Integrating eG Enterprise with Third-party SNMP Management Systems

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 2008, Windows 2012, Windows 2016, Windows 7, Windows 8 and Windows 10 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

Some environments may already be using network-monitoring systems such as HP OpenView, Tivoli NetView, etc., for monitoring their networks and systems. Administrators of such environments may desire that eG Enterprise's alarms be reported to their existing alarm consoles. By configuring the eG manager to send eG alarms as SNMP traps to one/more SNMP management consoles in an environment, you can enable eG Enterprise to support the integrated display and tracking of alarms from a single monitoring console.

The broad steps towards this integration are as follows:

1. Configure the SNMP managers/trap receivers to which the eG manager needs to send SNMP traps
2. Define the SNMP trap settings
3. Configure the third-party SNMP managers to receive SNMP traps from the eG manager.

Each of these steps have been discussed in detail below.

1.1 Configuring the SNMP Managers/Trap Receivers

To configure the SNMP managers/trap receivers to which the eG manager needs to send SNMP traps, do the following:

1. Login to the eG administrative interface as *admin*.
2. Select the **Receivers and Settings** option from the **SNMP Traps** menu in the **Alerts** tile. Figure 1.1 then appears.

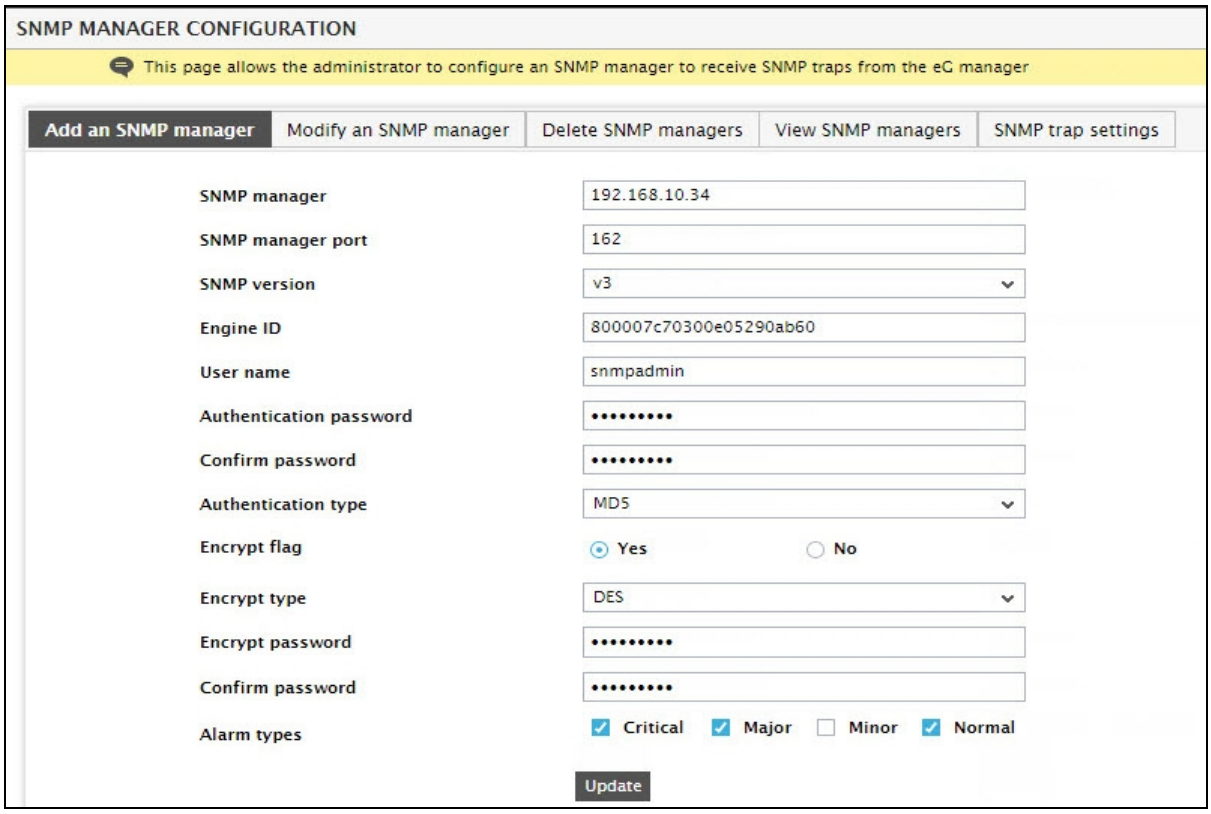

Figure 1.1: Adding an SNMP Trap Receiver

3. The IP address of the SNMP manager on which the SNMP manager application is executing has to be provided in the **SNMP manager** text box in Figure 1.1. The port number on which the SNMP manager is listening for traps from the eG manager is to be specified in the **SNMP manager port** field. The default port is *162*.

4. By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMP** version 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.

5. The **SNMP community** field appears only if the **SNMP version** chosen is **1** or **2**. Here, specify the community string that is used by an eG manager to report alarm information via SNMP to an SNMP manager.

6. If the **SNMP version** is **3**, then you will have to specify the following parameters (see Figure 1.1):

   - **Engine ID**: Specify the engine ID of the trap sender. This should be in hexadecimal - i.e., should begin with "0x".

