message before the recipient was actually created in the post office.</td><td>Verify the existence of the user in the post office before the sender tries to send the message again.</td></tr>
</table>

			If the sender is selecting a group, rather than an individual recipient, from the GroupWise Address Book, the group could be out of date if the recipient's user ID has changed.	Re-create the group by selecting each individual user from the Address Book to make sure current user IDs and post offices are included in the group.
	Error messages: Indicates the number of error messages found by this MTA during the last measurement period. These messages will be placed in the domain\wpcsout\problem directory.	Msgs/Sec	Check the messages and attached files for damage.	
	Domain available disk space: Indicates the free space available in the volume in which the domain resides.	MB	If this value is very low, check the MTA input queue size and resolve the problems with the closed facilities so that normal message flow resumes.	

3.1.3 MtaAdminThreads Test

The MtaAdminThread test measures the health of the GroupWise Message Transfer Agent's (MTA) admin thread.

Purpose	Measures the health of the GroupWise Message Transfer Agent's (MTA) admin thread
Target of the test	A GWMTA application
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **mtadomainname** - The name of the domain on which the MTA has been installed. 16. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every domain specified.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Thread status: Indicates the status of the admin thread.	Number	If the value is 1, it indicates that the thread is running. If the value is 0, it indicates that the thread is not running. Therefore, start the thread. If the value is –1, it indicates that the status is "unknown". In such a case, restart the MTA.
	Message processing rate: Indicates the rate at which admin messages were processed by this MTA during the last measurement period.	Msgs/Sec	A high value may be indicative of an excessive load on the admin thread.
	Error messages: Indicates the rate at which admin message errors were detected by this MTA during the last measurement period.	Msgs/Sec	If this value is high, check the domain DB status.
	Messages in queue: Indicates the number of admin messages waiting to be processed.	Number	If this value is high, check the admin thread status and Msgs_processing_rate, and then, act accordingly.
	Database status: Indicates the status of the domain database.	Number	The status indicators are: ➢ 1 - Normal ➢ 0 - Database error ➢ -1 - Unknown 0 indicates a critical database error. The domain database cannot be recovered. Rebuild the domain database using ConsoleOne. The MTA admin thread will not process any more administrative messages until the database status has returned to Normal. If the value is –1, restart the MTA.

	Database recoveries: Indicates the number of DB recoveries performed during the last measurement period.	Number	If the frequency of db_recovery is more, it may be indicative of a critical database error.

3.1.4 MtaLocalQueues Test

This test reports the performance metrics pertaining to the local queue on a GroupWise Message Transfer Agent (MTA).

Purpose	Reports the performance metrics pertaining to the local queue on a GroupWise Message Transfer Agent (MTA)
Target of the test	A GWMTA application
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here.

	15. **mtadomainname** - The name of the domain on which the MTA has been installed. 16. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for every domain specified.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Router queue length: Indicates the number of messages in the routing queue. These messages will be available in the gwinprog directory, which is the MTA "in progress" queue directory.	Number	A consistently high value indicates a problem in delivering messages. This value should be preferably low.
	Postoffice messages hold queue length: Indicates the number of messages in local post office and gateway queues. Such messages will be available in the "postx" directory, which is the holding directory for post offices.	Number	If the value is high, check for closed post offices.
	Postoffice messages hold queue size: Indicates the total size of the messages in the local post offices.	KB	If the value is high, check for closed post offices.
	Domain messages hold queue length: Indicates the number of messages in the other domain queues. Such messages will be available in the "domainx" directory, which is the holding directory for other domains.	Number	If the value is high, check for closed domains.

	Domain messages hold queue size: Indicates the total size of the messages in other domain queues.	KB	If the value is high, check for closed domains.
	Gateway messages hold queue length: Indicates the number of messages in gateway queues. Such messages will be available in the "gatewayx" directory, which is the holding directory for gateways.	Number	If the value is high, check for closed gateways.
	Gateway messages hold queue size: Indicates the size of all the messages in gateway queues.	KB	If the value is high, check for closed gateways.

To know the domain name of an MTA, do the following:

1. Execute Novell's **ConsoleOne** utility. This utility allows you to manage eDirectory objects, rights, and schema, and Netware file system resources.
2. Upon logging into the console, you will find a tree-structure in the left pane that hosts an NDS container (see Figure 3.3). Expanding this container will reveal the eDirectory trees that you are currently logged into. Expand the eDirectory tree that hosts the MTA application to be monitored. Upon expanding, the list of contexts defined within the tree will appear. Next, expand the context, which houses the MTA application.

