Monitoring GroupWise WebAccess Agent Application

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

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. This can be achieved using a specialized monitoring model offered by eG Enterprise.

Chapter 2: How to Monitor GroupWise WebAccess Agent Application Using eG Enterprise?

eG Enterprise monitors the GroupWise WebAccess Agent application 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 WebAccess, 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 WebAccess Agent Application
- Configuring the tests

These steps have been discussed in following sections.

2.1 Managing the GroupWise WebAccess Agent Application

eG Enterprise can automatically discover the GroupWise WebAccess Agent application in the environment and also lets you to add the GroupWise WebAccess Agent component if the application is not auto-discovered. The following steps explain you how to manually add the GroupWise WebAccess Agent component using the eG administrative interface.

1. Log into the eG administrative interface.
2. If a GroupWise WebAccess Agent application 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. 2.1 clearly illustrates the process of adding a GroupWise WebAccess Agent application.

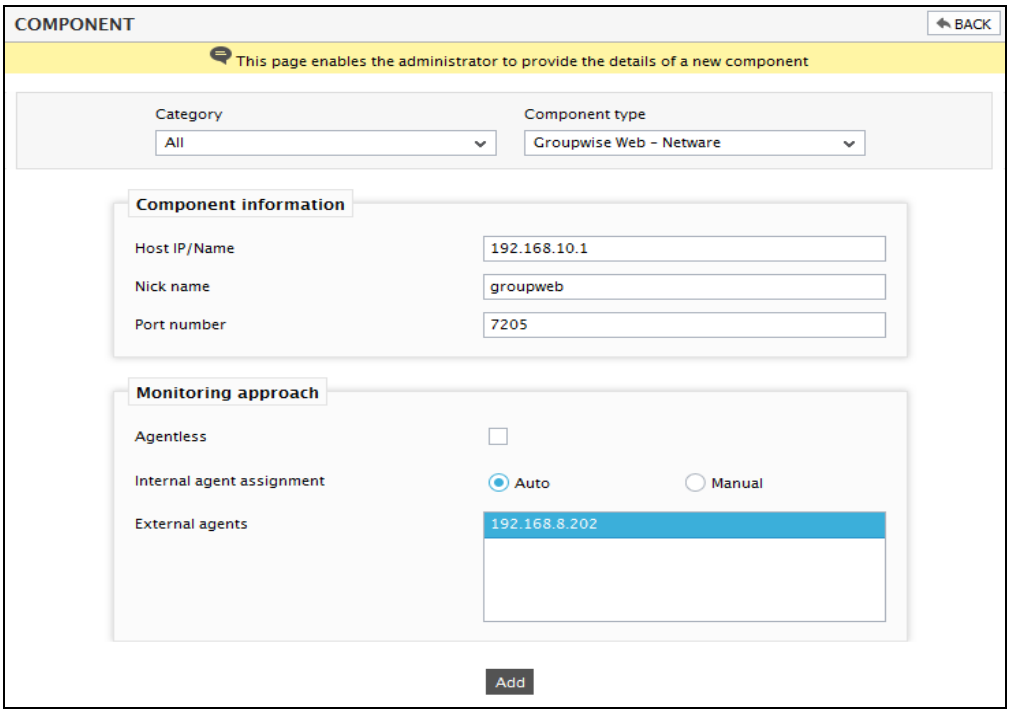

Figure 2.1: Adding a new GroupWise WebAccess Agent application

4. Specify the **Host IP**, the **Nick name** and **Port Number** for the GroupWise WebAccess Agent Application 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.

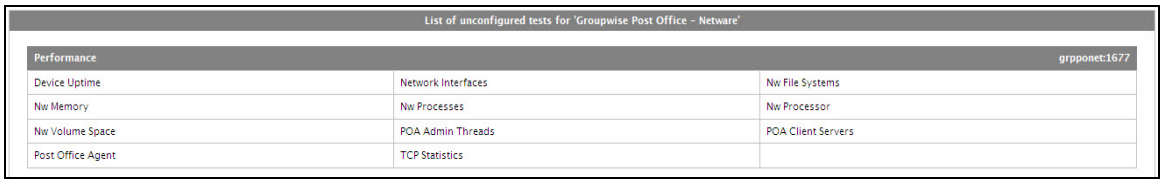

Figure 2.2: The list of tests that need to be manually configured for the Groupwise Post Office Application

2. Click on the test name to configure. To know how to configure the tests, refer to **Monitoring GroupWise WebAccess (GwWeb)**.

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. Refer to *Monitoring Cisco Routers* document to know how to configure this test.
4. Once all the tests are configured, sign out of the eG administrative interface.

Chapter 3: Monitoring GroupWise WebAccess (GwWeb)

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 3.1 depicts the Netware GwWeb monitoring model.