- **User name**: As SNMPv3 traps require authentication, specify a valid user name here.
- **Authentication password**: Enter the password of the above-mentioned **User name**.
- **Confirm password**: Confirm the **Authentication Password** by retyping it here.
- **Authentication type**: Choose the authentication algorithm using which SNMP v3 converts the specified **User name** and **Authentication 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
- **Encrypt flag**: By default, the eG manager does not encrypt SNMP traps. Accordingly, this parameter is set to **No** by default. To ensure that SNMP traps sent by the eG manager are encrypted, select the **Yes** option.
- **Encrypt type**: If the **Encrypt flag** is set to **Yes**, then you will have to mention the encryption type by selecting an option from the **Encrypt type** list. SNMP v3 supports the following encryption types:
  - **DES** - Data Encryption Standard
  - **AES** - Advanced Encryption Standard
- **Encrypt password**: Specify the encryption password here.
- **Confirm password**: Confirm the encryption password by retyping the password here.

7. Select the required check boxes against **Alarm types** to indicate which alarm priorities need to be sent out as SNMP traps to the third-party SNMP management console.
8. Next, select one or more of the check boxes from the **Alarm types** section, to indicate your preference in terms of the priority of problems for which you wish to receive alerts via the SNMP manager console. For instance, if you choose **Critical**, you would receive critical priority alarms alone and not the other types. Normal alerts are generated by the eG system as and when a problem is corrected.
9. Finally, click the **Update** button to add the new trap receiver.
10. This way, multiple trap receivers can be added.

1.2 Configuring the SNMP Trap Settings

To do this, follow the steps detailed below:

1. Login to the eG administrative interface as **admin**.
2. Select the **Receivers and Settings** option from the **SNMP Traps** menu in the **Alerts** tile. When Figure 1.1 appears, click the **SNMP trap settings** tab page therein. Figure 1.2 will then appear.

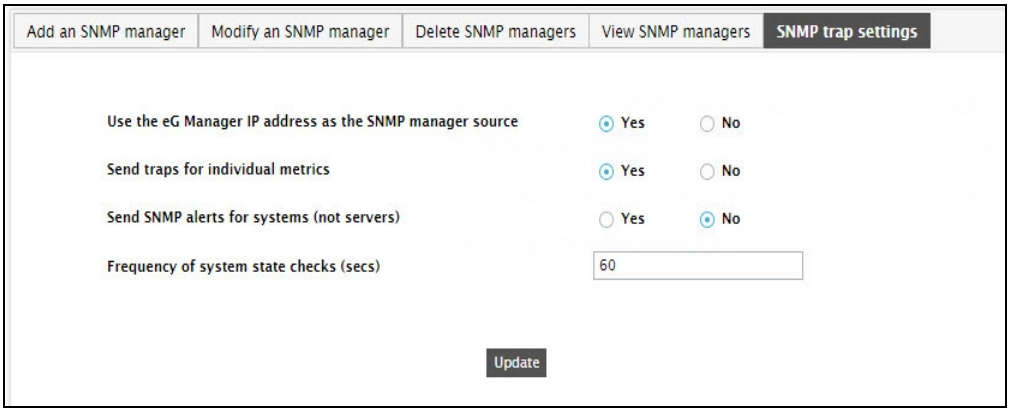

Figure 1.2: Configuring SNMP Trap Settings

3. To ensure that the SNMP trap's source field includes the IP address of the eG manager from which the traps originated, set the **Use the manager's IP address (not name) in the SNMP trap's source field** flag to **Yes**. Setting this flag to **No** will include the host name of the eG manager in the source field.
4. Set the **Send traps for components** flag to **Yes**, if you want the eG manager to send out SNMP traps whenever:
   - A new alarm is raised on a component
   - An existing alarm related to a component changes - an alarm change can be a change in the alarm priority, a change in the alarm description (eg., an addition/removal of a descriptor from an alarm), or change in the list of impacted services

   If you set the **Send traps for components** flag to **No**, then the test will not send out SNMP traps for problems detected in components. By default, this flag is set to **Yes**.
5. If multiple applications operate on a single host - i.e., if multiple components are managed using the same nick name - then, you can set the **Send SNMP traps for systems (not servers)** flag to **Yes**, so that the eG manager generates an SNMP trap for only the very first alarm that is raised on that nick name. In this case therefore, subsequent alarms for the same nick name will not be considered for trap generation. To turn off this capability, set the **Send SNMP traps for systems (not servers)** flag to **No**.

   Note:

- If both the **Send traps for components** and **Send traps for systems** flags are set to **Yes**, then only the **Send traps for components** flag setting will take effect.
- If both the **Send traps for components** and **Send traps for systems** flag are set to **No**, then the eG manager will not send out any SNMP traps for any alarm it generates.

6. Indicate the frequency (in seconds) with which the eG manager needs to check the state of a host for SNMP trap generation, in the **Frequency of system state checks (secs)** text box. The default is 60 seconds (i.e., 1 minute).
7. Finally, click the **Update** button to enable the transmission of SNMP traps.

1.3 Configuring the Third-Party SNMP Trap Receiver to Receive the SNMP Traps sent by the eG Manager

This procedure will differ from one SNMP manager to another. The sections below discuss the steps involved in integrating the HPOV NNM with the eG manager, and viewing the results of the integration in the HPOV NNM console.

1.3.1 Integrating with HP OpenView NNM v7.0

While integrating with HPOV NNM v 7.0 specifically, the following steps are necessary to ensure that NNM receives the SNMP traps sent by eG Enterprise:

1. Copy the file **eg_ov.conf** from the eG manager directory (for e.g., /opt/egurkha/manager/config on Unix or <EG_HOME_DIR>\egurkha\manager\config on Windows environments) to the OpenView system.
2. On the OpenView system, run the command:

```
<OpenView_HOME_Dir>\NNM\bin\xnmevents -load <full path to eg_ov.conf>
```

Note:

When you run the above command, make sure that the **NNM Event Configuration** window (see Figure 1.4) is closed.

