TOC

Chapter 2: Introduction

The architecture of the eG monitoring suite is characterized by a single, central eG manager to which eG agents report critical performance data pertaining to the monitored components. Typically, the number and type of agents to be deployed in a target environment depends upon the infrastructure size (i.e. the number of hosts to be monitored), the applications residing on the hosts, and the level of complexity that the environment embeds. Naturally, large, mission-critical infrastructures, hosting a wide variety of components distributed across multiple domains, will require a significant number of agents. In such environments, manual installation of agents could prove to be both laborious and time-consuming. Besides, other key operations such as starting and stopping the eG agents will have to be performed individually for each of the monitored servers, thereby adding aplenty to the administrator's workload.

In order to simplify the installation and management of agents, the eG monitoring suite provides the eG Remote Agent Controller (RAC). Designed specifically for agent deployments on Microsoft Windows environments, this tool enables administrators to quickly and easily install eG agents on the Windows hosts in a target environment from a central location, without having to switch between numerous server consoles. In addition, the tool ensures that the starting, stopping, and uninstallation of the installed agents can be performed with a few mouse clicks. This eliminates the drudgery of manual agent installation, and saves the time and effort involved in exercising manual control on every agent.

Chapter 2: Installation of the eG Remote Agent Controller

This chapter describes the steps involved in installing the eG remote agent controller.

The eG RAC has to be installed on a system that should fulfill the following pre-requisites:

- Windows 2008 server (OR) Windows 7 (OR) Windows 8 (OR) Windows 10 (OR) Windows 2012
- 100 MB disk space with 256 MB RAM

2.1 Installing the eG Remote Agent Controller

The steps involved in installing the eG RAC are as follows:

1. To start the installation process, insert the installation CD in your CD-drive and run the **RAC.exe** program within the **Remote Agent Controller** directory therein. Figure 2.1 then appears. Clicking on the **Next >** button at the bottom of this screen takes the user to the next step of the

setup.

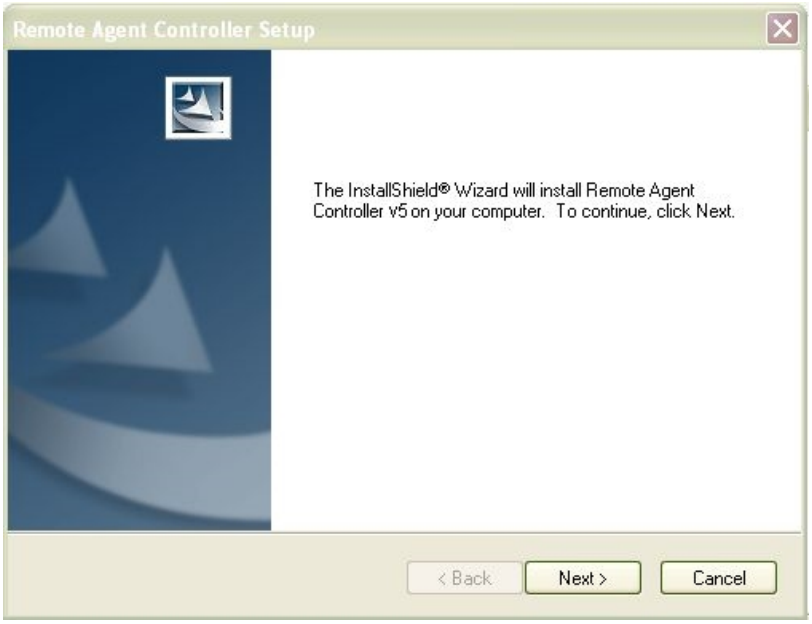

Figure 2.1: Welcome screen of the eG RAC Setup program

2. Click on the **Yes** button in Figure 2.2 to accept the displayed license terms and proceed. Clicking on **No** here will terminate setup.

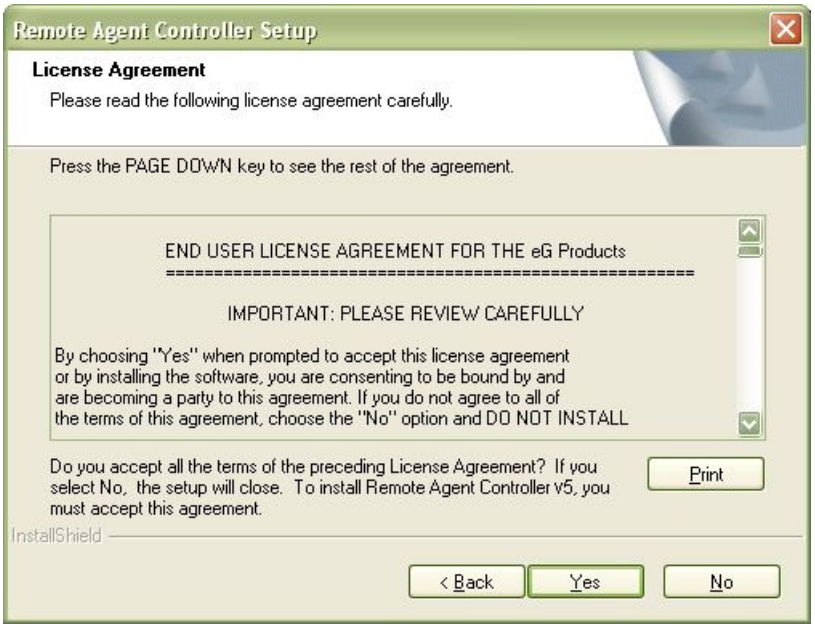

Figure 2.2: Accepting the license terms

3. The installation process then prompts you to select the destination location for the eG RAC (see Figure 2.2).

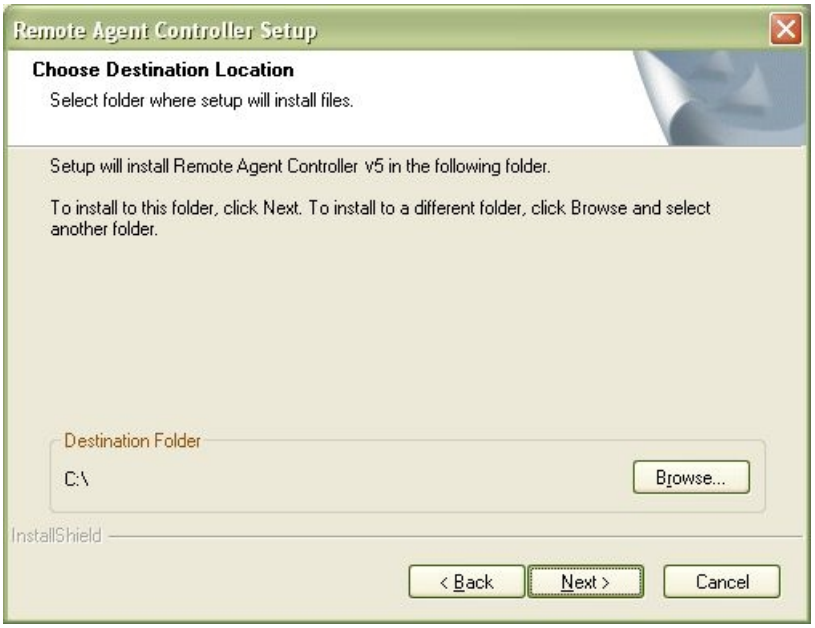

Figure 2.3: Specifying the location of RAC

4. If the configuration process succeeds, the following screen will be displayed (Figure 2.4). The Setup requires the user to restart the system. This can be done immediately or at a later point of time. Clicking on the **Finish** button will exit the Setup.

Figure 2.4: Setup program indicating the completion of the eG RAC installation

2.2 Uninstalling the eG Remote Agent Controller

To uninstall the eG RAC, do the following:

1. To begin uninstalling the eG RAC, follow the menu sequence: Start -> Programs -> eG Monitoring Suite -> Uninstall Agent Controller.
2. The screen depicted by Figure 2.5 will appear. Here, select the **Remove** option and click the **Next >** button.

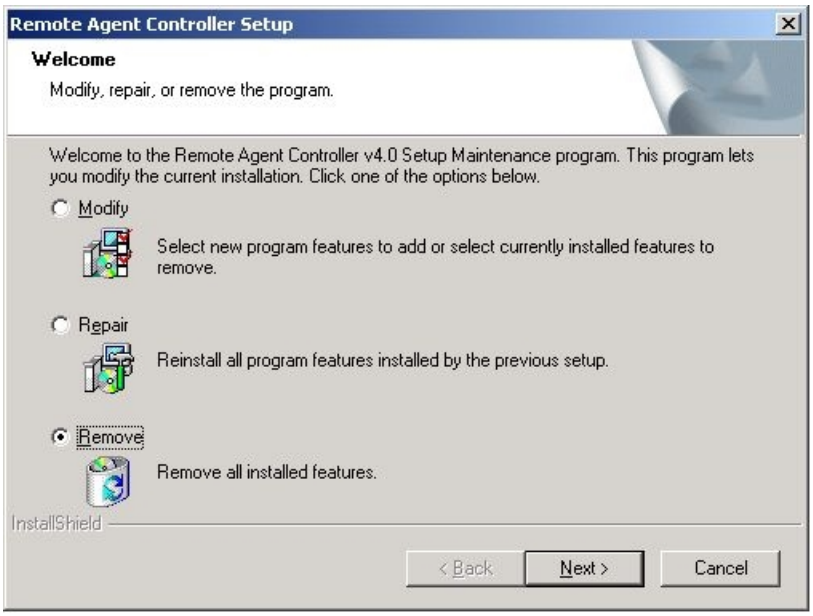

Figure 2.5: Uninstalling the eG RAC

3. This process requires the confirmation of the user to remove the package and its related components as in Figure 2.6. Click the **OK** button.