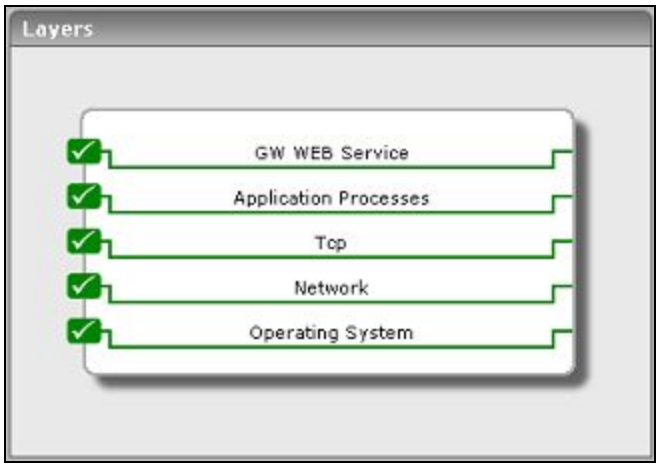

Figure 3.1: Layer model of a GWWeb

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 3.1. To know the details of tests mapped to these 4 layers on Windows environments, refer to *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 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 3.2: The tests associated with the GW WEB Service layer

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

3.1.1 Groupwise Web Agent Port Test

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

Target of the test : A GwWeb application

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the 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	Percent	An availability problem can be caused by different factors – e.g., the server

Measurement	Description	Measurement Unit	Interpretation
	not.		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 Groupwise Web Agent Test

This test 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

Outputs of the test : One set of results for the 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 is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.

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

Parameter	Description
	• **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
WebAgentName	The distinguished name of the WebAccess agent. Refer to Section **3.1.2.1** to know how to find it.

Measurements made by the test

Measurement	Description	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	

3.1.2.1 Determining Distinguished Name of Web Agent

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 3.3). 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 3.3).

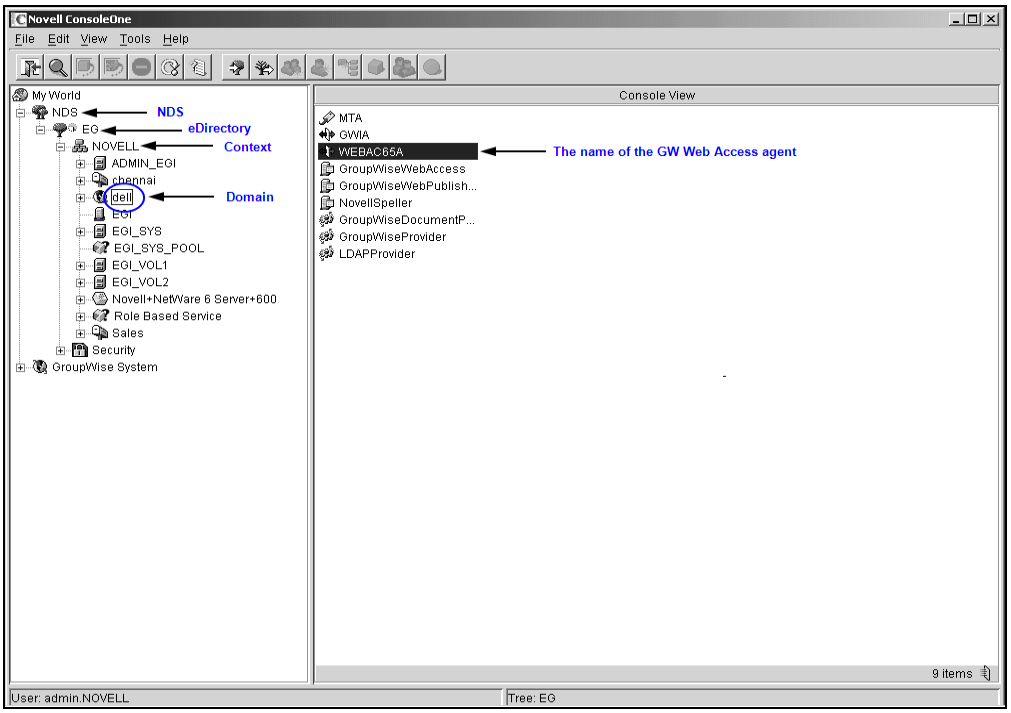

Figure 3.3: The Novell ConsoleOne window

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 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 3.3). From this right pane, select the GwWeb application to be monitored. The name of this application will become the <*webagentname*>. In

Figure 3.3, "WEBAC65A" is the agent name, and "dell" is the domain name. Therefore, the webagentname should be specified as “WEBAC65A.dell”.

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.

Copyright © 2018 eG Innovations Inc. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations 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. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.