With that, the integration is complete. To verify whether the integration was successful or not, follow the steps below:

1. Using the *Options -> Event Configuration* menu items (see Figure 1.3) on the OpenView NNM Console, open the **NNM Event Configuration** window.

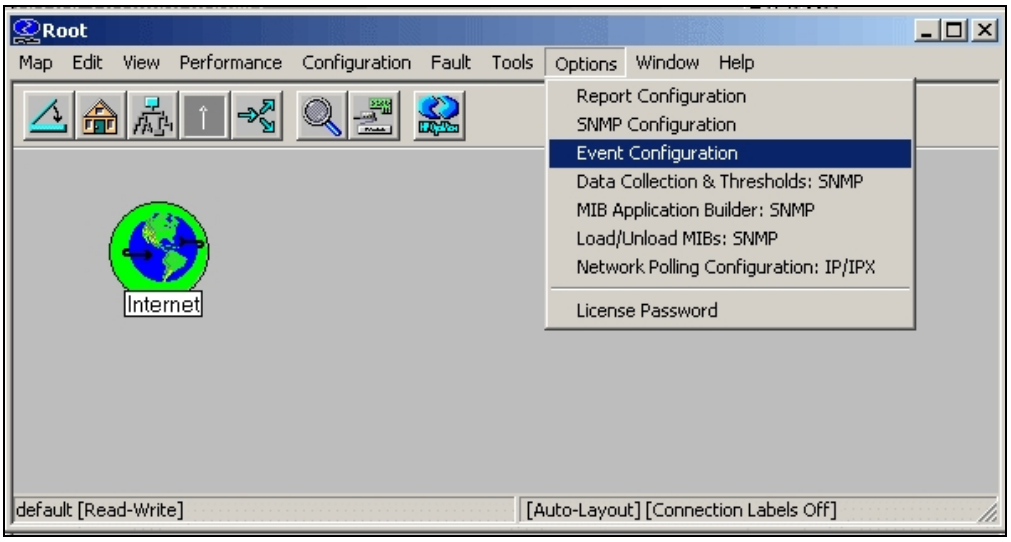

Figure 1.3: Opening the Event Configuration window

2. Under the **Enterprises** section, you should see a listing for **eG** (see Figure 1.4). Clicking on this listing, will display a list of eG events - since we had earlier configured the eG manager to send out SNMP traps for Critical, Major, Minor, and Normal events (see Figure 1.4), you will find an entry for each of these configured events (see Figure 1.4) in the events list. Also, note that the events list includes the following entries: *eGAgentNormal* and *eGAgentWarning*. These additional listings ensure that the SNMP console also displays alerts when an eG agent stops and starts later.

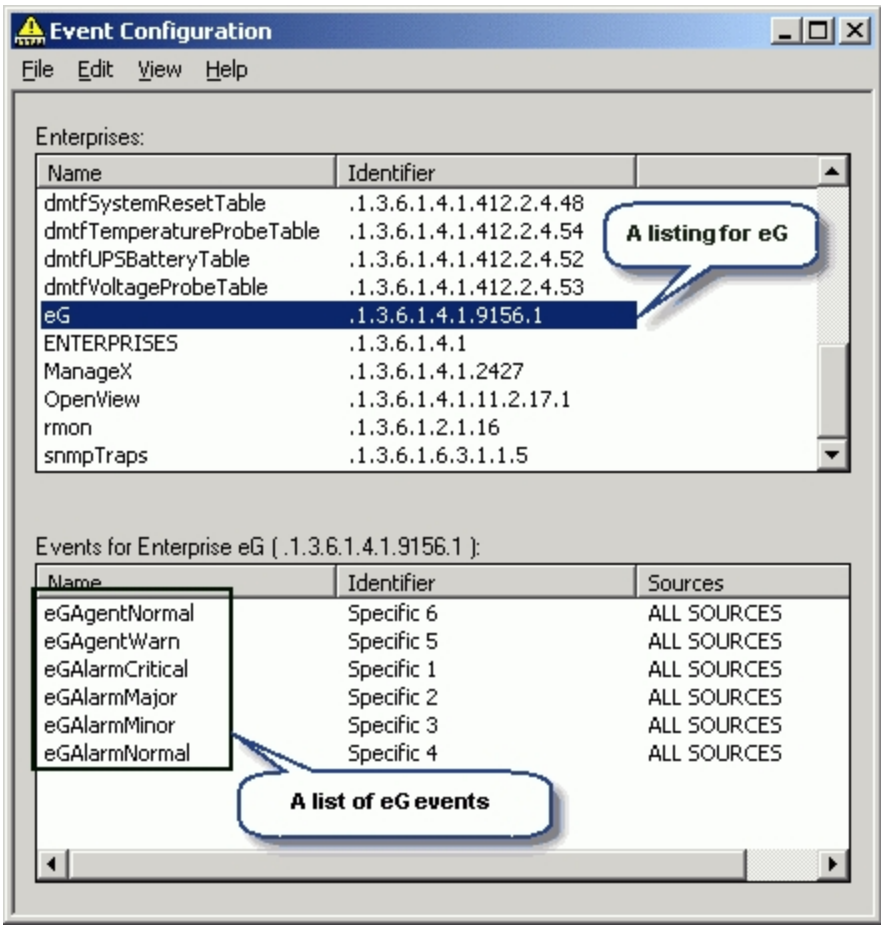

Figure 1.4: The Event Configuration window listing

3. The above process also adds a new category called **eG Alarms** in the OpenView NNM alarm categories list (see Figure 1.5 and Figure 1.6). All eG events are automatically associated with this category. Clicking on any of the events listed in Figure 1.4 will lead you to the **Modify Events** dialog box (see Figure 1.5). In the **Event Message** tab page of the dialog box, you should see the **eG Alarms** category in the list of categories that appears on selecting the **Log and display in category** option. You will also see the new category in the **Alarm Categories** window depicted by Figure 1.6.