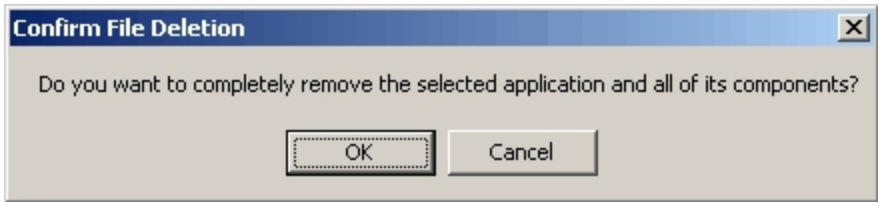

Figure 2.6: Uninstall process seeking the confirmation of the user to delete the eG manager

4. Upon clicking **OK**, the following screen will appear. Click **Finish** here to complete uninstalling the RAC.

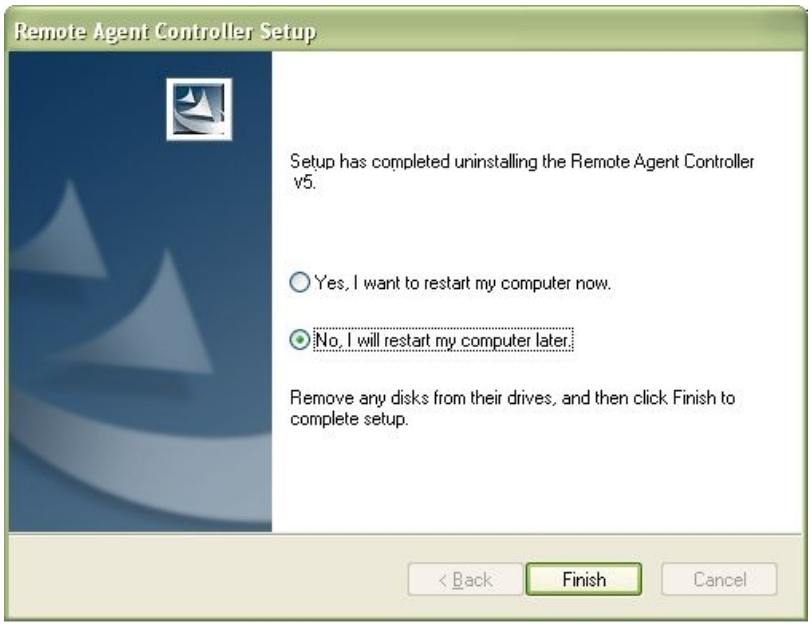

Figure 2.7: Completion of the eG RAC uninstallation

2.3 Installing the eG Remote Agent Controller

The eG RAC has to be installed on a system that should fulfill the following pre-requisites:

- Windows 2008 server (OR) Windows 7 (OR) Windows 8 (OR) Windows 10 (OR) Windows 2012
- 100 MB disk space with 256 MB RAM

The steps involved in installing the eG RAC are as follows:

1. To start the installation process, insert the installation CD in your CD-drive and run the **RAC.exe** program within the **Remote Agent Controller** directory therein. Figure 2.8 then appears. Clicking on the **Next >** button at the bottom of this screen takes the user to the next step of the setup.

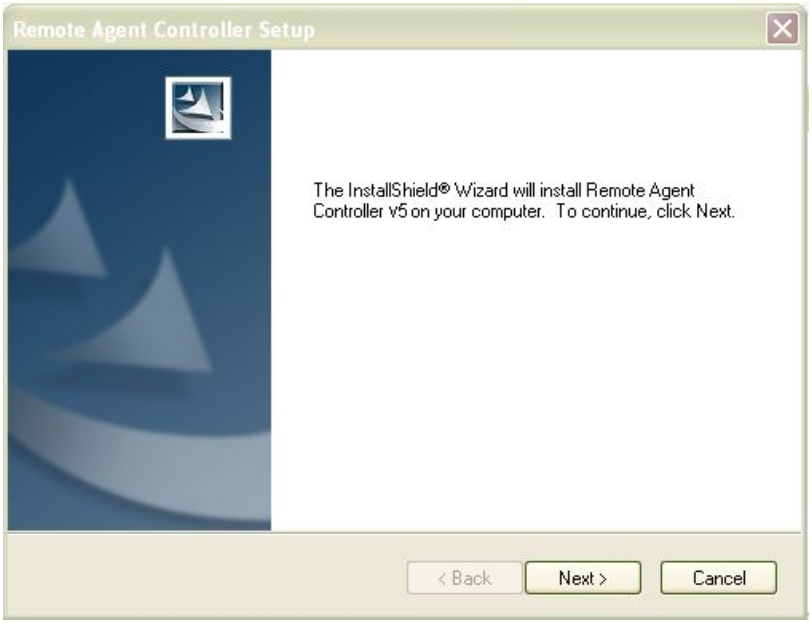

Figure 2.8: Welcome screen of the eG RAC Setup program

2. Click on the **Yes** button in Figure 2.2 to accept the displayed license terms and proceed. Clicking on **No** here will terminate setup.

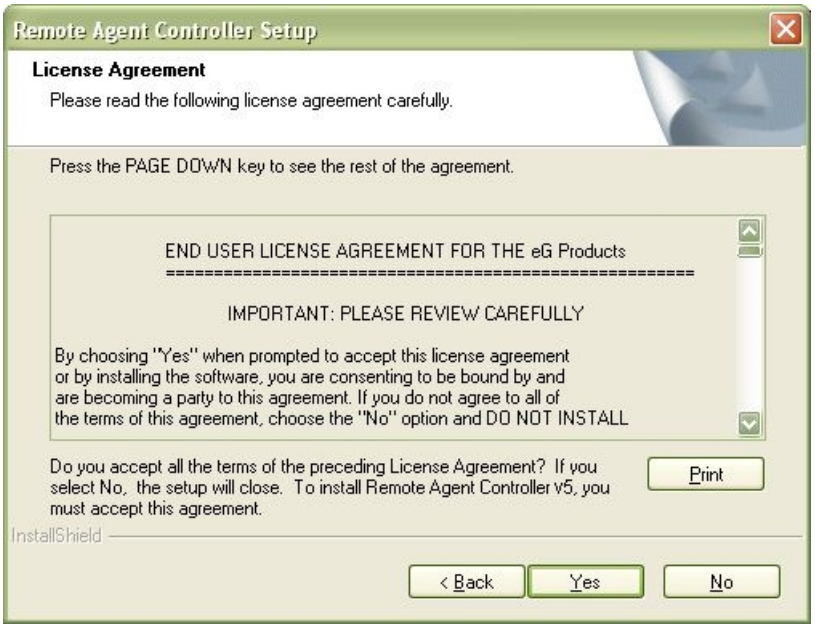

Figure 2.9: Accepting the license terms

3. The installation process then prompts you to select the destination location for the eG RAC (see

Figure 2.9).

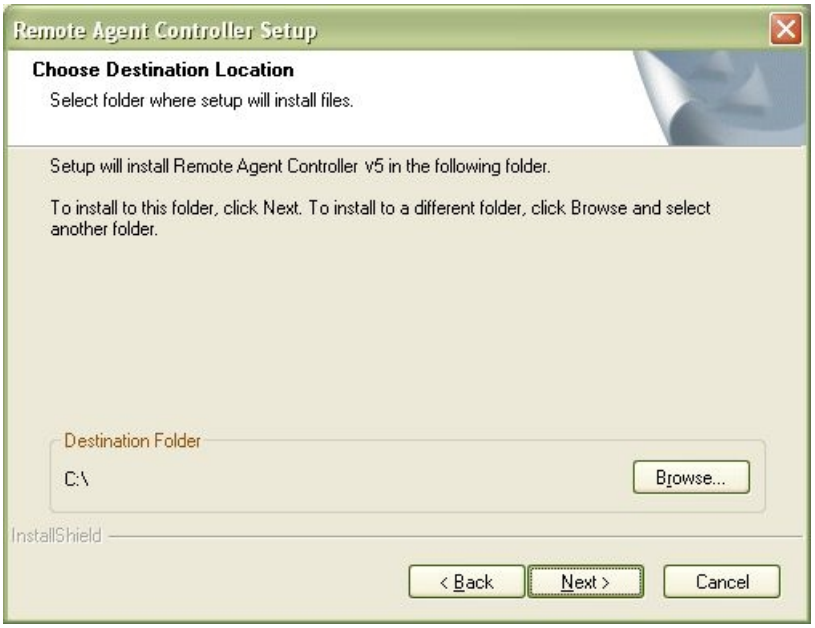

Figure 2.10: Specifying the location of RAC

4. If the configuration process succeeds, the following screen will be displayed (Figure 2.11). The Setup requires the user to restart the system. This can be done immediately or at a later point of time. Clicking on the **Finish** button will exit the Setup.

Figure 2.11: Setup program indicating the completion of the eG RAC installation

2.4 Uninstalling the eG Remote Agent Controller

To uninstall the eG RAC, do the following:

1. To begin uninstalling the eG RAC, follow the menu sequence: Start -> Programs -> eG Monitoring Suite -> Uninstall Agent Controller.
2. The screen depicted by Figure 2.12 will appear. Here, select the **Remove** option and click the **Next >** button.

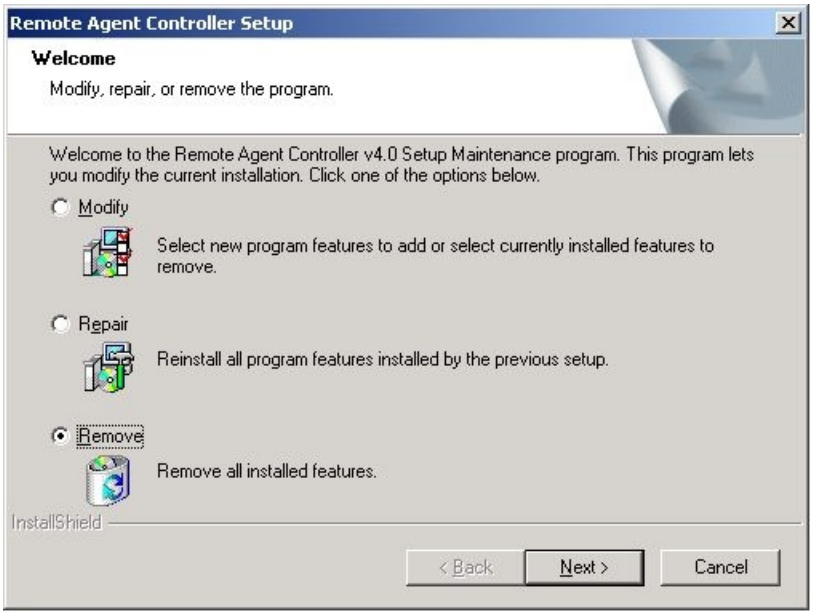

Figure 2.12: Figure 2.5: Uninstalling the eG RAC

3. This process requires the confirmation of the user to remove the package and its related components as in Figure 2.13. Click the **OK** button.

