Monitoring GroupWise MTA

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

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. This is where eG Enterprise lends helping hands to administrators to continuously track performance of the MTA.

Chapter 2: How to Monitor GroupWise MTA Using eG Enterprise?

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

Once you SNMP-enable the components and feed the eG Enterprise system with the SNMP port and community string, the eG agent can easily contact the SNMP-MIB of GroupWise to extract the measures of interest.

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

- Managing the GroupWise MTA Application
- Configuring the tests

These steps have been discussed in following sections.

2.1 Managing the GroupWise MTA Application

The eG Enterprise cannot automatically discover the GroupWise MTA. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a GroupWise MTA component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *GroupWise MTA - Netware* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

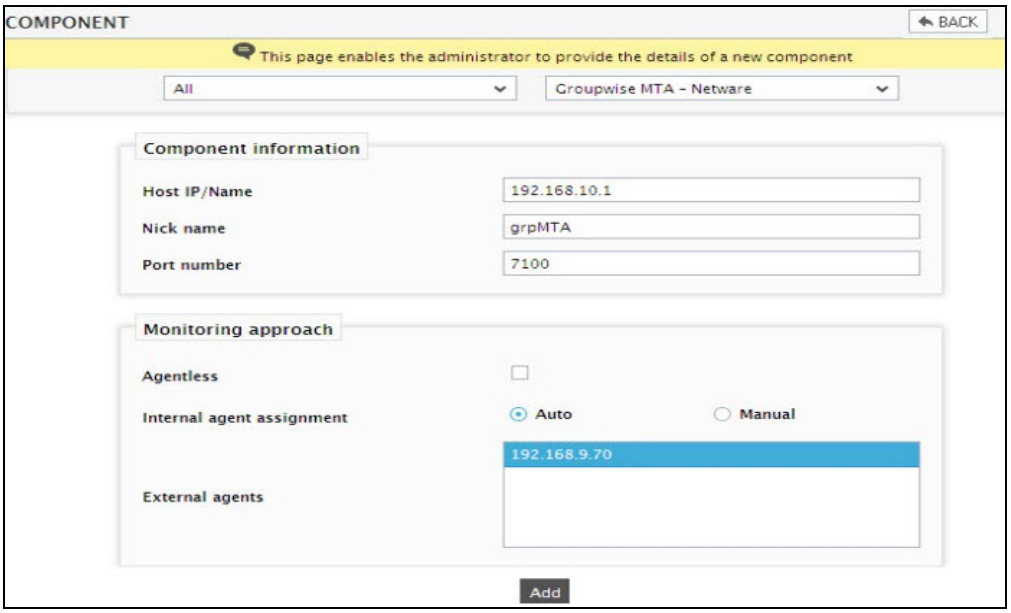

Figure 2.1: Adding the GroupWise MTA

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

2.2 Configuring the tests

1. When you attempt to sign out of eG administrative interface, a list of unconfigured tests will appear as shown in Figure 2.2. This list reveals the unconfigured tests requiring manual configuration.

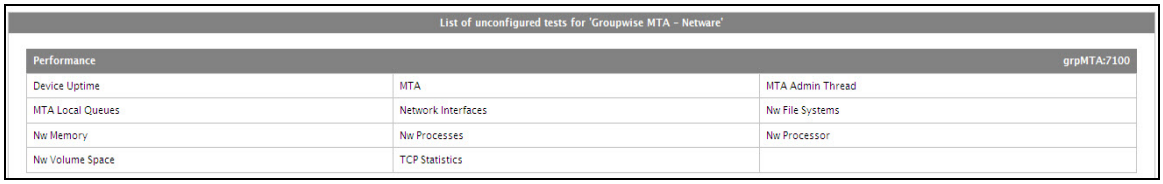

Figure 2.2: List of tests to be configured for the GroupWise MTA

2. Click on the test name to configure. To know how to configure the tests, refer to **Monitoring the GroupWise MTAs**.
3. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the GroupWise MTAs

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.

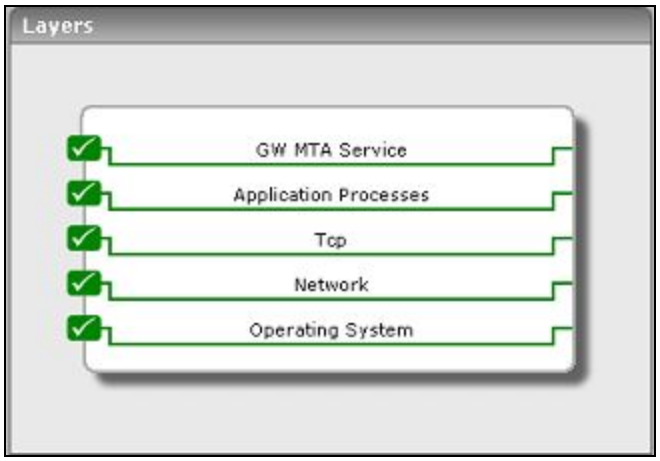

Figure 3.1: The layer model of a GroupWise MTA application

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 *Monitoring Netware* document.