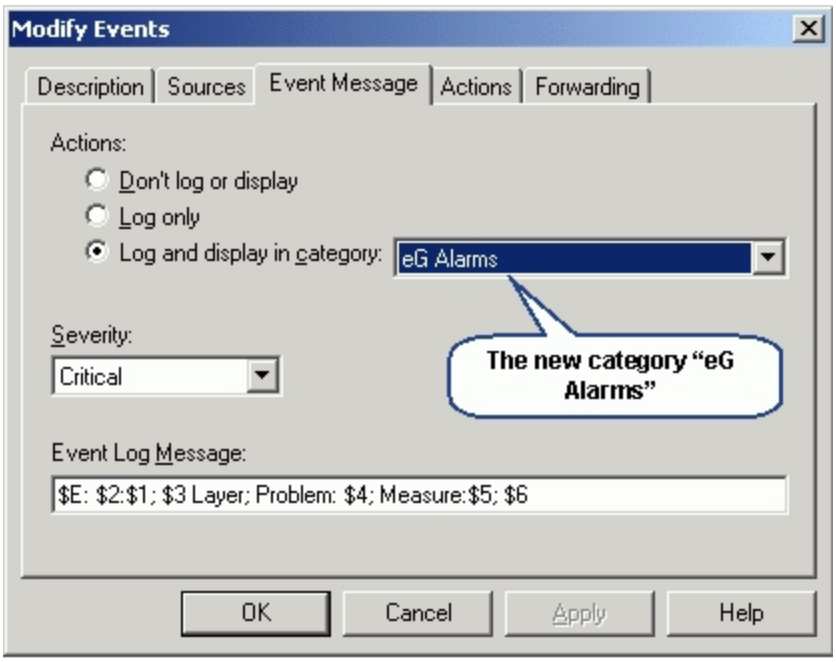

Figure 1.5: The Event Message tab page of the window displaying a new category called eG Alarms

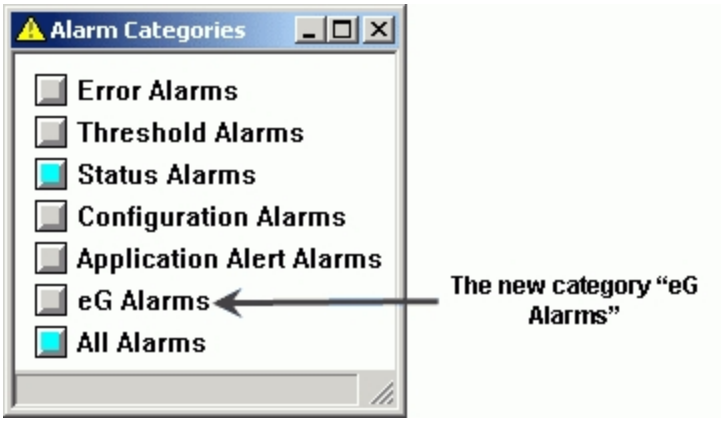

Figure 1.6: The Alarm Categories window displaying the eG Alarms category

4. Stop the OpenView NNM alarm manager and then, start it using the command **xnmevents**. The **Alarm Categories** window (as depicted by Figure 1.6 above) will come up. Clicking on the **eG Alarms** option in this window will open the **eG Alarms Browser**, which displays the details of alarms sent by the eG manager. If there are no issues in the environment currently, then the browser will display no alarms (see Figure 1.7).

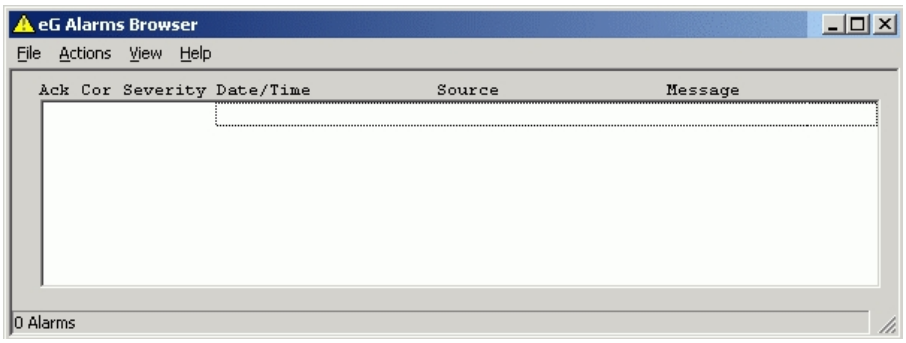

Figure 1.7: The eG Alarms browser displaying no alarms

5. Once the eG manager detects performance issues, it will generate and display alarms in the **Alarms** window of the eG monitoring console. The **Alarms** window depicted by Figure 1.8 and Figure 1.9, for example, indicates that the MS FTP server in the environment has crashed, thereby bringing down the FTP publishing service!