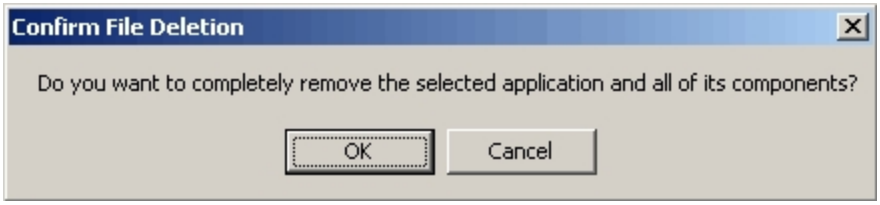

Figure 2.13: Figure 2.6: Uninstall process seeking the confirmation of the user to delete the eG manager

4. Upon clicking **OK**, the following screen will appear. Click **Finish** here to complete uninstalling the RAC.

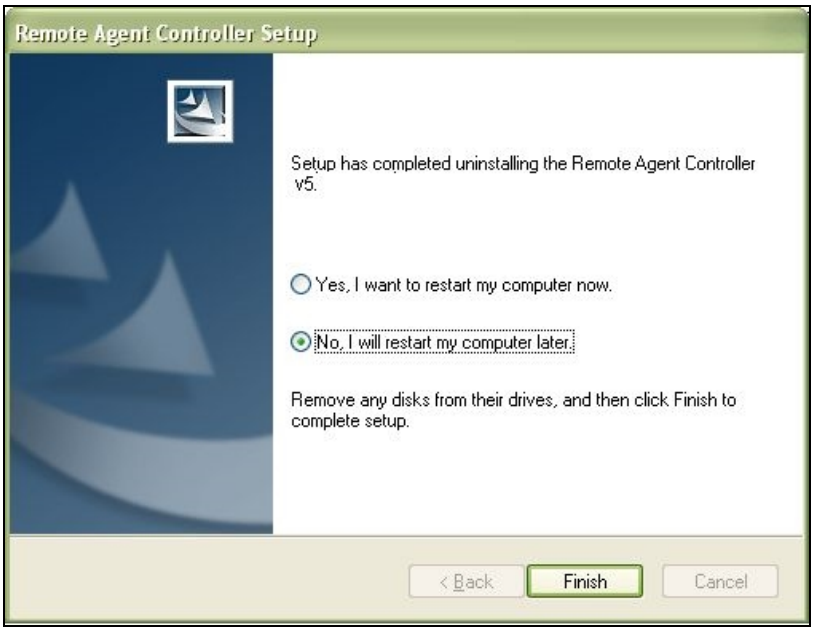

Figure 2.14: Figure 2.7: Completion of the eG RAC uninstallation

Chapter 2: Using the eG Remote Agent Controller

After installing the RAC, proceed to use the application to install/uninstall/control agents remotely.

Using RAC, the following key tasks can be performed:

- Automatic discovery of servers across domains
- Automatic grouping of the discovered servers based on agent status
- Retrieving recently discovered hosts
- Connecting to individual servers and retrieving their environment information
- Remote installation of agents on chosen hosts
- Defining the nick names for an eG agent
- Changing agent settings
- Starting / stopping agents on remote hosts

- Uninstalling the eG agents which have been remotely/manually installed
- Remotely enabling/disabling agent logs, and more!

This chapter discusses these functions and many others in great detail.

However, prior to using RAC, ensure that the pre-requisites outlined in Section 3.1 are fulfilled.

2.5 Pre-requisites for Using RAC

Before attempting to use RAC, make sure that the pre-requisites detailed in this section are fulfilled. For ease of use, we have grouped the pre-requisites into requirements for host discovery and remote agent operations.

2.5.1 Pre-requisites for Performing Host Discovery Using RAC

1. After installing RAC, start RAC by using the Run as Administrator option.
2. All the remote Windows hosts on which you want eG agents installed should be accessible from the RAC host.
3. In order to remotely connect to all the Windows servers and desktops in a domain, RAC requires domain administrator privileges. To use RAC therefore, a user should login to the RAC host as a domain administrator only.
4. Make sure that **File and Print Sharing** is turned on for all remote Windows hosts. For this, select **Network Connections** (or on some Windows flavors, **Network and Sharing Center -> Advanced Settings**) from the **Control Panel** on each Windows host, and choose the **Turn on file and printer sharing** option from the **File and printer sharing** section (see Figure 2.15).

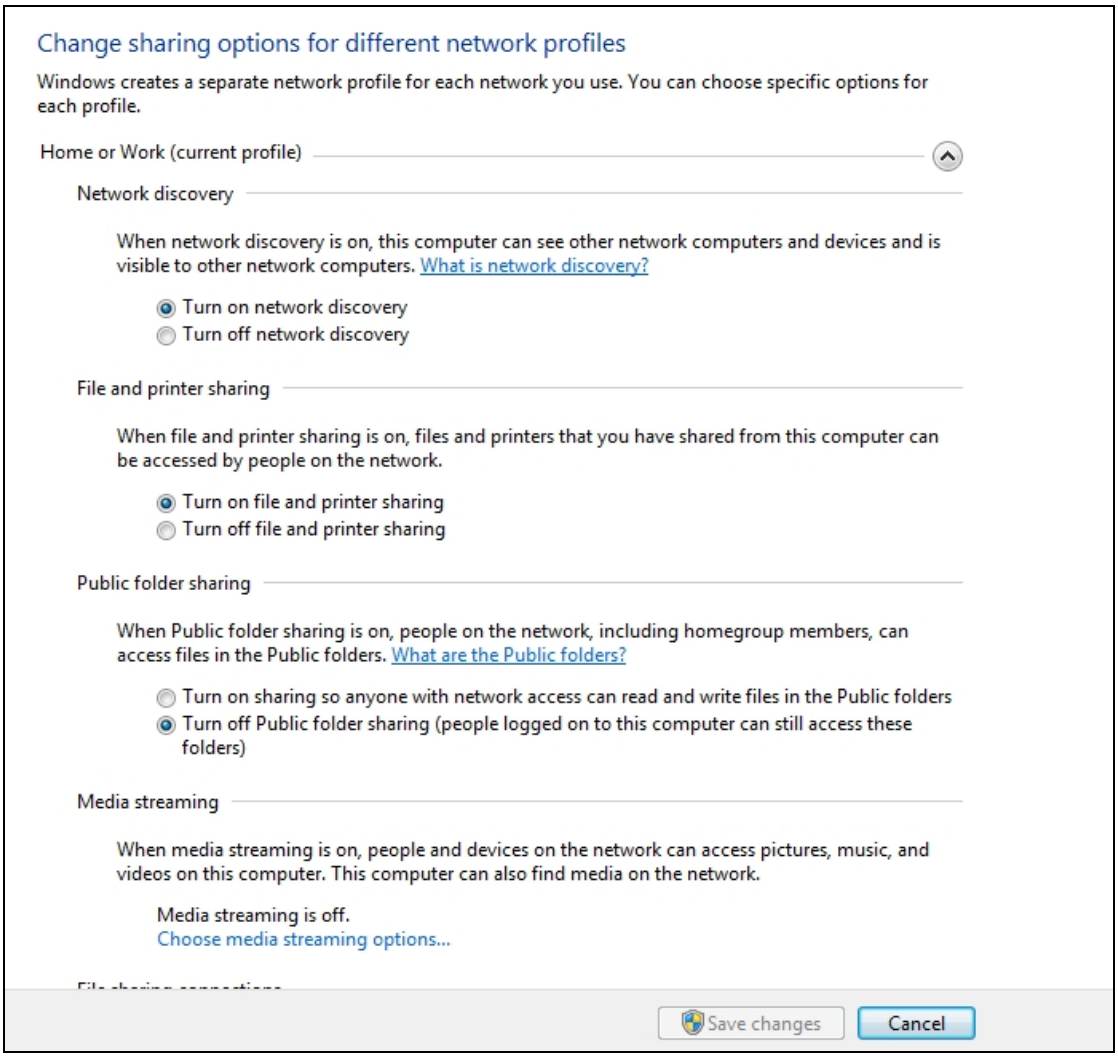

Figure 2.15: Turning on file and print sharing

5. Make sure that the Windows Firewall on each of the remote Windows hosts that RAC needs to access has been configured to allow the **File and Printer Sharing** program. For that, do the following:

   - Log into the target Windows host.
   - Click on **Windows Firewall** within **Control Panel**.
   - Then, click on the **Allow a program or feature through Windows Firewall** option in the left panel of Figure 2.16 that appears.

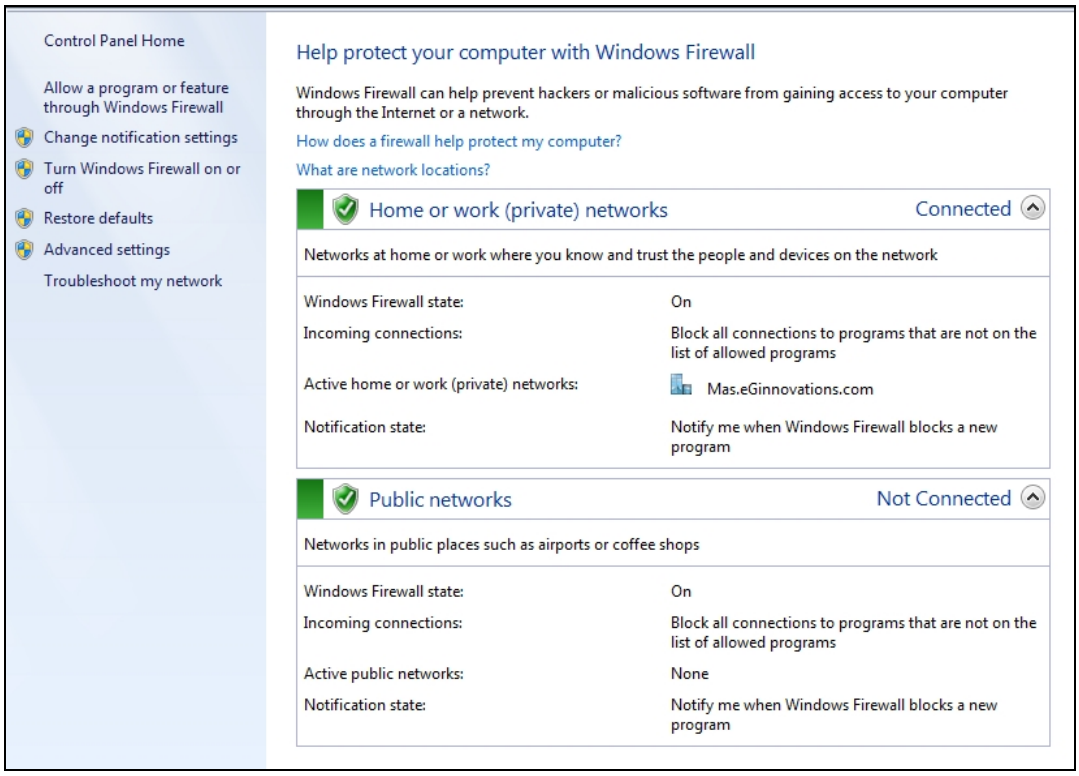

Figure 2.16: Configuring the Windows Firewall

- Figure 2.17 will then appear. Click the **Change Settings** button in Figure 2.17.
- Then, locate the **File and Printer Sharing** program in the **Allowed Programs and Features** list. Next, select the check box alongside **File and Printer Sharing** to allow the program through the firewall.
- You also have to indicate the network profile (i.e., location) in which the firewall should allow this program. The options here are: Home/Work, Public, Private, or Domain. Your choice depends upon where the target hosts are and where RAC is. For instance, to allow RAC to only access the hosts in its work group, the **File and Printer Sharing** program should be allowed for **Home/Work**. For that, you need to select the check box in the **Home/Work** column corresponding to the **File and Printer Sharing** program (as done in Figure 2.17).