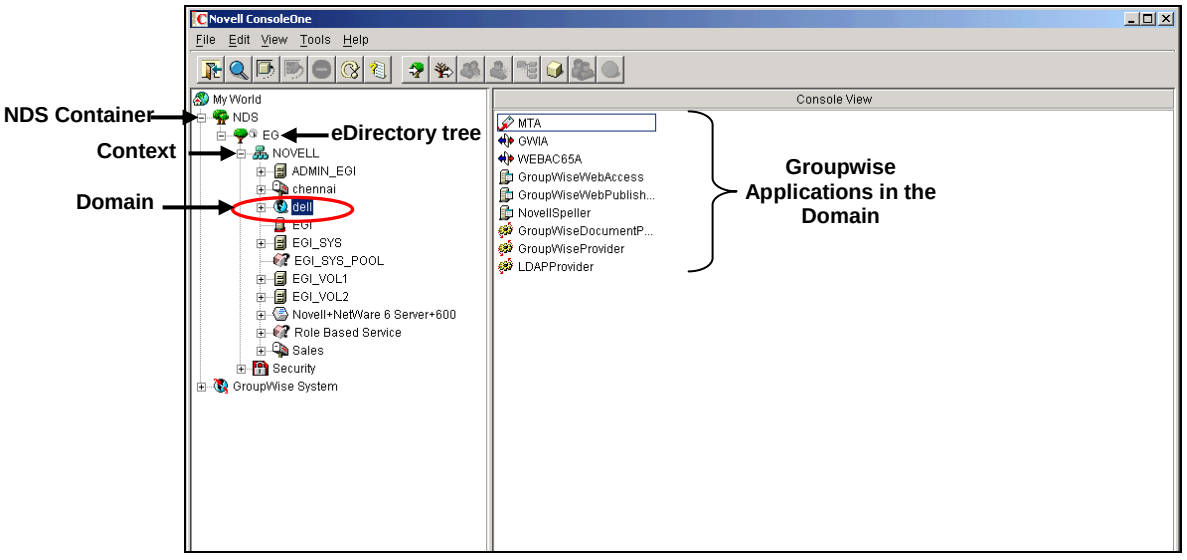

Figure 3.3: The Novell ConsoleOne window

3. The complete list of objects within the selected context will then be available to you. The objects in the list that are prefixed by the symbol represent the domains within the context (see Figure 3.3). Now, click on the domain that hosts the MTA application to be monitored. When this is done, all the Groupwise applications that exist in the domain will appear in the right pane (see Figure 3.3).

4. From the right pane, select the MTA application to be monitored, right-click on it, and select **Properties** (see Figure 3.4). Click on the GroupWise tab to open the **Identification** tab page. In this page, look for the domain name of the MTA application (see Figure 3.5).

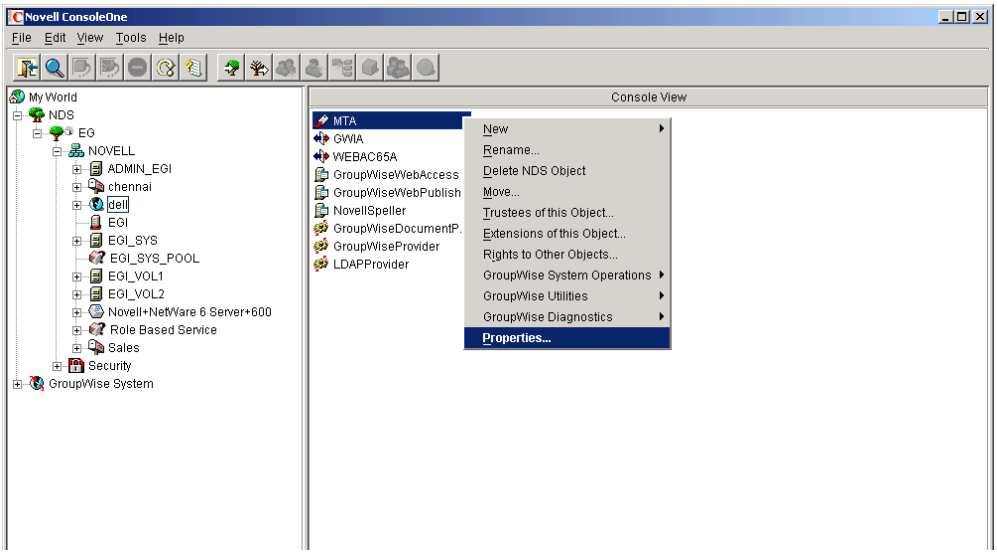

Figure 3.4: Selecting the Properties option from the MTA application's right-click menu