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

This test 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

Outputs of the test : One set of results for the GWMTA port specified.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the server listens.
TargetPorts	The port number of the MTA component to be monitored. By default, the value in the Port text box will be displayed here.

Measurements made by the test

Measurement	Description	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).

Target of the test : A GWMTA application

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every domain specified.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the server listens.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This

Parameter	Description
	parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following

Parameter	Description
	encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
MTADomainName	The name of the domain on which the MTA has been installed. Refer to Section **3.1.4.1** to know how to find out the domain name of MTA.

Measurements made by the test

Measurement	Description	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.

Measurement	Description	Measurement Unit	Interpretation
			• **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.
Total gateways	Indicates the number of gateways serviced by this MTA.	Number	
Closed gateways	Indicates the number of closed gateways serviced by this MTA.	Number	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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>improperly configured, then configure it correctly.
• Gateway crash: In this case, revive the POA by restarting it.</td></tr>
<tr><td>Messages transferred</td><td>Indicates the number of messages routed by this MTA during the last measurement period.</td><td>Msgs/Sec</td><td>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>Undeliverable messages</td><td>Indicates the number of messages that were not delivered by this MTA during the last measurement period.</td><td>Number</td><td>
<table>
<tr><th>Possible Cause</th><th>Action</th></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</td><td>Verify the existence of the user in the post office before the sender tries to send the message again.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Possible Cause</th><th>Action</th></tr>
<tr><td>actually created in the post office.</td><td></td></tr>
<tr><td>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.</td><td>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.</td></tr>
</table>
</td></tr>
<tr><td>Error messages</td><td>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.</td><td>Msgs/Sec</td><td>Check the messages and attached files for damage.</td></tr>
<tr><td>Domain available disk space</td><td>Indicates the free space available in the volume in which the domain resides.</td><td>MB</td><td>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.</td></tr>
</table>

3.1.3 MTA Admin Thread Test

This test 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

Outputs of the test : One set of results for every MTA application.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the server listens.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the

Parameter	Description
	Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
MTADomainName	The name of the domain on which the MTA has been installed. Refer to Section **3.1.4.1** to know how to find out the domain name of MTA.

Measurements made by the test

Measurement	Description	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.

Measurement	Description	Measurement Unit	Interpretation
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 MTA Local Queues Test

This test 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

Outputs of the test : One set of results for every domain specified.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the server listens.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB

Parameter	Description
	using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.

Parameter	Description
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
MTADomainName	The name of the domain on which the MTA has been installed. Refer to Section **3.1.4.1** to know how to find out the domain name of MTA.

Measurements made by the test

Measurement	Description	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	Number	If the value is high, check for closed domains.

Measurement	Description	Measurement Unit	Interpretation
	messages will be available in the "domainx" directory, which is the holding directory for other 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.

3.1.4.1 Determining Domain Name of MTA

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.