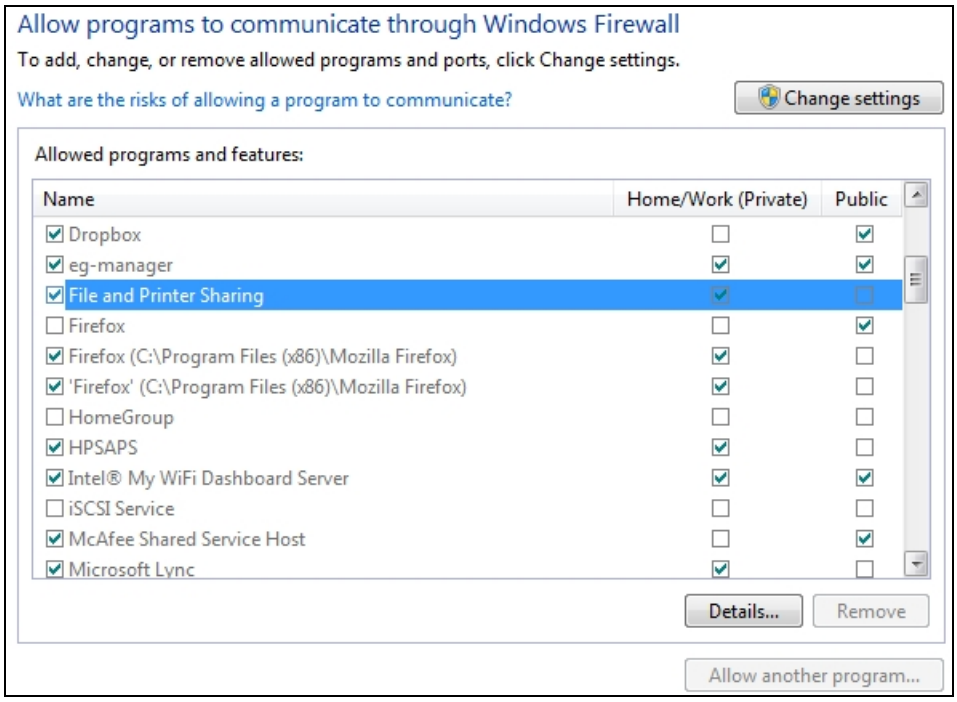

Figure 2.17: Allowing File and Printer Sharing program through Windows Firewall

- Finally, click on the **OK** button (not shown in Figure 2.17).

6. If you have a **3rd party firewall** installed, then you will also need to allow **File and Printer Sharing** through that firewall as well.

7. By default, Windows Firewall blocks Network discovery. Network discovery is a network setting that governs whether/not the system hosting RAC will be able to find other hosts and devices on the network and whether/not other hosts/devices on the network will be able to find the RAC host. To enable RAC to discover and communicate with target Windows hosts, **Network Discovery** should be turned on for the RAC host and for each remote Windows host that the RAC host seeks to interact with. To achieve this, do the following:

   - Log into the remote host or RAC (as the case may be).
   - Select **Network and Sharing Center** from the **Control Panel**.
   - Click on **Change Advanced Settings**.
   - Figure 2.18 will then appear. Typically, using Figure 2.18, you will be able to define the network sharing properties of different network profiles (or locations), namely:

- Home/Work
- Private
- Public
- Domain

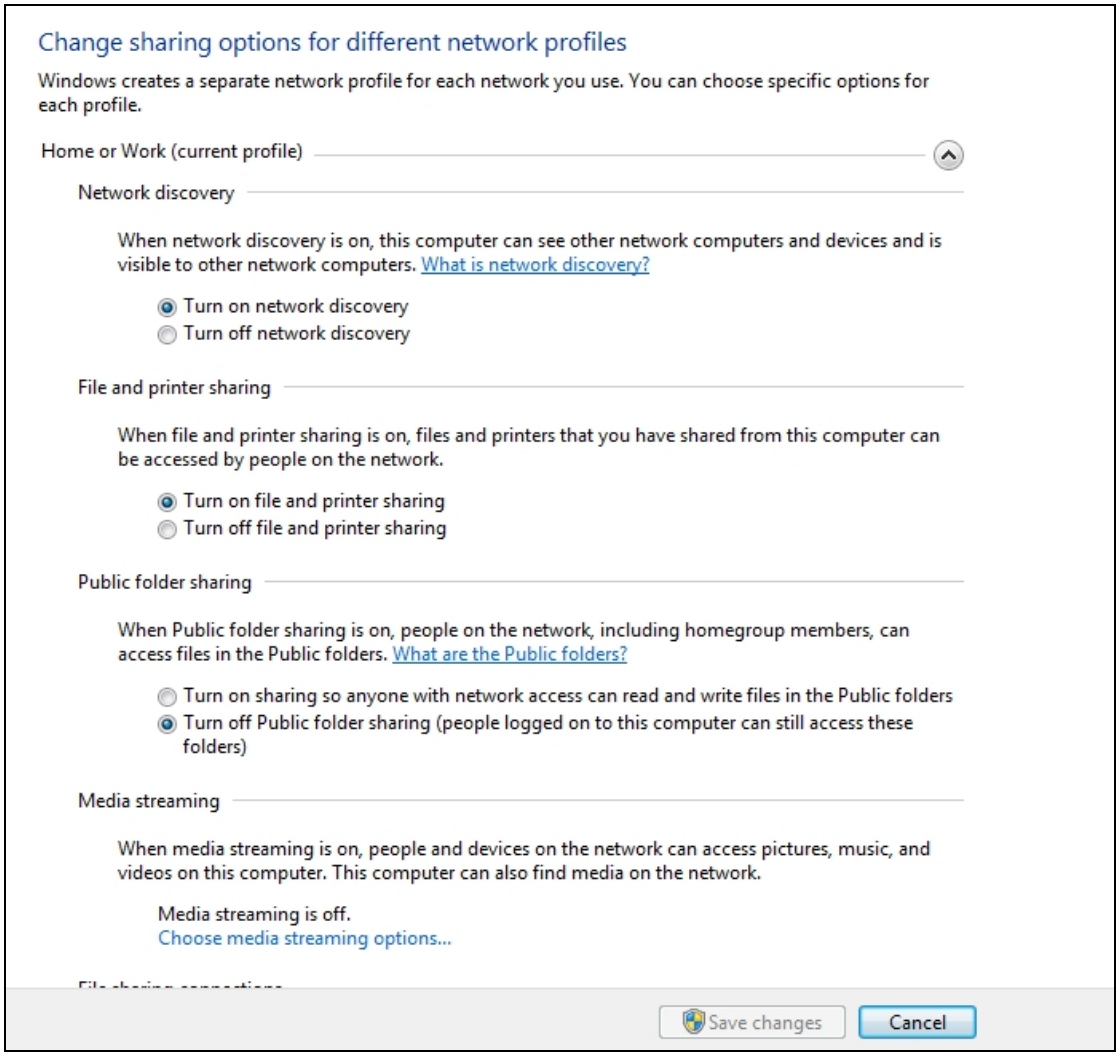

Figure 2.18: Enabling network discovery

- Depending upon which remote hosts the RAC will be accessing and where these hosts are, you can enable **Network discovery** for the corresponding profile. For instance, if RAC needs to discover and communicate with only those remote hosts that are in its work group, then network discovery should be enabled for the **Home/Work** profile only. For this, first expand the **Home/Work** section by clicking the down-arrow at the far right end of the section label (if the

section is already expanded, as in the case of Figure 2.18 above, you can skip this step). Next, under the **Network Discovery** section of **Home/Work**, select the **Turn on network discovery** option, and click the **Save changes** button (see Figure 2.18). Once this is done, RAC will be able to discover hosts in its work group alone, and not in a domain / public internet / private network.

8. Additionally, you need to configure the Windows Firewall on each remote Windows host with which RAC will communicate to allow the **Network Discovery** feature. For this, do the following:

   - Login to the remote host.
   - Select **Windows Firewall** from the **Control Panel**.
   - Figure 2.19 will then appear:
   - Then, click on the **Allow a program or feature through Windows Firewall** option in the left panel of Figure 2.19 that appears.

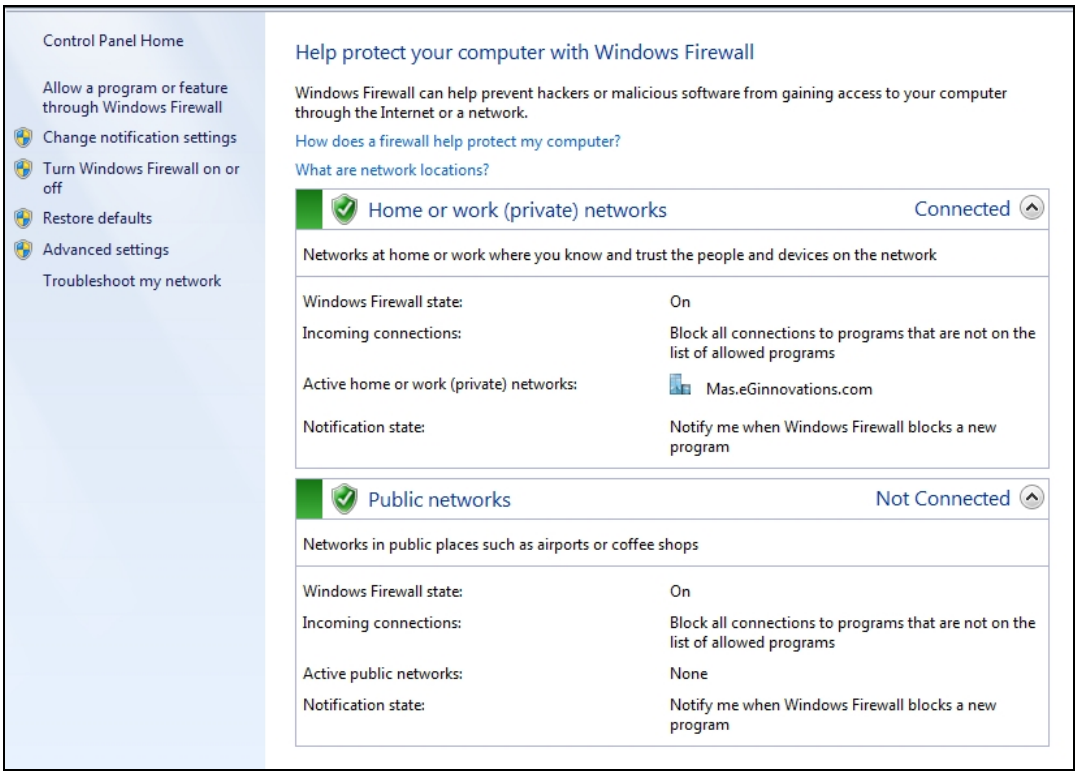

Figure 2.19: Choosing to allow a feature through Windows Firewall

   - Figure 2.20 will then appear. Click the **Change Settings** button in Figure 2.20.

