Monitoring GroupWise Post Office Agents (POA)

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

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. This can be achieved using eG Enterprise that offers a specialized monitoring model to continuously monitor the POA.

Chapter 2: How to Monitor GroupWise Post Office Agents (POA) Using eG Enterprise?

eG Enterprise monitors the GroupWise Post Office Agents (POA) 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 POA via SNMP. Before attempting to monitor the GroupWise POA, 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 POA to extract the measures of interest. What more, these monitoring models do not even require an agent to be installed on the monitored system. If a target server/device supports the HOST-RESOURCES MIB, then eG Enterprise can provide in-depth insights into the performance of those targets in a non-intrusive, agentless manner. For more details related to agentless monitoring, refer to the *Administering eG Enterprise* document.

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

- Managing the GroupWise POA Application
- Configuring the tests

These steps have been discussed in following sections.

2.1 Managing the GroupWise POA Application

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

1. Log into the eG administrative interface.
2. If a GWIA POA is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page.
3. However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or add the component manually using the **COMPONENTS**page (Infrastructure -> Components -> Add/Modify). Remember that components manually added are

managed automatically. Figure 2.1 clearly illustrates the process of adding a Groupwise Post Office - Netware component.

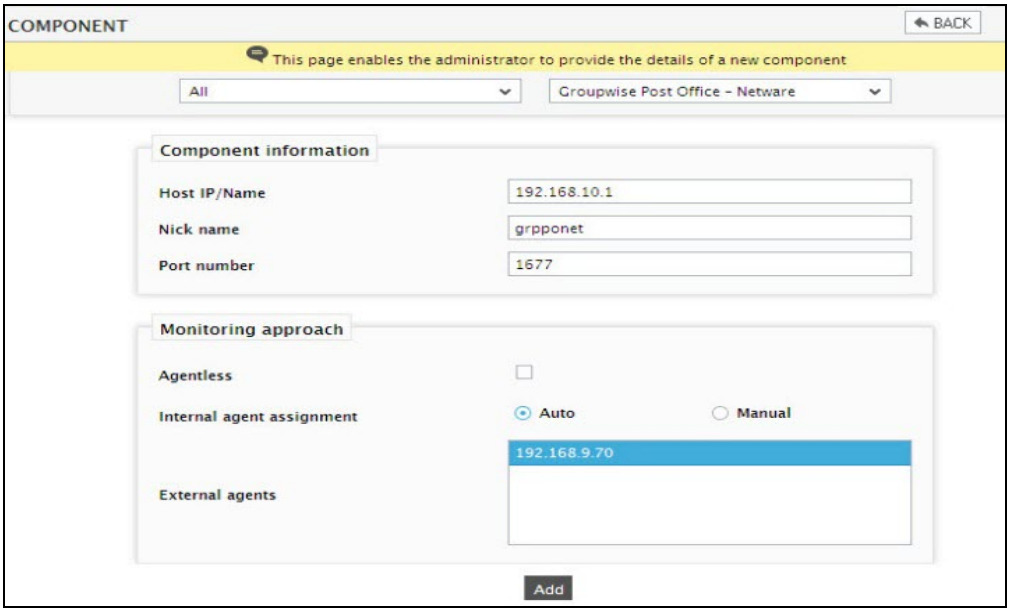

Figure 2.1: Adding a new Groupwise Post Office Application

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

2.2 Configuring the tests

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

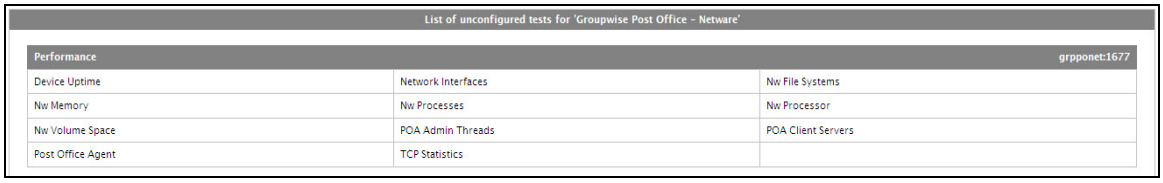

Figure 2.2: The list of Unconfigured tests that need to be configured for the Groupwise Post Office Application

2. Upon doing so, a **LIST OF UNCONFIGURED TESTS** listing the tests requiring manual configuration, will appear. Click on the test names to configure. To know how to configure the tests, refer to **Monitoring the GroupWise Post Office Agents (POA)** chapter.

3. Then, try to sign out one more time. This time again, the list of unconfigured tests will appear. Click on the **Network Interfaces** test to configure it. To know the details on configuring this test, refer to the *Monitoring Cisco Routers* document.
4. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the GroupWise Post Office Agents (POA)

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 3.1 depicts the Groupwise Post Office - Netware monitoring model.