Figure 1.8: The Critical alarm indicating the MS FTP service has gone down

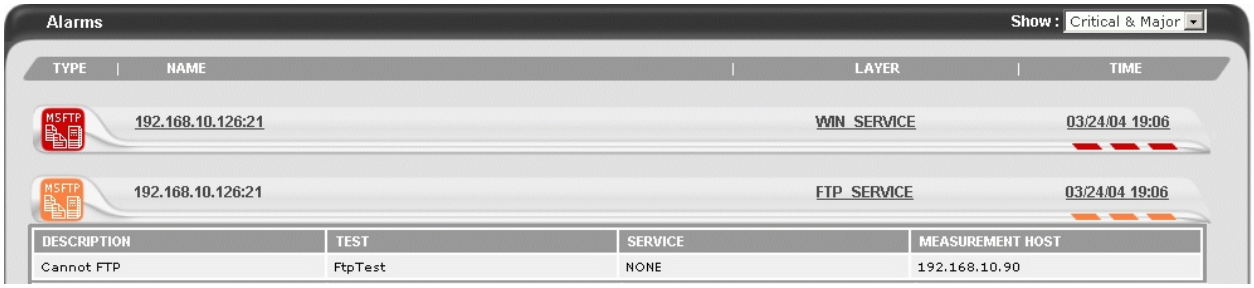

Figure 1.9: A Major alarm indicating that the agent is unable to FTP files

6. When the eG manager generates alarms, the color-coding of the **eG Alarms** category in the **Alarm Categories** window of the NNM console, will change to reflect the severity of the eG alarm. In Figure 1.10, for instance, the color-coding of the **eG Alarms** category has changed to **Red**, indicating the existence of one/more Critical issues.

Figure 1.10: The eG Alarms category indicating the existence of Critical alarms

7. Clicking on **eG Alarms** in Figure 1.10 will open Figure 1.11, where the details of the alerts raised by the eG manager will be displayed.

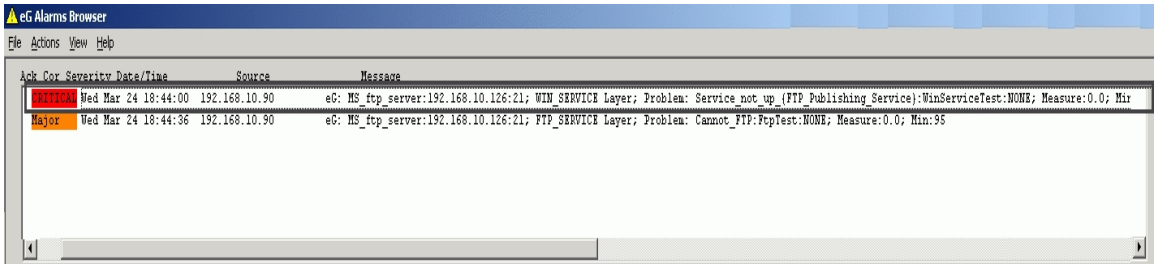

Figure 1.11: The eG Alarms Browser displaying the details of the alarms generated by the eG manager

8. To understand the contents of these alerts better, let us take a closer look at say, the first alert reported by 1.3.1.

Contents of the SNMP alert

The alarm severity	CRITICAL
The date/time of problem	Wed Mar 24 18:44:00
The IP address of the eG manager	192.168.10.90
The problem component-type	MS_ftp_server
The IP and TCP port of the problem component	192.168.10.126:21
The problem layer	WIN_SERVICE Layer
A brief description of the problem	Service_not_up (FTP_Publishing_ Service)

The problem test	WinServiceTest
The value of the measure	0.0
The threshold value that was violated	Not visible in the figure

9. If a problem is resolved, and the problem component is restored to its Normal state, the eG manager will send out **NORMAL** alerts to the SNMP management console. Accordingly, the color-coding of the **eG Alarms** category in the NNM console will change once again, indicating the return to normalcy (see Figure 1.12). Moreover, the **eG Alarms Browser** will display the details of the Normal alerts as well (see Figure 1.13.

Figure 1.12: The eG Alarms category in a Normal state

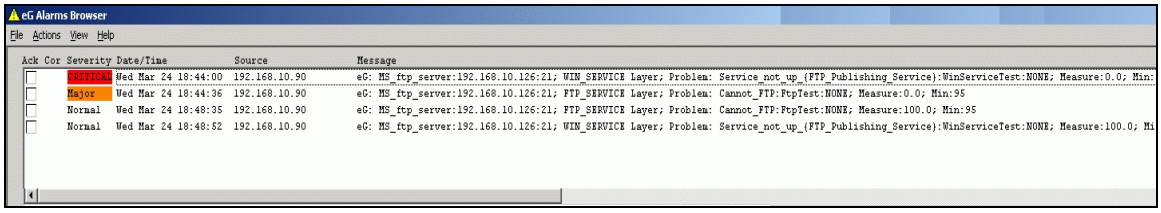

Figure 1.13: The eG Alarms Browser displaying Normal alerts

10. In addition to tracking changes in the state of eG-managed components, this integration also enables you to track changes in the state of eG agents deployed in an environment, from a single monitoring console. If an eG agent suddenly stops, and comes back up later, you will find equivalent alerts displayed in the **eG Alarms Browser** of the NNM console (see Figure 1.14). From Figure 1.14, it is evident that while a *Warning* event was raised for the eG agent failure, a *Normal* event was raised when the agent started running subsequently.