- Then, locate the **Network Discovery** feature in the **Allowed Programs and Features** list. Next, select the check box that precedes **Network Discovery** (in Figure 2.19) to allow that feature through the firewall.

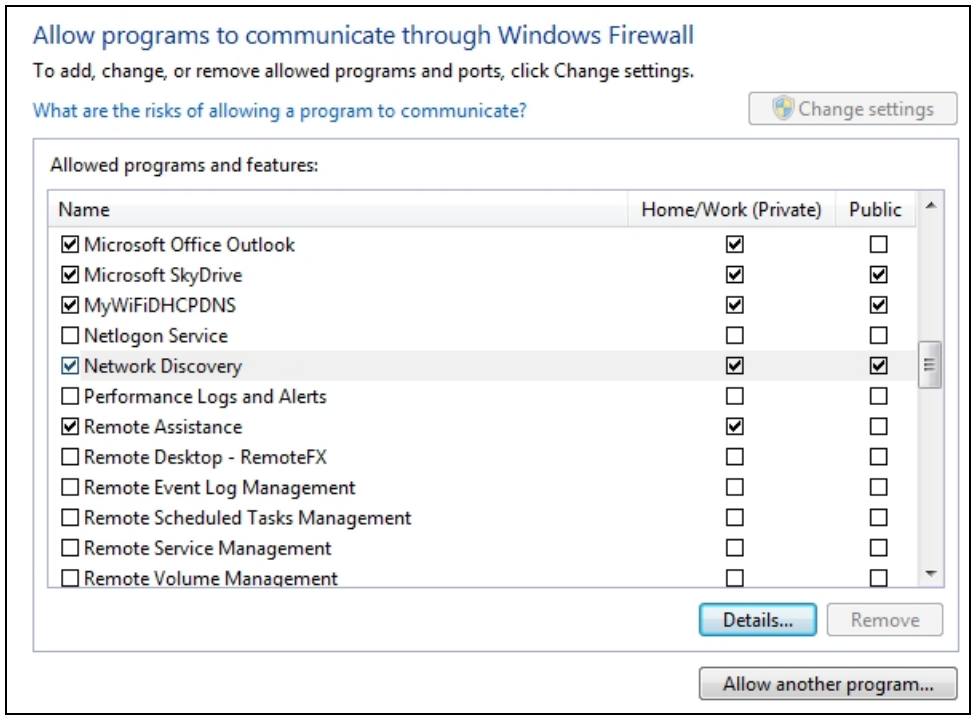

Figure 2.20: Configuring the Windows Firewall to allow Network discovery

- You also have to indicate the network profile (i.e., location) in which the firewall should allow this feature. The options here are: Home/Work, Public, Private, or Domain. Your choice depends upon where the target hosts are and where RAC is. For instance, to allow RAC to access the hosts in its work group and in the public internet, the **Network Discovery** feature should be allowed for **Home/Work** and **Public** profiles. For that, you need to select the check boxes in the **Home/Work** and **Public** columns corresponding to the **Network Discovery** feature (as shown by Figure 2.19).
- Finally, click on the **OK** button (not shown in Figure 2.19).

Network Discovery can also be enabled via a GPO. Given below are the steps for the same:

- While you are log on Windows server, type "**gpmc.msc**" on Run and press enter to open **Group Policy Management**.
- Try to expand **Forest – Domains** and right-click on the domain for which you want to create a group policy. Then, click **Create a GPO in this domain, and link to here**. It will create a new

GPO and linked to the chosen domain.

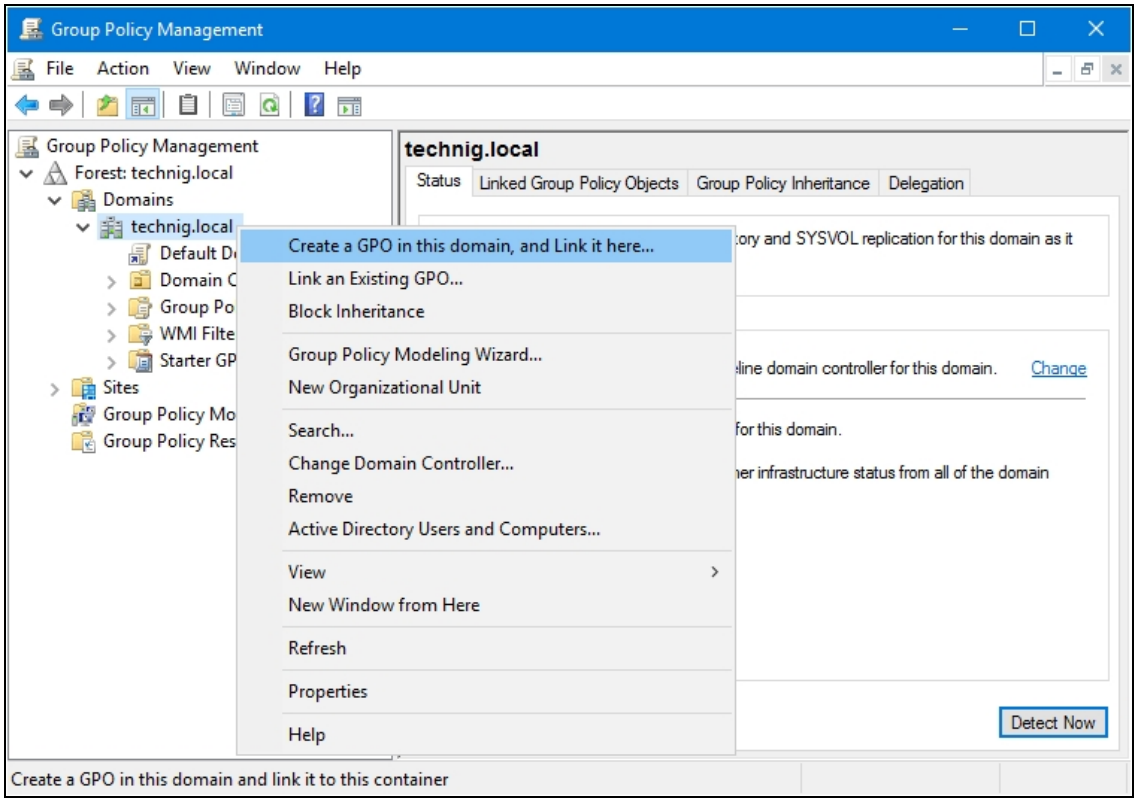

Figure 2.21: Choosing the option to create a GPO for a domain

- Name the new GPO. Then, right-click on the new GPO and click **Edit**.

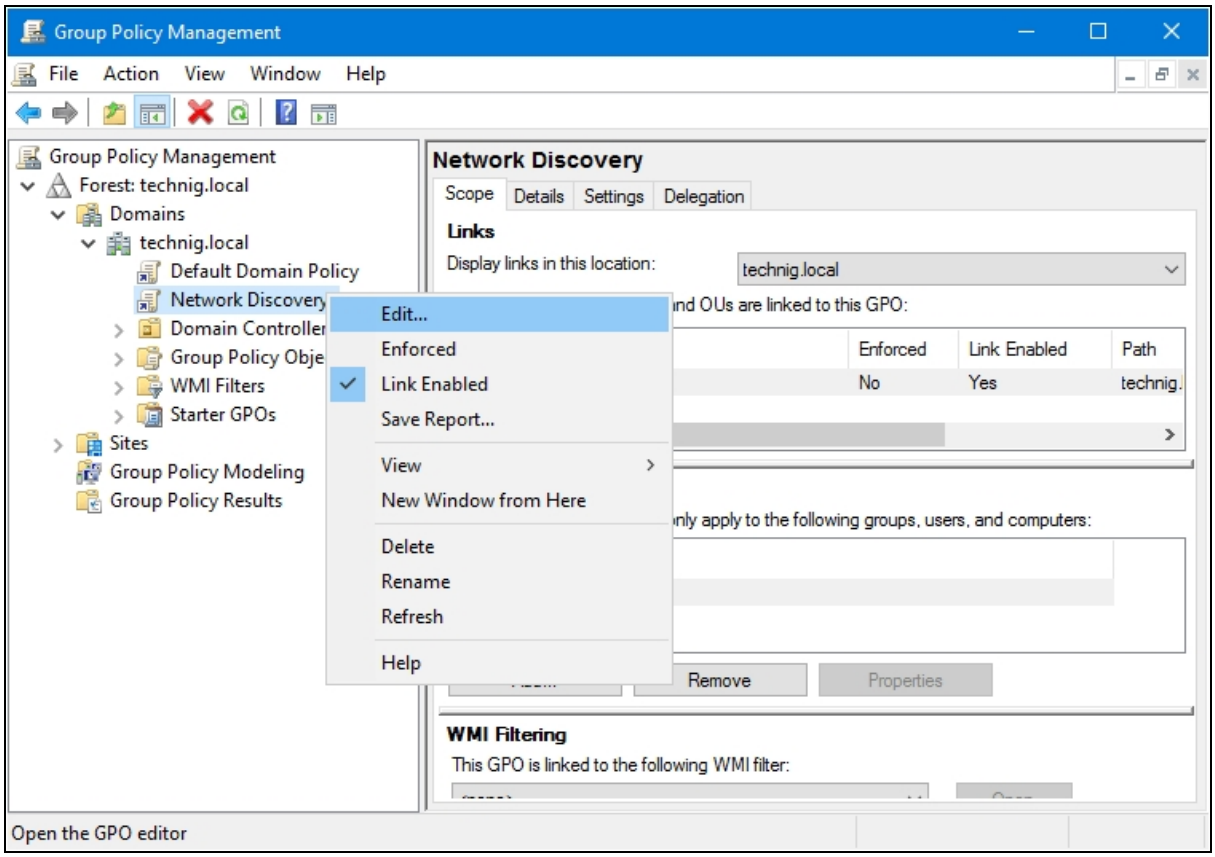

Figure 2.22: Editing the new GPO

- On **Computer Configuration**, expand Policy – Administrative Templates – Network and select **Link-ayer Topology Discovery**. Right- click the first policy "**Turn on Mapper I/O (LLTDIO) driver**" to enable it. Tick the check box of **Allow operation while in domain**.