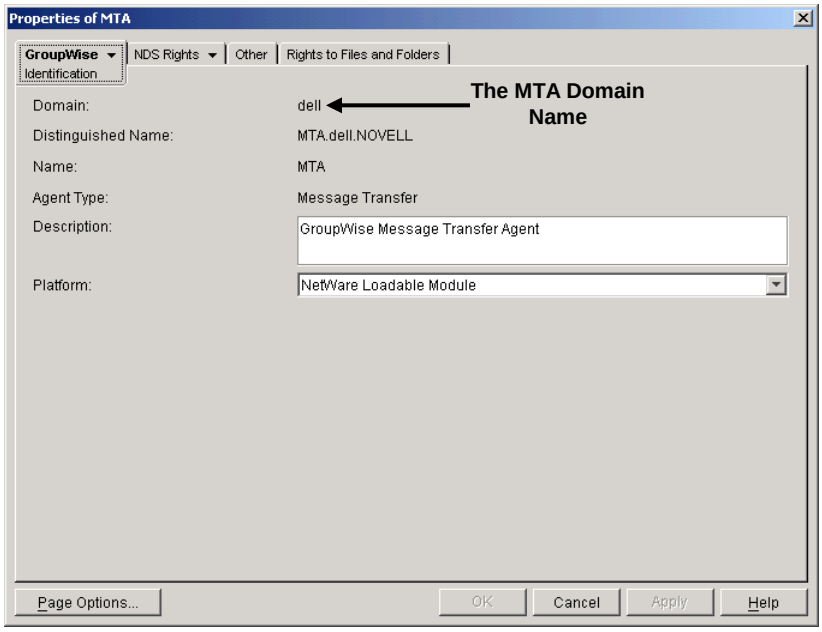

Figure 3.5: Viewing the MTA domain name

Chapter 4

Monitoring the GroupWise Post Office Agents (POA)

A post office is a collection of user mailboxes and GroupWise® objects. Messages are delivered into mailboxes by the Post Office Agent (POA). If the POA is unavailable or very slow, then many messages, even some of a high priority, might not be able to reach the mailboxes of recipients, and would be queued instead. If the situation is not rectified soon, the message queue might get choked, and many critical messages might be lost in the process. If such ill consequences are to be avoided, then the POA should be constantly monitored.

eG Enterprise prescribes two specialized monitoring models for the POA – one for every operating system that it executes on. While the POA on Netware can be monitored using the *Groupwise Post Office - Netware* component-type, the one on Windows can be managed as *Groupwise Post Office - Win*. Figure 4.1 depicts the *Groupwise Post Office - Netware* monitoring model.

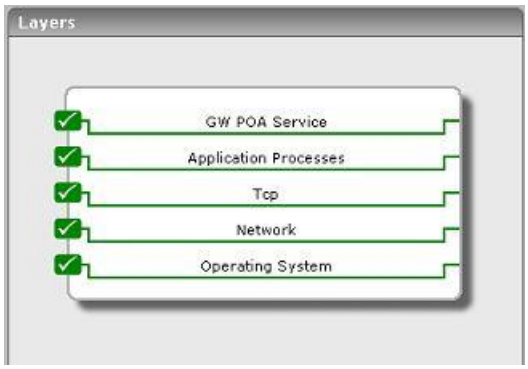

Figure 4.1: Layer model of a GWPOA

Though both the *Groupwise Post Office - Netware* and *Groupwise Post Office - Win* 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 Figure 4.1. 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 Chapter 4 in the *Monitoring Applications that Support the Host Resources MIB* document.

Since the bottom layers of Figure 4.1 have all been dealt with in other documents, let us simply focus on the top layer of Figure 4.1.