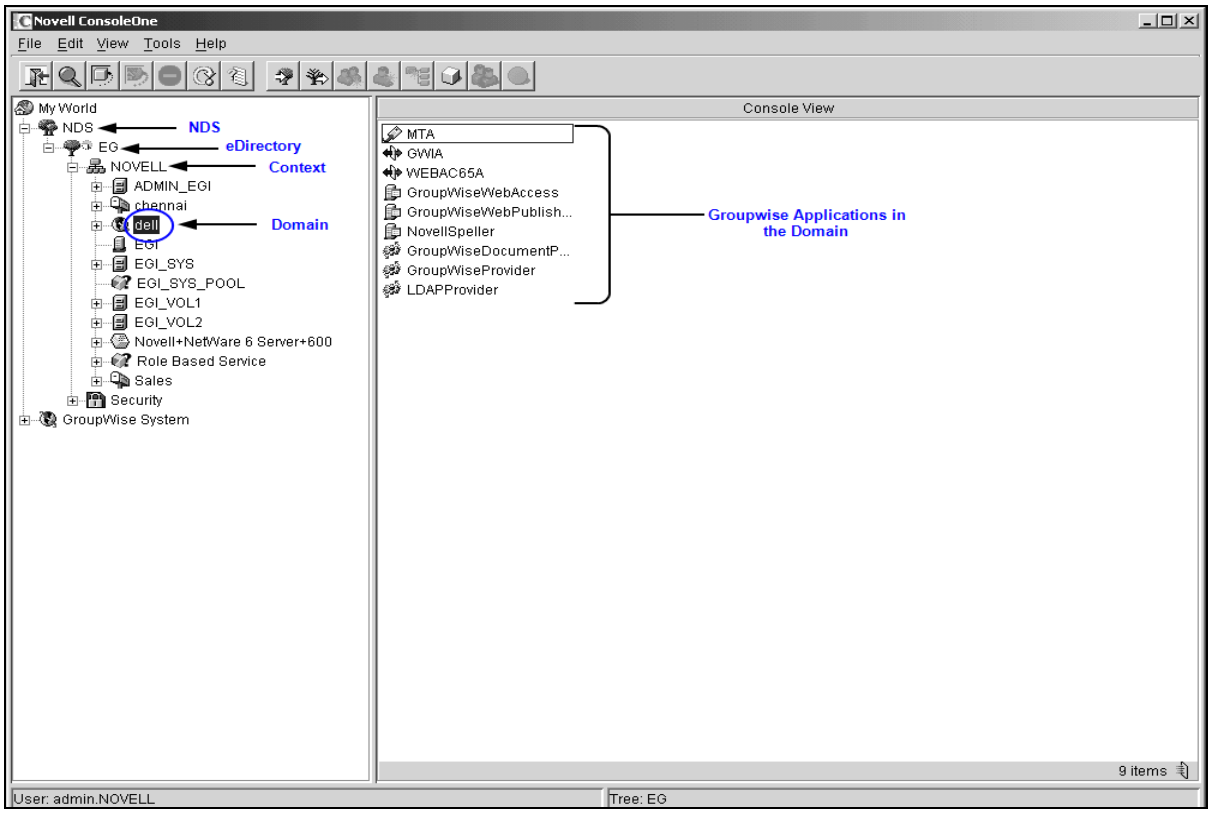

Figure 3.3: The Novell ConsoleOne window

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).

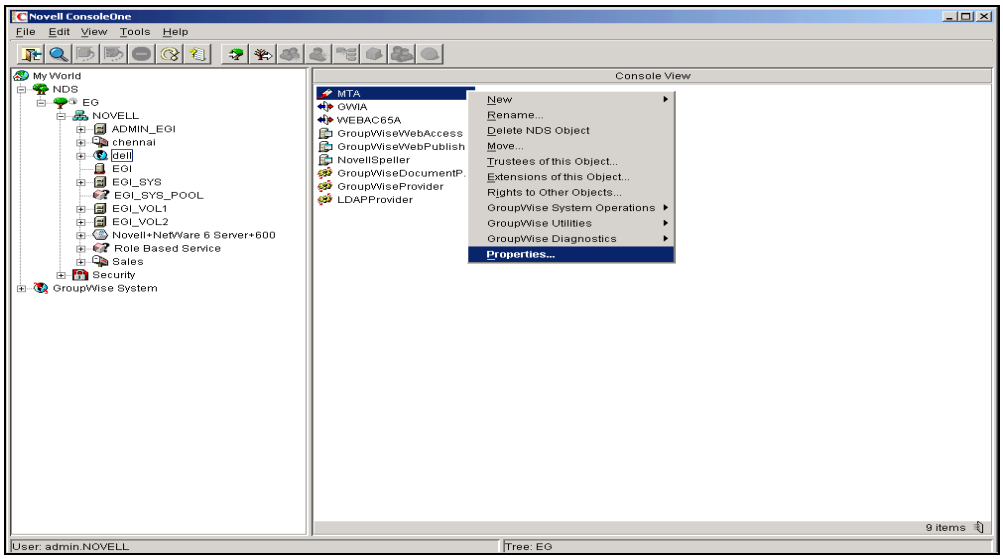

Figure 3.4: Selecting the Properties option from the MTA application's right-click menu

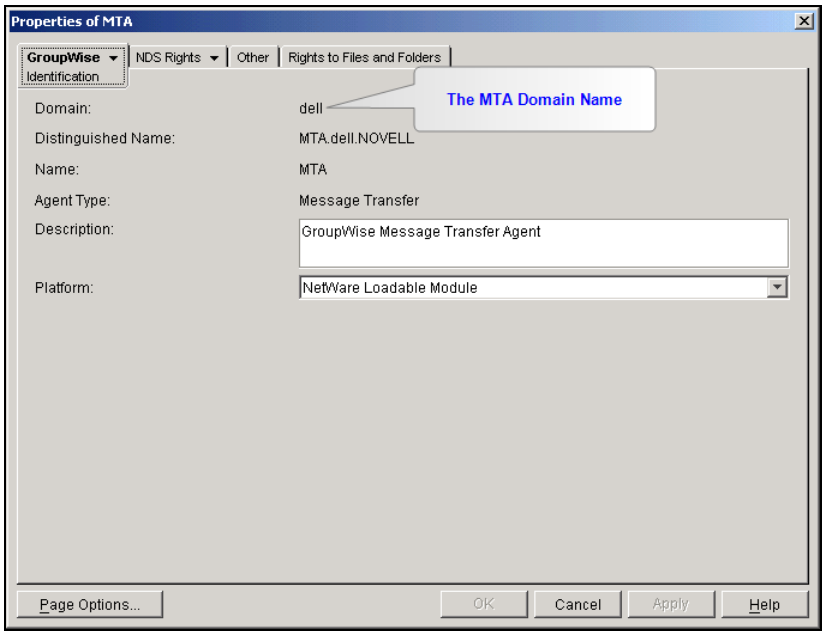

Figure 3.5: Viewing the MTA domain name

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.