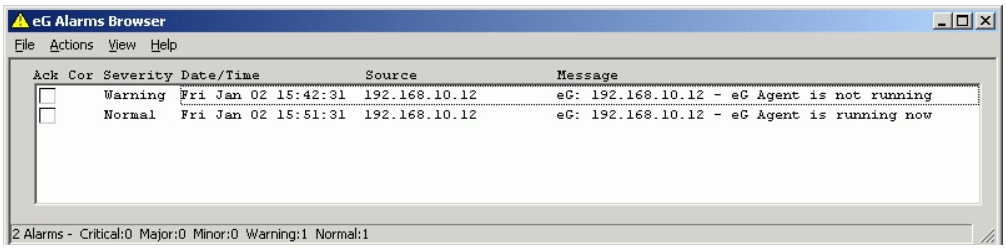

Figure 1.14: The eG Alarms browser indicating agent state changes

1.3.2 Integrating with HP OpenView NNM v9.10

Typically, HPOV NNM v9.10 blocks all SNMP traps. Naturally therefore, the first step towards integrating the eG manager with HPOV NNM v9.10 is to configure the NNM to receive and display the SNMP traps sent by the eG manager. For this, follow the steps given below:

1. Login to the NNM host and go to the command prompt.
2. At the command prompt, go to *c:\progra~2\HP\HP BTO Software\bin* and run the following command:

   nnmtrapconfig.ovpl -showProp

3. The output depicted by Figure 1.15 will then appear:

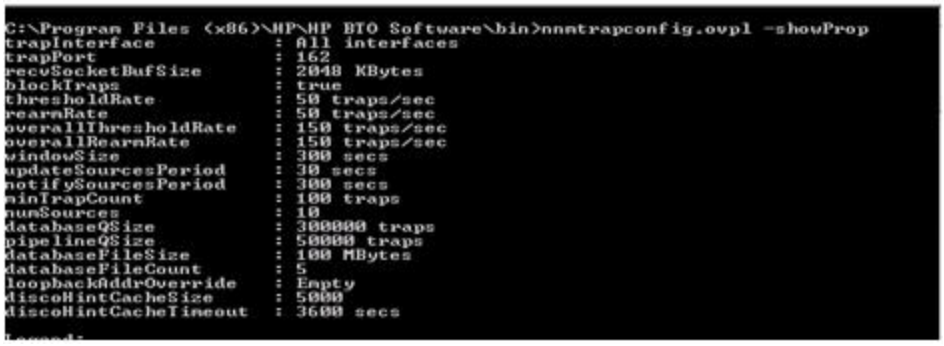

Figure 1.15: The output of the nnmtrapconfig.ovpl command

4. From Figure 1.15, it is evident that the **blockTraps** property of the NNM is set to **true**, indicating that the NNM will block all SNMP traps that are sent to it. To 'unblock' the traps, issue the following command at the prompt:

   nnmtrapconfig.ovpl -setProp -unblockTraps

5. This will result in the output shown by Figure 1.16 below.

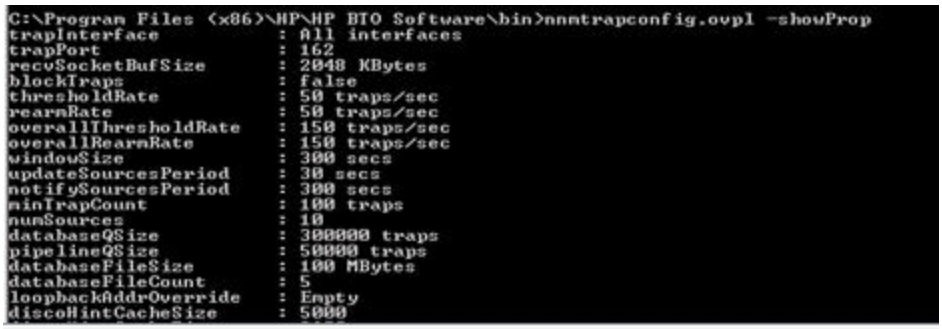

Figure 1.16: Unblocking SNMP traps

6. As you can see, the **blockTraps** property of the NNM is now set to **false**. Next, go to the NNM web console and follow the Configuration -> Incidents -> Incident Configuration node sequence. Figure 1.17 will then appear. Make sure that the **Discard Unresolved SNMP Traps** check box in Figure 1.17 is unchecked.