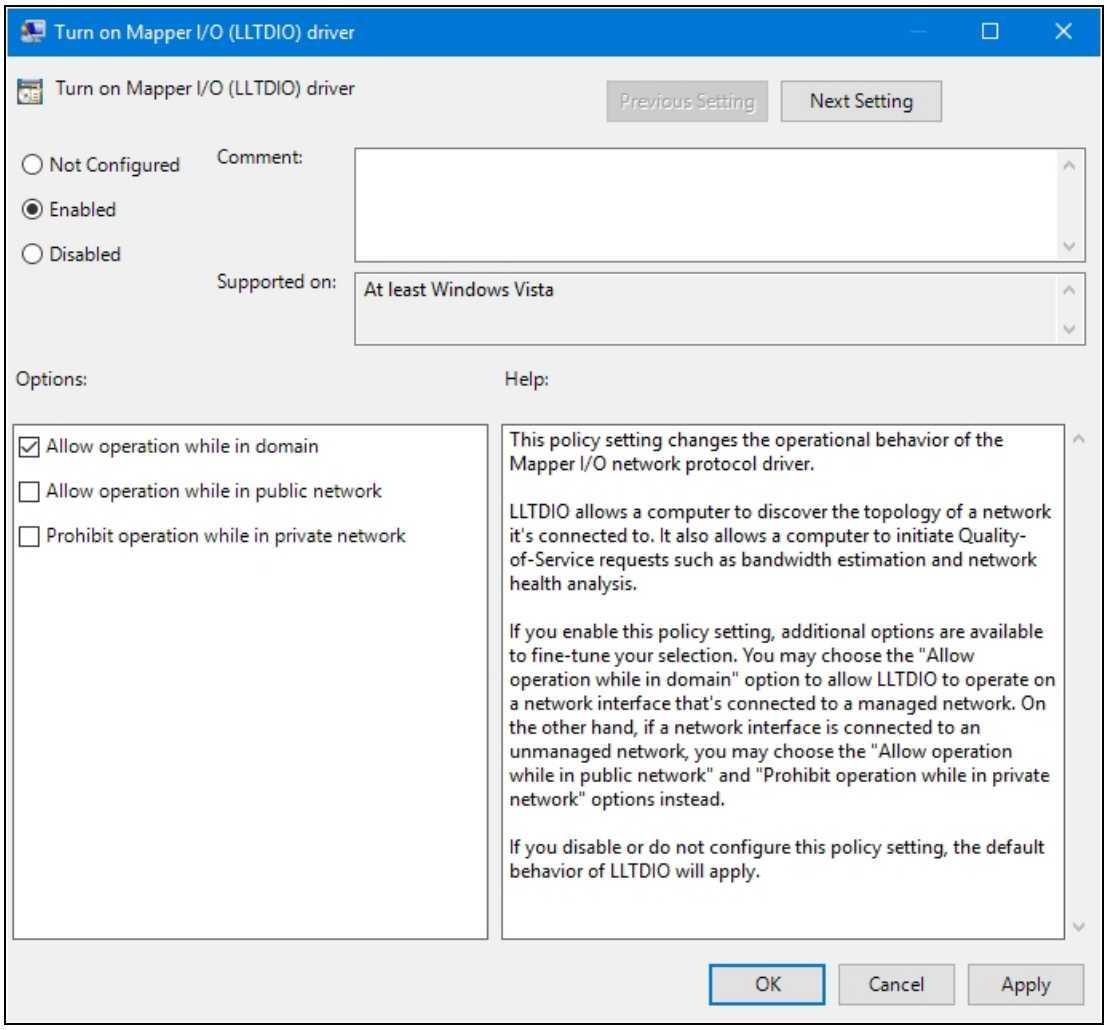

Figure 2.23: Turning on Mapper I/O

Note:

LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis.

- Now, enable **Turn on Responder (RSPNDR) driver** also. Do the same settings for **Turn on Responder (RSPNDR)** driver as above screenshot.

  Note:

  The Responder allows a computer to participate in **Link Layer Topology Discovery** requests so that it can be discovered and located on the network. It also allows a computer to

participate in Quality-of-Service activities such as bandwidth estimation and network health analysis. It enables Network Discovery via group policy.

- Finally, go to the command prompt and type "**gpupdate /force**" to update the group policy on the Windows Server. Execute the command on client computer as well or it will apply automatically when system restarts.

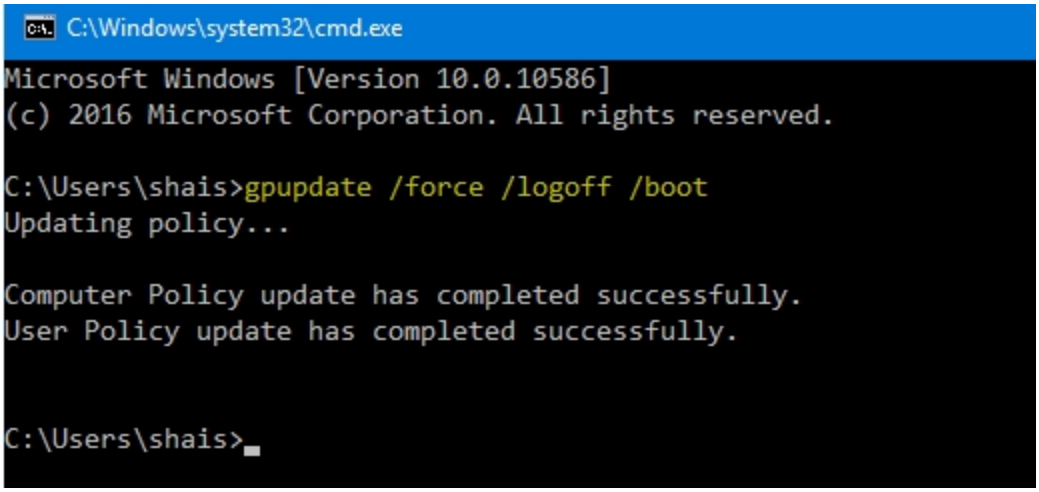

Figure 2.24: Updating group policy on Windows server

9. Moreover, if you have a **3rd party firewall** installed, then you will also need to allow **Network Discovery** through that firewall as well, for network discovery to function without a glitch.
10. Furthermore, network discovery relies on a few Windows services for normal functioning. These services need to be started on the remote Windows hosts to fully enable network discovery. Such services are as follows:

    - DNS Client
    - Function Discovery Resource Publication
    - Function Discovery Provider Host
    - SSDP Discovery
    - UPnP Device Host
    - Server
    - Workstation
    - Computer Browser

- Registry
- Link-Layer Topology Mapper.

11. Similarly, make sure that the following ports are opened on each remote Windows host that you want discovered using RAC, so as to enable network discovery:

    - TCP 2869 (UPnP Device Host)
    - TCP 5357 (WSDAPIEvents)
    - TCP 5358 (WSDEvents Source)
    - TCP 445 (NetBIOS Helper)
    - UDP 5355 (LLMNR)
    - UDP 3702 (WSD publishing)
    - UDP 1900 (SSDP)
    - UDP 138 (NetBIOS Datagram)
    - UDP 137 (NetBIOS Name)
    - TCP 139 (Session Services)

12. Some remote Windows hosts might continue to be inaccessible to RAC even after all the requirements above are in place. This can happen if the User Access Control (UAC) feature is enabled on those Windows hosts.

    UAC is a security feature of Windows, which helps prevent unauthorized changes to your computer. These changes can be initiated by applications, viruses or other users. User Account Control makes sure these changes are made only with approval from the administrator. If the changes are not approved by the administrator, they are not executed and Windows remains unchanged.

    If RAC attempts to install/control an eG agent on a UAC-enabled Windows host, then UAC will instantly request RAC for confirmation to proceed with the installation. This confirmation can only be provided by manually clicking the **OK** button in the message prompt that UAC triggers on a target host. Since its quiet cumbersome to provide this manual confirmation on each UAC-enabled Windows host in an environment, and that too every time RAC launches a remote activity on the hosts, its recommended that UAC be disabled on all target Windows hosts in an environment.

    For this, do the following on every remote Windows host that RAC is unable to access:

- Login to the Windows host.
- Launch the Windows Registry Editor by typing **regedit** in the Run box.
- In the key-tree in the left panel of the editor, follow the key sequence: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
- Look for the value **LocalAccountTokenFilterPolicy** within.
- Once found, double-click on this value to edit it.
- Set its **Value data** to 1.
- Then, reboot the Windows host for the changes to take effect. On Windows 8 however, no reboot is required.

2.5.2 Pre-requisites for Performing Remote Operations on Agent Host Using RAC

In addition to the requirements listed in Section 3.1.1, you have to make sure that the following requirements are also fulfilled, if you want to perform any remote operation - eg., agent installation, uninstallation, starting, or stopping – on an agent host:

1. RAC uses the hidden shares – **Admin$** and **IPC$** - for performing the remote control activities. While the **Admin$** facilitates the discharge of administrative duties, the **IPC$** allows inter-process communication. These hidden shares have to be enabled on a remote Windows host for RAC to establish a connection with it.
2. Using RAC, agent deployments on the RAC host itself or on the eG Manager host cannot be performed; agents therefore will have to be manually installed on these hosts
3. Once RAC is installed, ensure that the agent install packages corresponding to the Windows operating systems in use in your environment, are copied to the relevant folders in the **<EG_RAC_INSTALL_DIR>**. For example, the agent install package for Windows 2008 32-bit operating system should be copied to the **<EG_RAC_INSTALL_DIR>\Windows 2000** directory.
4. Though you can remotely install agents of version 5.x and above using RAC, remember that at any given point in time, the agent install package of only one of the versions should be copied to the relevant folders in the **<EG_RAC_INSTALL_DIR>**. Decide on which installable to copy to the **<EG_RAC_INSTALL_DIR>** depending upon which agent version you intend installing shortly.

5. Only the *system administrator* of a remote Windows host is privileged to remotely install, start, stop, or uninstall an eG agent on it. Therefore, before attempting to use RAC to perform any of the above-mentioned remote operations, ensure the following:

   - Make sure you choose the **Change Logon account** option at the system-level, and then, proceed to provide the credentials of the *system administrator* of the target Windows host.
   - Make sure that the *system administrator* account that you have used above is added to the **Log on as a service** list of the target Windows 2008/Vista/7/8/2012 host. The related steps have been detailed in the **Troubleshooting the Remote Agent Controller** chapter.

Once the aforesaid pre-requisites are in order, proceed to perform each of the tasks discussed in the sections that follow.