4.1 The GW POA Service Layer

Using the tests associated with it, the **GW POA Service** layer indicates the following:

- Availability and responsiveness of the POA
- How well the POA processes messages
- How well the POA handles client/server requests
- The health of the POA's admin thread

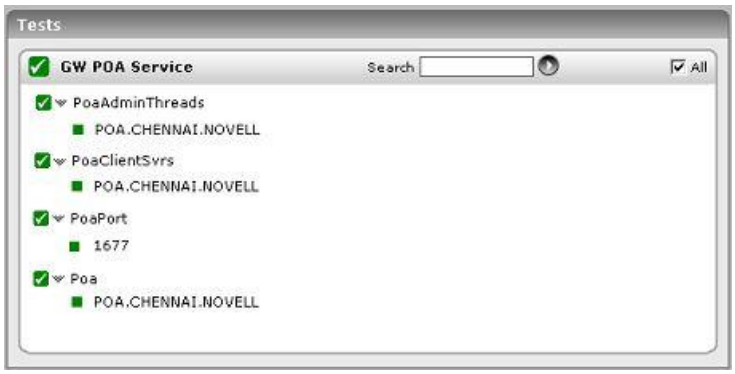

Figure 4.2: The tests associated with the GW POA Service layer

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

4.1.1 PoaPort Test

The PoaPort test reports the availability and responsiveness of the GroupWise Post Office Agent (POA).

Purpose	Reports the availability and responsiveness of the GroupWise Post Office Agent (POA).		
Target of the test	A GWPOA application		
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **targetports** – The port number of the POA component to be monitored. By default, the value in the **PORT** text box will be displayed here.		
Outputs of the test	One set of results for the GWPOA port specified		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Availability:** Indicates whether the TCP connection is available or not.	Percent	An availability problem can be caused by different factors – e.g., the server process may not be up, a network problem may exist, or there could be a configuration problem with the DNS server.
	Response time: Indicates the time taken (in seconds) by the server to respond to a request.	Secs	An increase in response time can be caused by several factors such as a server bottleneck, a configuration problem with the DNS server, a network problem, etc.

4.1.2 Poa Test

The Poa test measures the health of the GroupWise Post Office Agent (POA).

Purpose	Measures the health of the GroupWise Post Office Agent (POA)
Target of the test	A GWPOA application
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here. 15. **POAname** - The distinguished name of the POA.

	16. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for the distinguished name specified		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Message processing rate: Indicates the rate at which messages were processed during the last measurement period.	Msgs/Sec	This measure is indicative of the throughput of the POA. If this rate is high, it indicates that the POA is processing a high volume of mails. A low value indicates a lower throughput.
	Problem messages: Indicates the number of problem messages.	Number	If this value is high, it indicates that a large number of problem messages are being handled by the POA. Under such circumstances, you should first determine the cause of the damage. Sometimes a problem file can be handled successfully if re-queued. In such cases, place the file in the proper priority 0 subdirectory, as indicated by the extension on the message file. Placing it in the 0 subdirectory gives it high priority for reprocessing. If conditions have changed on the network, the message might be able to be processed. If the message still cannot be processed after being re-queued, it means that it has been damaged in some way that makes it unreadable. This will happen only rarely.
	High priority queue messages: Indicates the number of high priority messages waiting to be processed.	Number	If this value is high, you can increase throughput for the high priority queue directory using the /FAST4 startup switch of the MTA. This causes the MTA to monitor and process the high priority messages separately from the normal and low priority messages. This helps avoid bottlenecks in the processing of administrative messages and high priority user messages versus normal and low priority user messages.

	Normal priority queue messages: Indicates the number of normal priority messages waiting to be processed.	Number	If this value is high, you can increase throughput for the normal priority queue directory using the /FAST4 startup switch of the MTA. This causes the MTA to monitor and process the high priority messages separately from the normal and low priority messages. This helps avoid bottlenecks in the processing of administrative messages and high priority user messages versus normal and low priority user messages.
	Post office disk space problem: Indicates the disk space available in the volume on which the Post office resides.	MB	If this value is very low, free some space on this volume.
	Mtp status: Indicates the status of the Message Transfer Protocol (MTP).	Number	The status indicators are: ➢ 0 – Unknown ➢ 1 – Closed ➢ 2 – Open ➢ 3 – Sendopen ➢ 4 – Receiveopen If the status is unknown, restart the POA. If the status is closed, start the MTP to send and receive threads.

4.1.3 PoaClientSvrs Test

This test reports the performance metrics pertaining to the GroupWise client connections of the GroupWise Post Office Agent (POA).