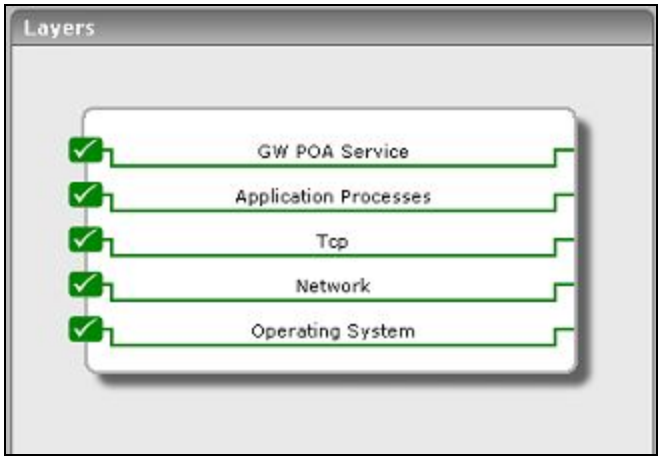

Figure 3.1: Layer model of a GWPOA

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 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 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

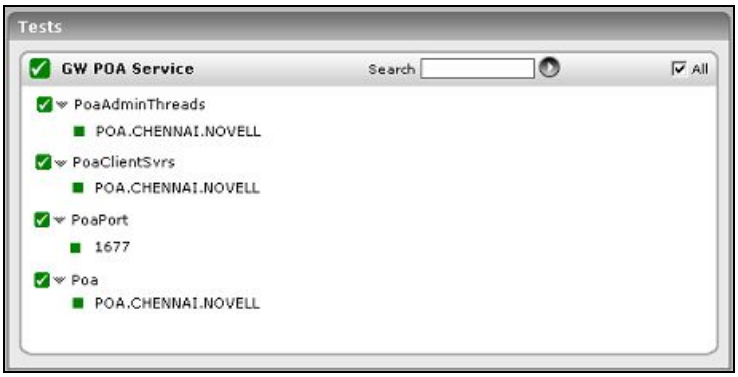

Figure 3.2: The tests associated with the GW POA Service layer

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

3.1.1 POA Ports Test

The PoaPort test 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

Outputs of the test : One set of results for the GWPOA 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 POA 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 Post Office Agent Test

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

Target of the test : A GWPOA application

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the distinguished name 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**.
POAName	The distinguished name of the POA. To know how to find out the name of POA, refer to Section **3.1.4.1**.

Measurements made by the test

Measurement	Description	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

Measurement	Description	Measurement Unit	Interpretation
			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.

Measurement	Description	Measurement Unit	Interpretation
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.

3.1.3 POA Client Servers Test

This test 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

Outputs of the test : One set of results for the distinguished name 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.

Parameter	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **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

Parameter	Description
	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**.
POAName	The distinguished name of the POA. To know how to find out the name of POA, refer to Section **3.1.4.1**.

Measurements made by the test

Measurement	Description	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:	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

Measurement	Description	Measurement Unit	Interpretation
	(Current measure – Previous measure)		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	

3.1.4 POA Admin Threads Test

This test 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

Outputs of the test : One set of results for the distinguished name 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.

Parameter	Description
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **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

Parameter	Description
	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**.
POAName	The distinguished name of the POA. To know how to find out the name of POA, refer to Section **3.1.4.1**.

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 POA.
Message processing rate	Indicates the rate at which admin messages were	Msgs/Sec	A high value may be indicative of an excessive load on the admin thread.

Measurement	Description	Measurement Unit	Interpretation
	processed by this MTA during the last measurement period.		
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.

3.1.4.1 Determining Name of a POA

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 3.3). 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.