2.6 Discovering Target Hosts and Agent Status

The first step towards agent installation is to identify the probable targets of installation. In order to achieve this, follow the steps given below:

1. First, access the eG Remote Agent Controller following the menu sequence: Start -> Programs -> eG Monitoring Suite -> Start Agent Controller (see Figure 2.25).

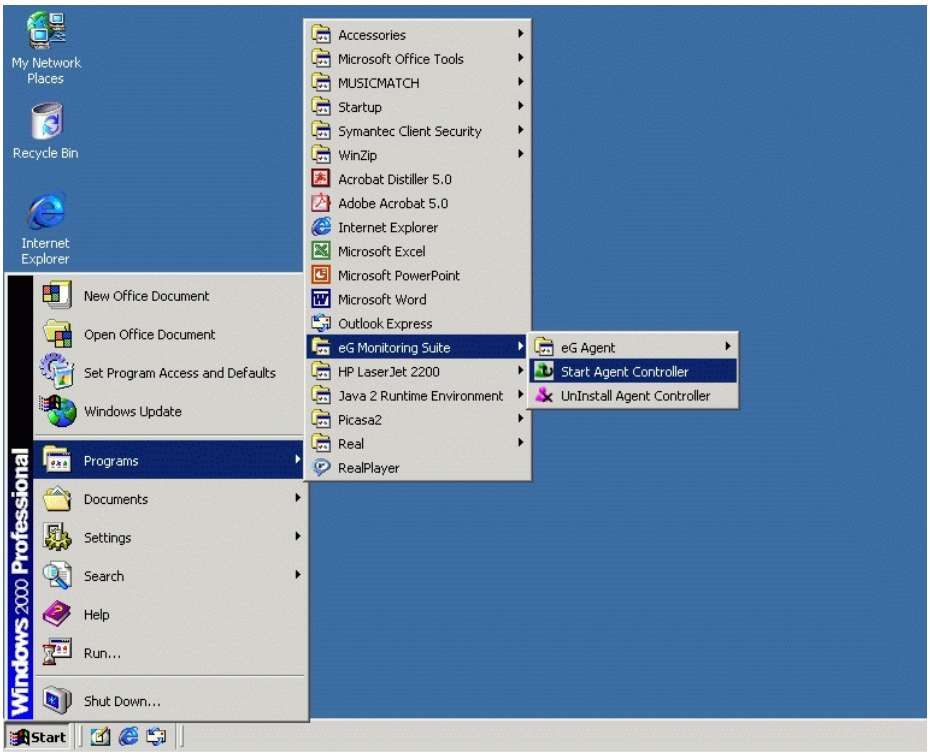

Figure 2.25: Starting the eG remote agent controller

2. The following screen will then appear:

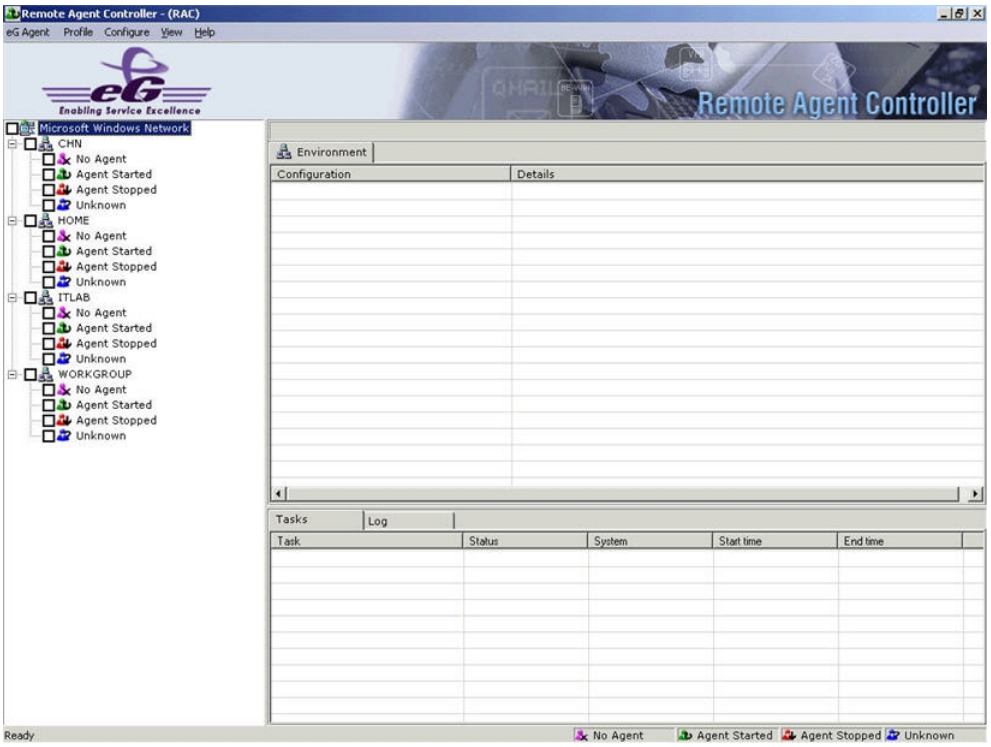

Figure 2.26: The eG Remote Agent Controller

3. The RAC console consists of a tree-structure in the left pane, containing nodes and sub-nodes. The nodes represent the domains in the target environment, and the sub-nodes are the hosts in each domain grouped according to the agent status - i.e., **No Agent**, **Agent Started**, **Agent Stopped** and **Unknown**.

   When RAC is started for the very first time, you will find that all the domains that constitute the monitored environment are automatically discovered, but the hosts in each of the domains are not. For instance, in Figure 2.26, **CHN** is a domain. While RAC automatically discovered **CHN**, the hosts within **CHN** have not been discovered. Accordingly, the **No Agent**, **Agent Started**, **Agent Stopped**, and **Unknown** nodes under **CHN** contain no sub-nodes. This is because, by default, RAC does not perform automatic host discovery on startup. You can override this default setting, so that hosts are automatically discovered whenever RAC is started next. To ensure this, first select the **Preferences** option from the **Configure** menu (see Figure 2.27).

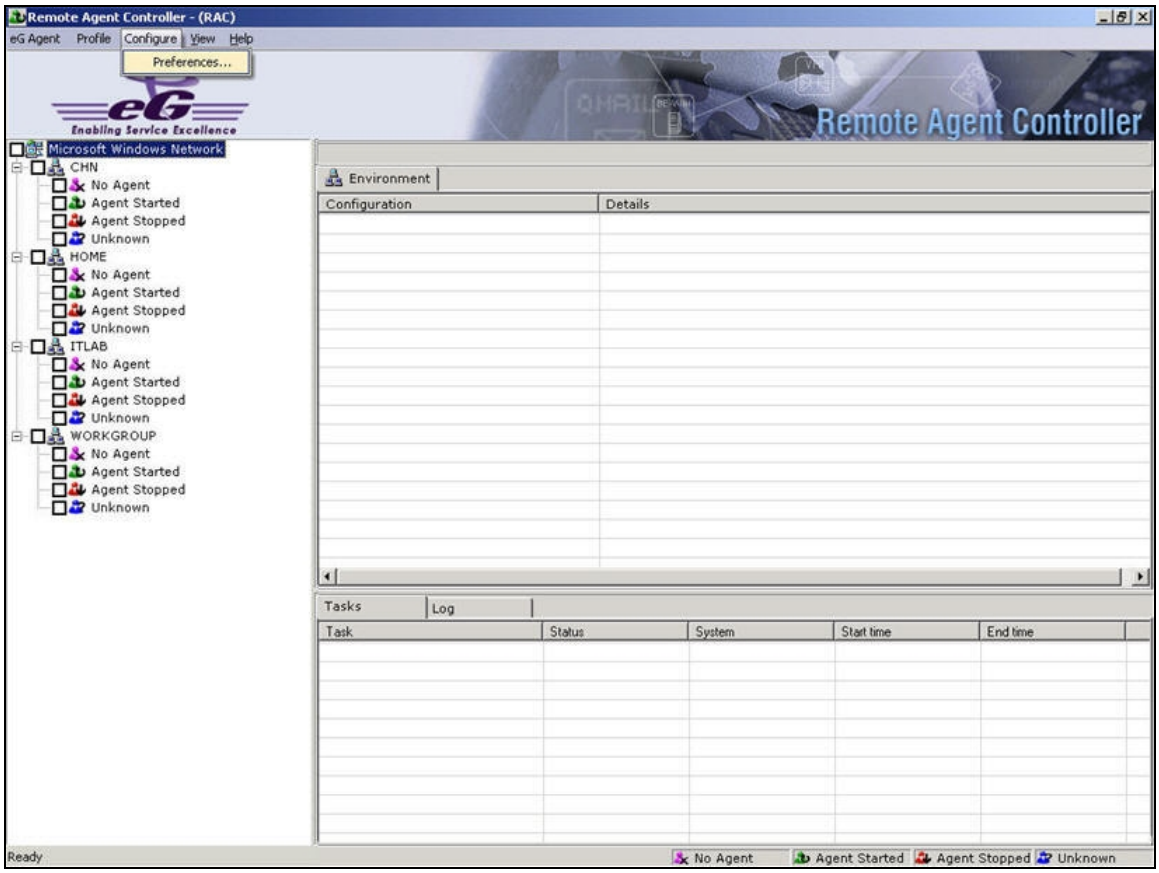

Figure 2.27: Selecting the Preferences option from the Configure menu

4. Next, select the **Startup** option in the left pane of the **Preferences** dialog box that appears (see Figure 2.28), and check the **Discover machines at startup** check box. This checkbox will be deselected by default.

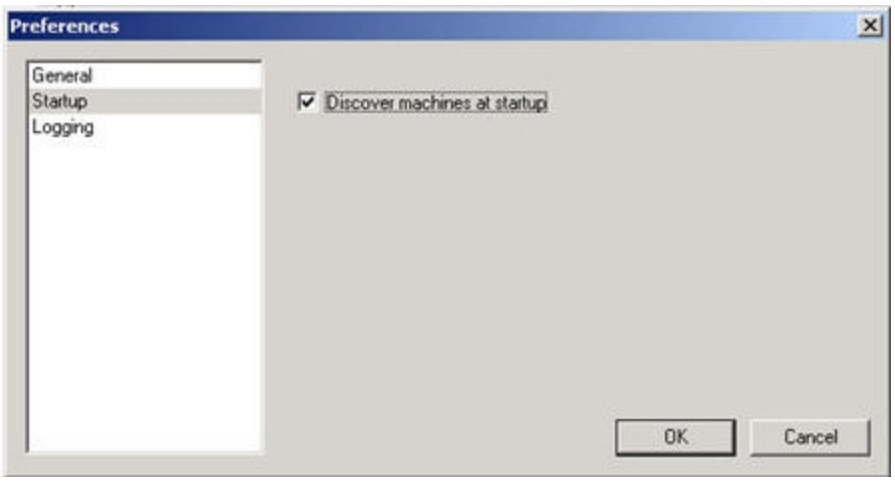

Figure 2.28: Selecting the option to discover hosts at startup

5. Click the **OK** button to register the changes (see Figure 2.28).

6. Now that the 'automatic host discovery' flag has been switched on, hosts in all the domains will be automatically discovered the next time you start RAC. On the other hand, if you choose not to enable automatic discovery, then you will have to manually run a discovery routine everytime you start RAC. This discovery procedure can be executed at the individual domain-level or across domains. To discover the hosts in a particular domain, select the domain, right-click on it, and choose the **Start discovery** option from the shortcut menu (see Figure 2.29). At any point in time, you can stop the discovery using the **Stop discovery** option in the shortcut menu displayed in Figure 2.29.