Purpose	Reports the performance metrics pertaining to the GroupWise client connections of the GroupWise Post Office Agent (POA)
Target of the test	A GWPOA application
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here. 15. **POAname** - The distinguished name of the POA.

	16. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for the distinguished name specified		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Request rate: Indicates the rate at which client/server requests were received during the last measurement period.	Reqs/Sec	A high value may be indicative of an excessive load on the POA.
	Pending requests: Indicates the number of Client/Server requests pending.	Number	If this value is high, increase the number of POA threads so that more users can be serviced by the POA.
	User timeouts: Indicates the number of user sessions that timed out during the last measurement period. This can be calculated by: **(Current measure – Previous measure)**	Number	Session timeouts do not indicate a problem with the POA, but rather a problem with the users. Users who have timed out are users for which the POA has closed the connection because the GroupWise client was no longer communicating. Timed out users may not be exiting GroupWise normally or may be having other problems with their workstations.
	Messages in queue: Indicates the number of messages in the queues.	Number	If this value is high, you can increase throughput for the message queues using the /FAST4 startup switch of the MTA. This causes the MTA to monitor and process the high priority messages separately from the normal and low priority messages. This helps avoid bottlenecks in the processing of administrative messages and high priority user messages versus normal and low priority user messages.
	Users connected: Indicates the number of connected user sessions.	Number	

4.1.4 PoaAdminThreads Test

This test reports the performance metrics pertaining to the admin thread executing on a GroupWise Post Office Agent (POA).

Purpose	Reports the performance metrics pertaining to the admin thread executing on a GroupWise Post Office Agent (POA).
Target of the test	A GWPOA application
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here. 15. **POAname** - The distinguished name of the POA.

	16. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for the distinguished name specified		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Thread status: Indicates the status of the admin thread.	Number	If the value is 1, it indicates that the thread is running. If the value is 0, it indicates that the thread is not running. Therefore, start the thread. If the value is –1, it indicates that the status is "unknown". In such a case, restart the POA.
	Message processing rate: Indicates the rate at which admin messages were processed by this MTA during the last measurement period.	Msgs/Sec	A high value may be indicative of an excessive load on the admin thread.
	Error messages: Indicates the rate at which admin message errors were detected by this MTA during the last measurement period.	Msgs/Sec	If this value is high, check the Post office DB status.
	Messages in queue: Indicates the number of admin messages waiting to be processed.	Number	If this value is high, check the admin thread status and Msgs_processing_rate, and then, act accordingly.
	Database status: Indicates the status of the Post office database.	Number	The status indicators are: ➢ 1 - Normal ➢ 0 - Database error ➢ -1 - Unknown 0 indicates a critical database error. The Post office database cannot be recovered. Rebuild the database using ConsoleOne. The POA admin thread will not process any more administrative messages until the database status has returned to Normal. If the value is –1, restart the POA.

	Database recoveries: Indicates the number of DB recoveries performed during the last measurement period.	Number	If the frequency of db_recovery is more, it may be indicative of a critical database error.

To know the distinguished name of a POA, do the following:

1. First, execute Novell's **ConsoleOne** utility. This utility allows you to manage eDirectory objects, rights, and schema, and Netware file system resources.
2. Upon logging into the console, you will find a tree-structure in the left pane that hosts an NDS container (see Figure 4.3). Expanding this container will reveal the eDirectory trees that you are currently logged into. Expand the eDirectory that hosts the POA application to be monitored. Upon expanding, the list of contexts defined within the tree will appear. Next, expand the context within the eDirectory, which houses the POA application.