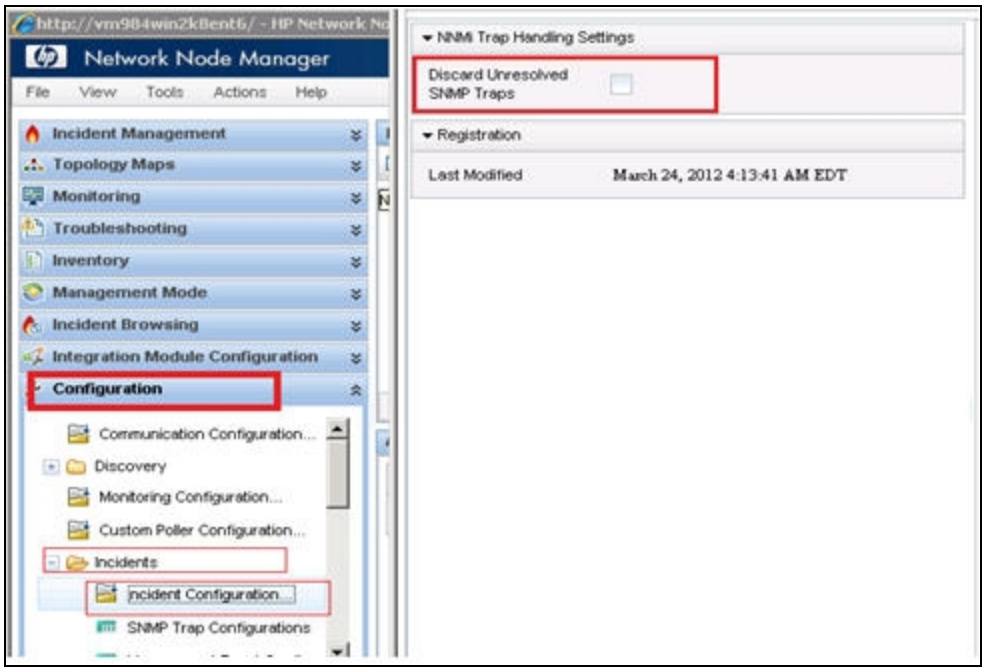

Figure 1.17: Deselecting the 'Discard Unresolved SNMP Traps' check box

7. Then, proceed to load the **egurkha.mib** into NNM, so that the NNM receives all traps sent by the eG manager. For this, run the following command at the prompt:

   c:\progra~2\HP\HP BTO Software\bin\nnmloadmib.ovpl <Full_ path_ to_ the_ eGMIB>\egurkha.mib

By default, the **egurkha.mib** will be available in the <EG_ MANAGER_ INSTALL_ DIR>\manager\config directory. In this case therefore, the command will be:

c:\progra~2\HP\HP BTO Software\bin\nnmloadmib.ovpl <EG_ INSTALL_ DIR>\manager\config\egurkha.mib

8. However, note that unblocking the SNMP traps and loading the **egurkha.mib** does not guarantee the free movement of eG traps into the NNM system; one/more OIDs may continue to be blocked by the NNM system. To lift such specific blocks, follow the steps discussed below:

   a. Run the following command at the prompt:

      c:\progra~2\HP\HP BTO Software\bin\nnmincidentcfg.ovpl -loadTraps EGURKHA-MIB

   b. Reset NNM's blocked OID cache using the following command:

      c:\progra~2\HP\HP BTO Software\bin\nnmtrapconfig.ovpl -resetBlockCache

9. Now, proceed to check whether the NNM system is able to receive eG alarms as traps. For this, switch to the *c:\progra~2\HP\HP BTO Software\bin* directory at the command prompt, and issue the following command:

   nnmtrapdump.ovpl

   This will invoke Figure 1.18, where you can view the SNMP traps that the eG manager sends to the NNM console, along with their OIDs.

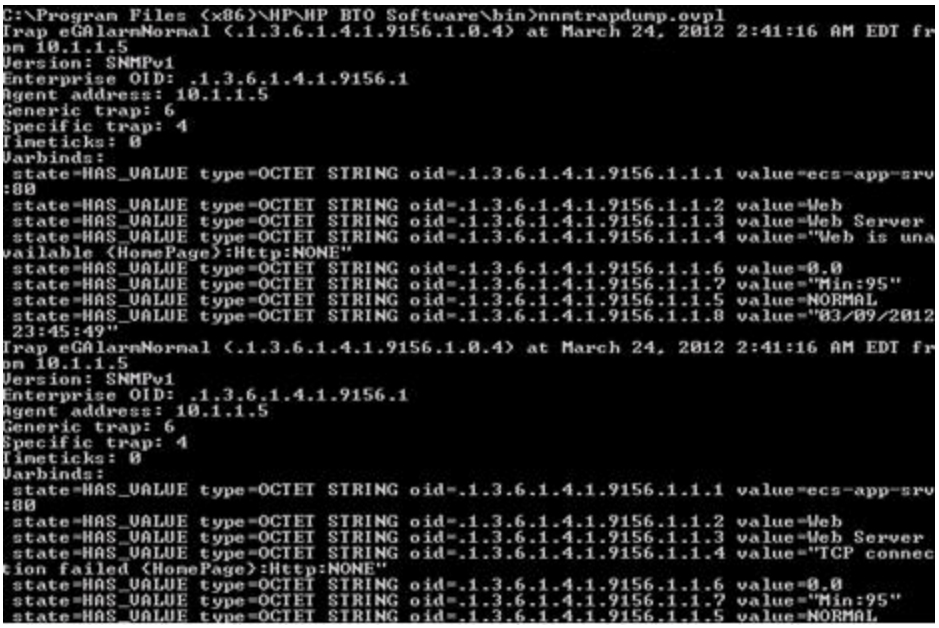

Figure 1.18: Viewing the eG trap dump

10. You can also view the eG alerts in the NNM console, when you follow the Incident Browsing -> All Incidents node sequence (see Figure 1.19).