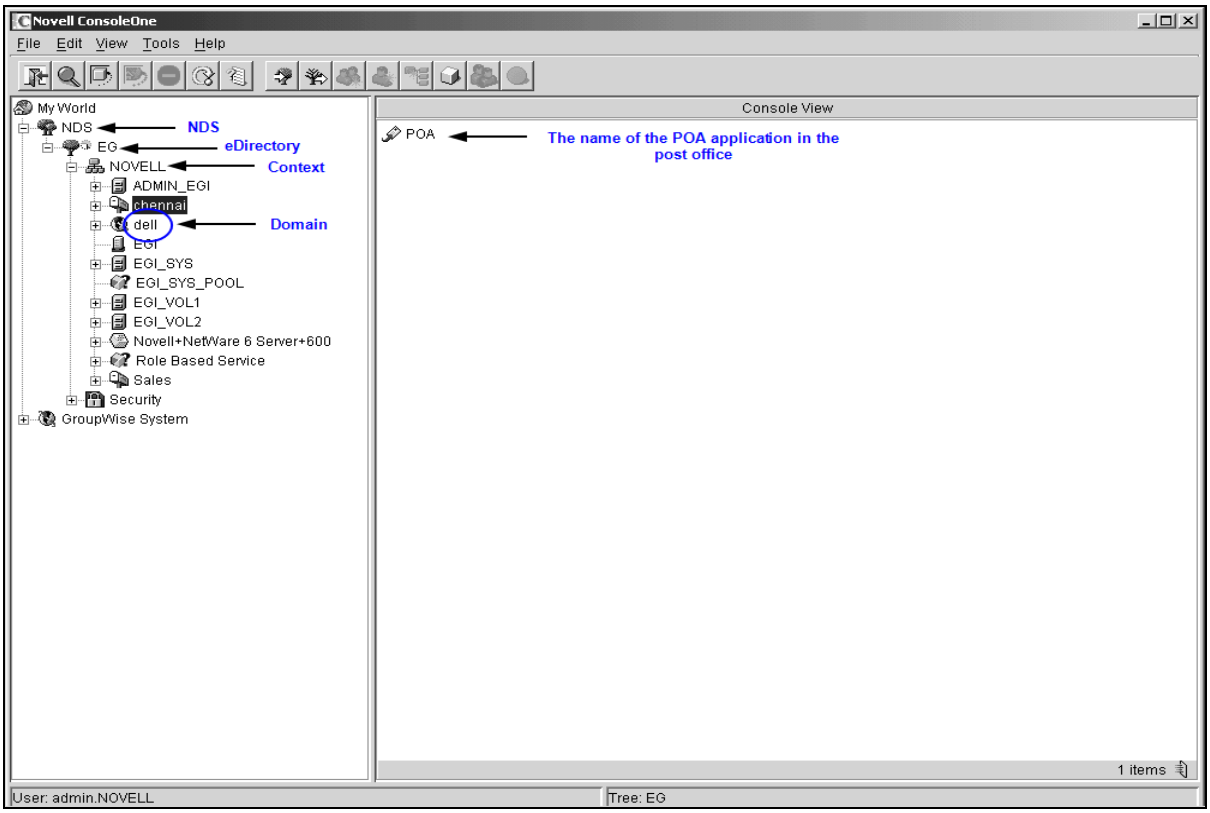

Figure 3.3: The Novell ConsoleOne window

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 post offices within the context (see Figure 3.3). 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 3.3).
4. From the right pane, select the POA 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 distinguished name of the POA application (see Figure 3.5). 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 3.5 will be: *POA.chennai.NOVELL*.

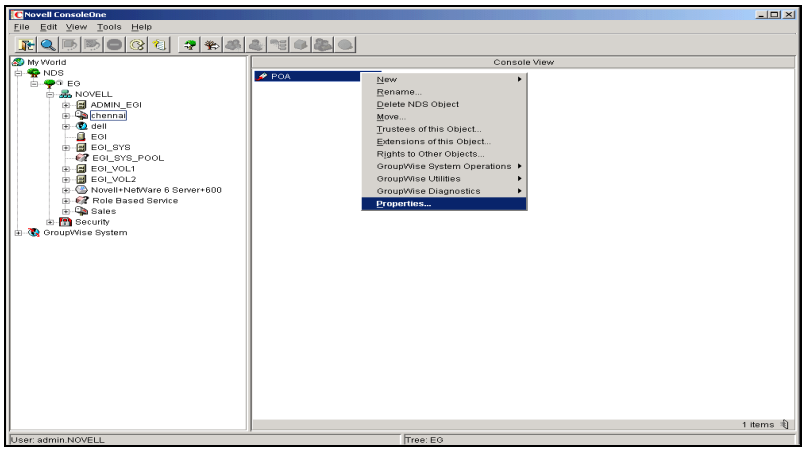

Figure 3.4: Selecting the Properties option from the POA application's right-click menu

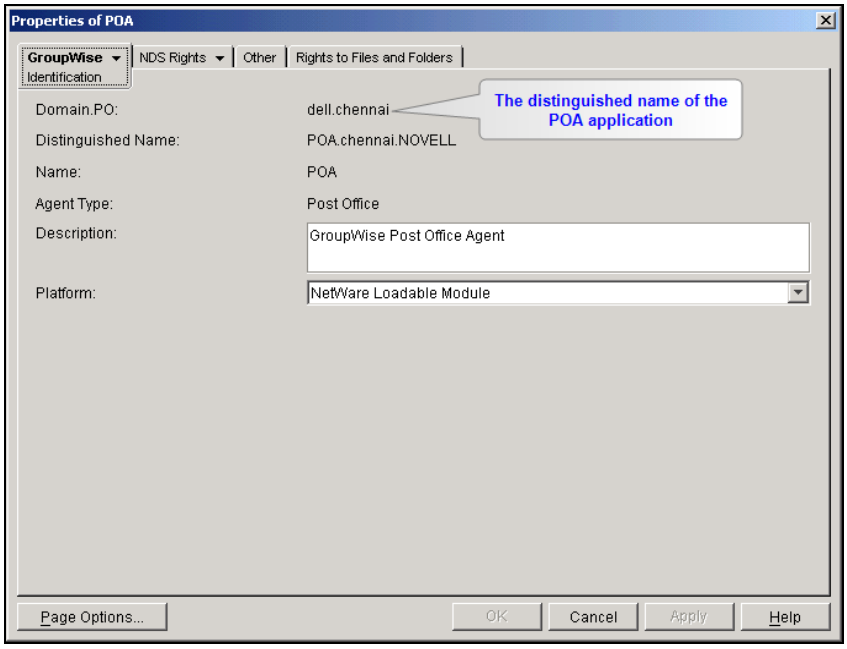

Figure 3.5: Viewing the distinguished name of the POA application

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.