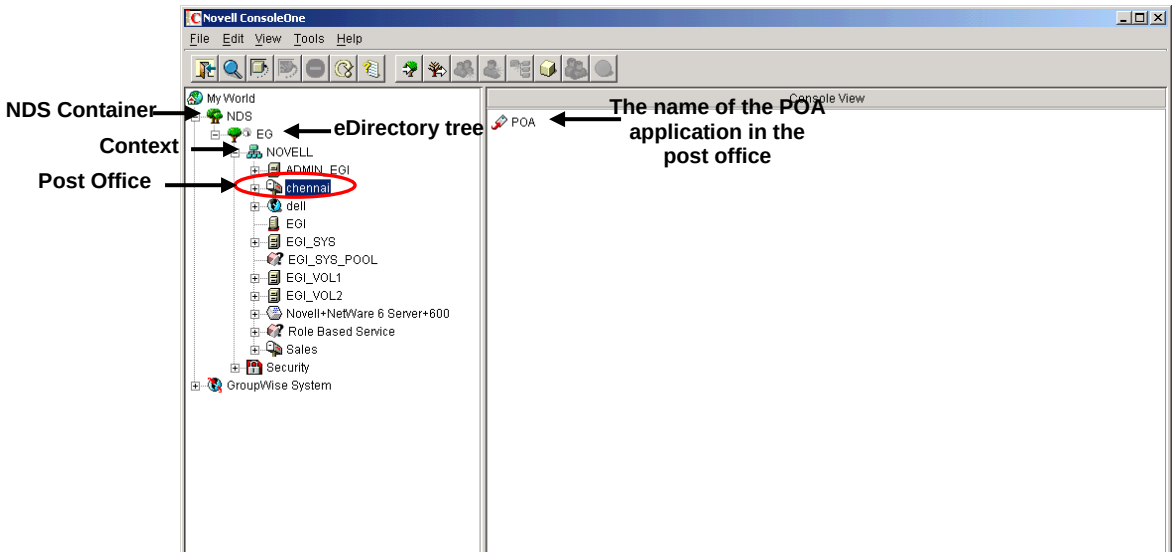

Figure 4.3: The Novell ConsoleOne window

3. The complete list of objects within the selected context will then be available to you. The objects in the list that are prefixed by the symbol represent the post offices within the context (see Figure 4.3). Now, click on the post office that hosts the POA application to be monitored. When this is done, the POA application that exists in the selected post office will appear in the right pane (see Figure 4.3).
4. From the right pane, select the POA application to be monitored, right-click on it, and select **Properties** (see Figure 4.4). Click on the **GroupWise** tab to open the **Identification** tab page. In this page, look for the distinguished name of the POA application (see Figure 4.5). The distinguished name should be in the following format:

   <The name of the POA application>.<The name of the post office>.<The name of the context>
5. Accordingly, the distinguished name of the POA application in the example of Figure 4.5 will be: *POA.chennai.NOVELL*.

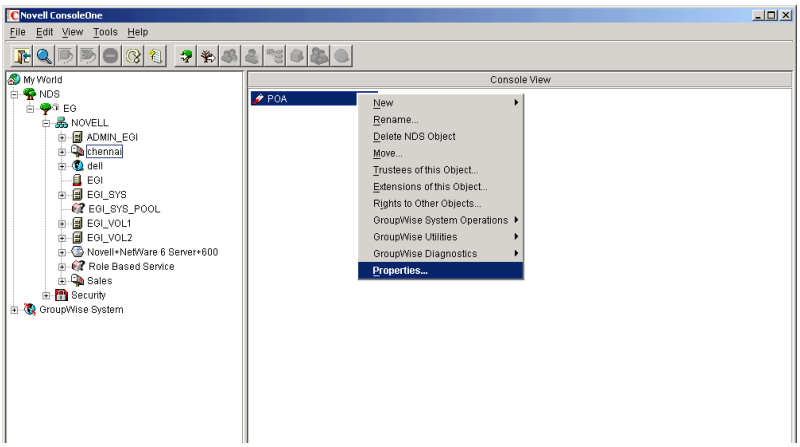

Figure 4.4: Selecting the Properties option from the POA application's right-click menu