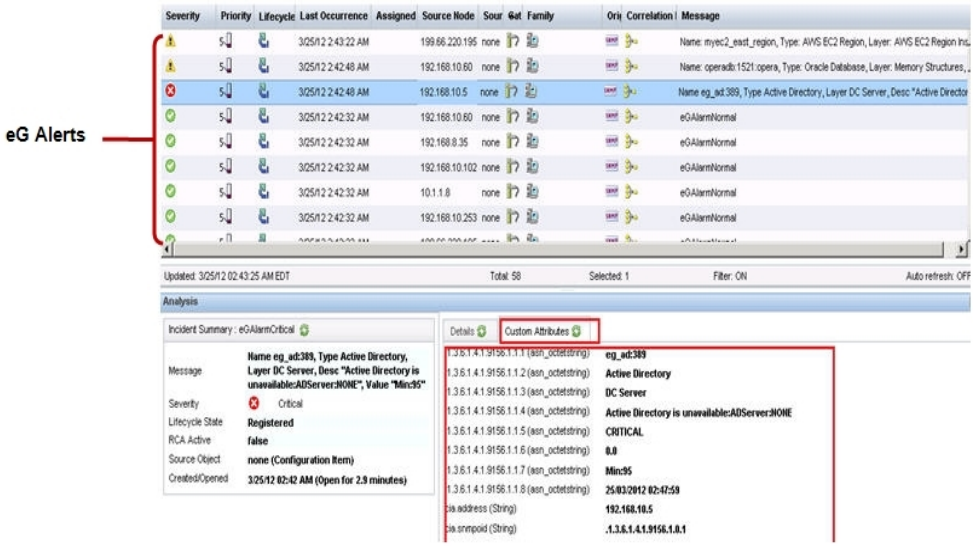

Figure 1.19: Viewing the eG alerts in the NNM console

11. If you double-click on an eG alert in the list, an **Analysis** section will open below (see Figure 1.19). In the **Custom Attributes** tab page of the **Analysis** section, you can find the complete details of the alert clicked on, which includes:

- The problem component name
- The problem component type
- The problem layer
- A brief description of the problem
- The alarm priority (Critical/Major/Minor), and more!

Alongside each such information, the trap OID vide which that information was sent to the NNM console will also be displayed.

12. By default, all eG alerts will be tagged as **Normal** alerts (i.e., priority/severity of the alerts will be **Normal**), when they are received and displayed in the NNM console for the very first time. You will have to manually map the priority of each alert in the eG manager with its corresponding state in the NNM console for the NNM console to accurately indicate the alarm priority. For this, do the following:

    - Follow the Incident Browsing -> All Incidents node sequence in the NNM console.
    - Once the eG alerts appear in the right panel, right-click on an alert, and select the **Open Incident Configuration** option from the shortcut menu that appears (see Figure 1.20).
    - An **SNMP Trap Configuration** window will then appear, where the details of SNMP trap that corresponds to the chosen eG alert will be displayed (see Figure 1.20).
    - From the **Severity** drop-down in the **SNMP Trap Configuration** window, select the alarm severity in the NNM console that maps to the priority of that alert in the eG manager. Then, click on the **Save and Close** option to save the configuration changes.

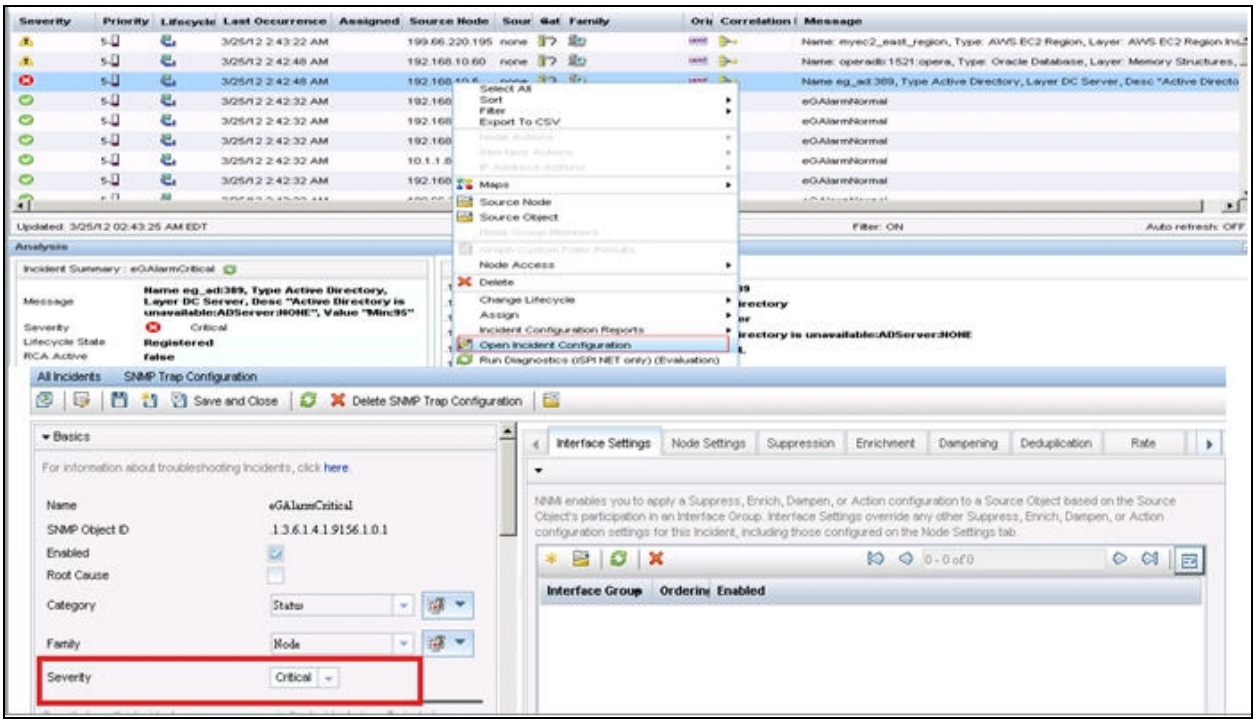

Figure 1.20: Mapping the priority of an eG alert with its corresponding severity level in the NNM console