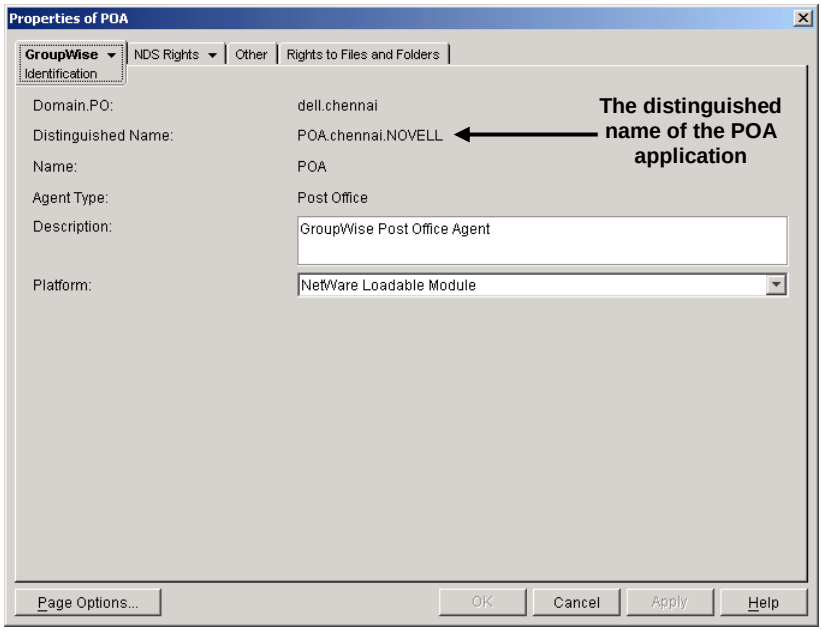

Figure 4.5: Viewing the distinguished name of the POA application

Chapter 5

Monitoring GroupWise WebAccess (GwWeb)

GroupWise® WebAccess is the World Wide Web version of GroupWise. Tapping the unique and powerful functionality of GroupWise messaging, GroupWise WebAccess lets you send and receive mail messages, appointments, tasks, notes, and attached files. In addition, you can keep track of your schedule with the Calendar, download copies of documents from document libraries you have access to, use Proxy to access other mailboxes, search for times when participants will be available for a meeting, check your shared and Find folders, and more.

Since the WebAccess component enables users to perform many critical tasks, if the component experiences performance degradations, these tasks may not be completed or might take too much time to complete. To avoid this, the performance of the WebAccess component must be continuously monitored.

eG Enterprise prescribes two specialized monitoring models for WebAccess – one for every operating system that it executes on. While WebAccess on Netware can be monitored using the *Groupwise Web - Netware* component-type, the one on Windows can be managed as *Groupwise Web - Win*. Figure 5.1 depicts the *Netware GwWeb* monitoring model.

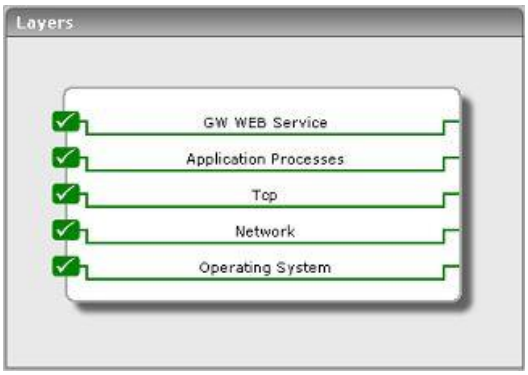

Figure 5.1: Layer model of a GWWeb

Though both the *Groupwise Web - Netware* and *Groupwise Web - Win* 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 Figure 5.1. 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 Chapter 4 in the *Monitoring Applications that Support the Host Resources MIB* document.

Since the bottom layers of Figure 5.1 have all been dealt with in other documents, let us simply focus on the top layer of Figure 5.1.

5.1 The GW WEB Service Layer

This layer, with the help of the tests mapped to it, enables administrators to figure out the following:

- Availability and responsiveness of the GwWeb
- Overall health of the GwWeb

Figure 5.2: The tests associated with the GW WEB Service layer

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

5.1.1 GwWebAgentPort Test

The GwWebAgentPort test reports the availability and responsiveness of the GroupWise Web Access Agent (GwWeb).

Purpose	Reports the availability and responsiveness of the GroupWise WebAccess Agent (GwWeb)		
Target of the test	A GwWeb application		
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **targetports** – The port number of the POA component to be monitored. By default, the value in the **PORT** text box will be displayed here.		
Outputs of the test	One set of results for the GWPOA port specified		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**Availability:** Indicates whether the TCP connection is available or not.	Percent	An availability problem can be caused by different factors – e.g., the server process may not be up, a network problem may exist, or there could be a configuration problem with the DNS server.
	Response time: Indicates the time taken (in seconds) by the server to respond to a request.	Secs	An increase in response time can be caused by several factors such as a server bottleneck, a configuration problem with the DNS server, a network problem, etc.

5.1.2 GwWebAgent Test

The GwWebAgent test reports performance metrics that indicate the overall health of the GroupWise Web Access Agent (GwWeb).

Purpose	Reports performance metrics that indicate the overall health of the GroupWise Web Access Agent (GwWeb)
Target of the test	A GwWeb application
Agent deploying the test	A remote 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. **port** – The port at which the server listens. 4. **snmpport** – The port at which the server exposes its SNMP MIB. The default is 161. 5. **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. 6. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 7. **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. 8. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 9. **confirm password** – Confirm the **authpass** by retyping it here. 10. **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 11. **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. 12. **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 13. **encryptpassword** – Specify the encryption password here. 14. **confirm password** – Confirm the encryption password by retyping it here. 15. **Webagentname** - The distinguished name of the WebAccess agent.

	16. **timeout** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for the name specified		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Request rate: Indicates the rate at which requests were serviced by the GwWeb.	Reqs/Sec	A high value over a long period of time may be indicative of an excessive load on the agent.
	Request failures: Indicates the number of failed requests per second	Reqs/Sec	This value must be low. A high value over a period of time indicates a problem in performance.
	Available threads: Indicates the number of available threads.	Number	If this value remains as 0 for a considerable period of time, increase the total number of threads.
	Busy threads: Indicates the number of currently busy threads	Number	
	Current users: Indicates the number of users currently connected	Number	

The distinguished name has to be specified in the format, <*webagentname*>.<*domainname*>. To know the <*webagentname*>, do the following:

1. First, execute Novell's **ConsoleOne** utility. This utility allows you to manage eDirectory objects, rights, and schema, and Netware file system resources.
2. Upon logging into the console, you will find a tree-structure in the left pane that hosts an NDS container (see Figure 5.3). Expanding this container will reveal the eDirectory trees that you are currently logged into. Expand the eDirectory that hosts the GwWeb application to be monitored. Upon expanding, the list of contexts defined within the tree will appear. Next, expand the context within the eDirectory, which houses the GwWeb application (see Figure 5.3).

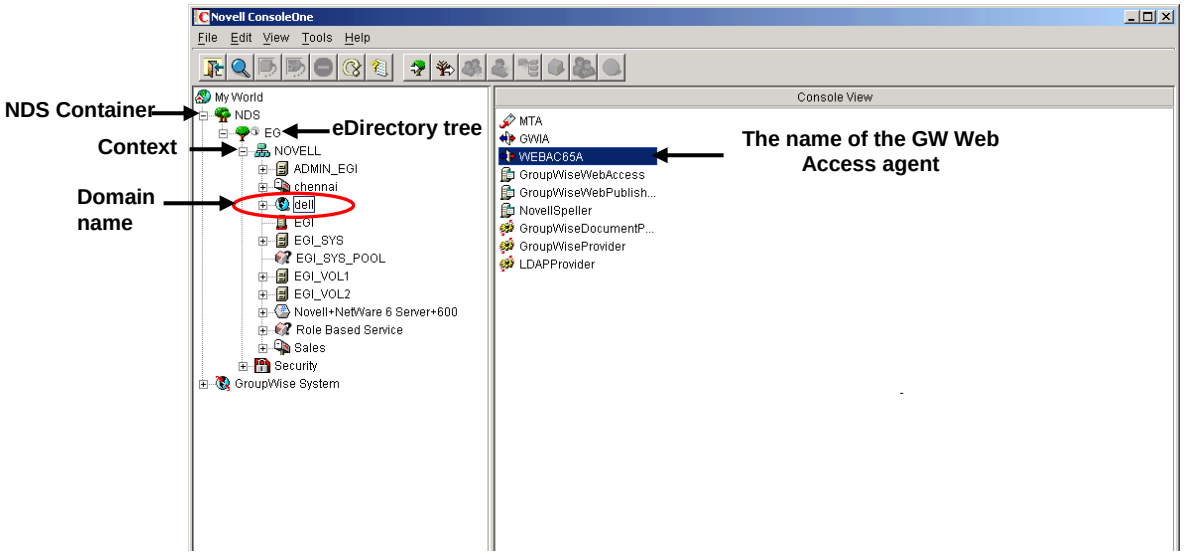

Figure 5.3: The Novell ConsoleOne window

3. The complete list of objects within the selected context will then be available to you. The objects in the list that are prefixed by the symbol represent the domains within the context (see Figure 5.3). Now, click on the domain that hosts the GwWeb application to be monitored. The name of this domain will become the *<domainname>.* Upon clicking the domain, the applications that exist within will appear in the right pane (see Figure 5.3). From this right pane, select the GwWeb application to be monitored. The name of this application will become the *<webagentname>*. In Figure 5.3, "WEBAC65A" is the agent name, and "dell" is the domain name. Therefore, the **webagentname** should be specified as "WEBAC65A.dell".

Chapter 6

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 **Novell Groupwise Components**. 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.