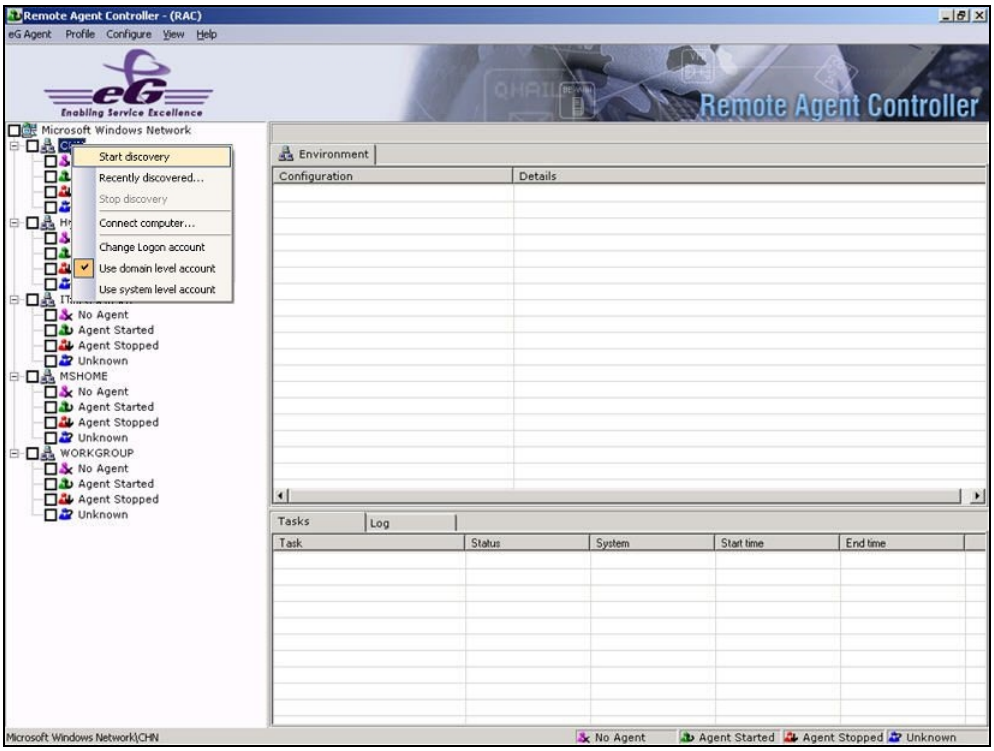

Figure 2.29: Discovery at domain-level

7. To discover the hosts in all the domains, right-click on the topmost node in the tree-structure (in Figure 2.30, this is **Microsoft Windows Network**), and select the **Rediscovering all computers** option from the shortcut menu. At any point in time, you can stop the discovery using the **Stop discovery** option in the shortcut menu displayed in Figure 2.30.

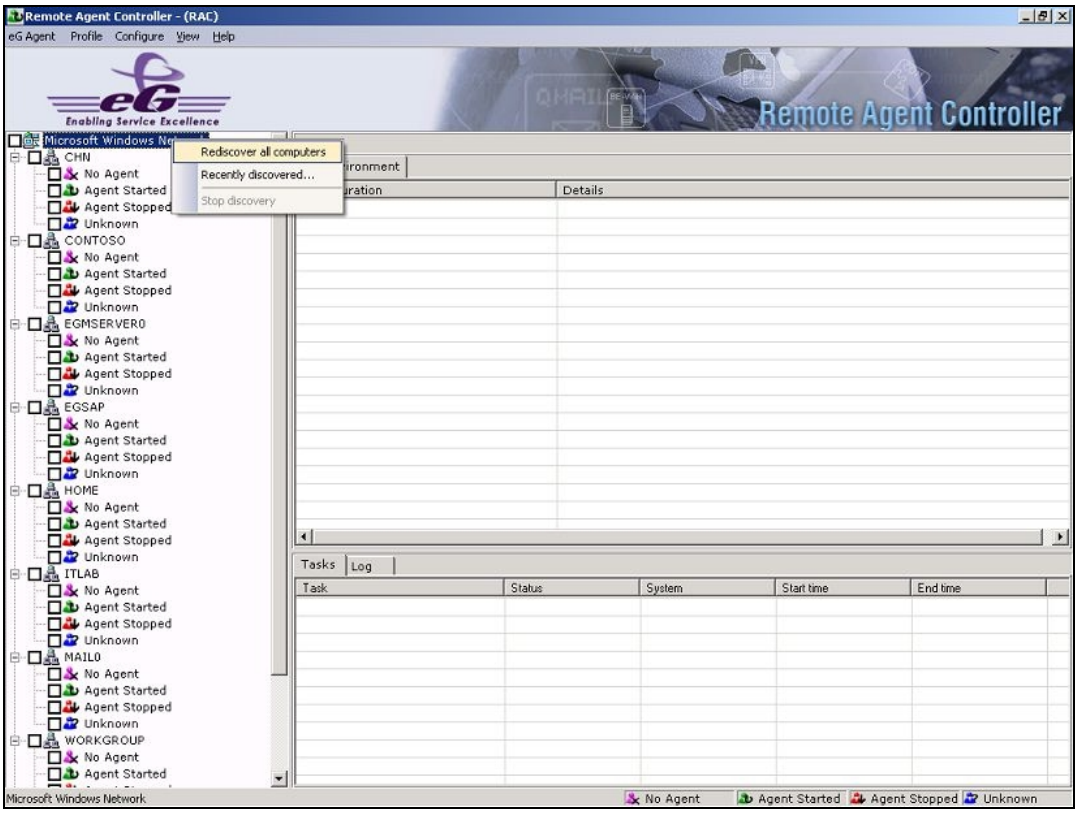

Figure 2.30: Rediscovering all computers

8. When discovery is run for the very first time, by default, all the discovered hosts are grouped under the **Unknown** node in the tree-structure as indicated by Figure 2.31. This is because, by default, RAC does not determine the agent status during discovery.

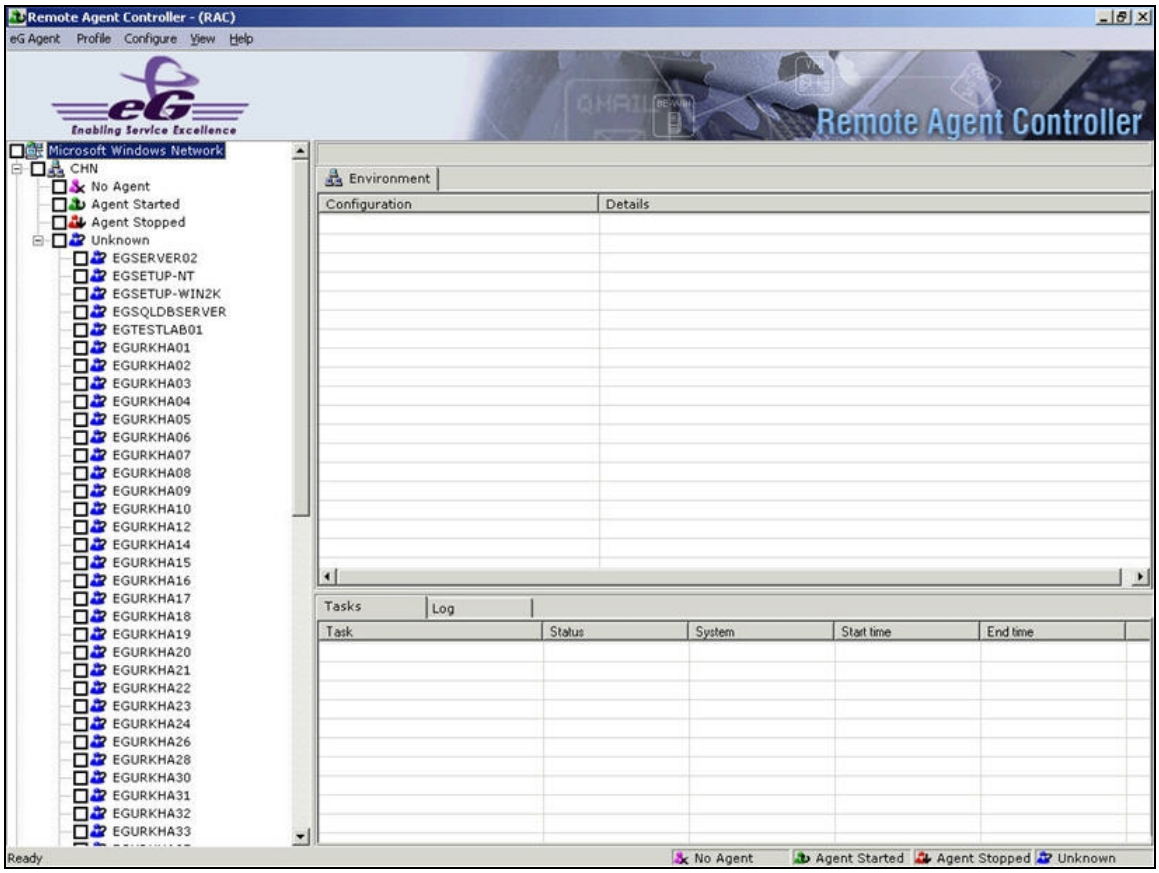

Figure 2.31: All hosts are discovered into the Unknown group

9. Prior to determining the status of agents, you might just want to view the environment information pertaining to specific hosts. To achieve this, select the host from the **Unknown** group, right-click on it, and then click the **Get Environment** option in the shortcut menu (see Figure 2.32). The critical configuration information pertaining to the chosen host will then be made available in the right pane (not shown in Figure 2.32). For more details on how RAC extracts and displays environment information, refer to the Section 3.2 on *Viewing Environment Information*.

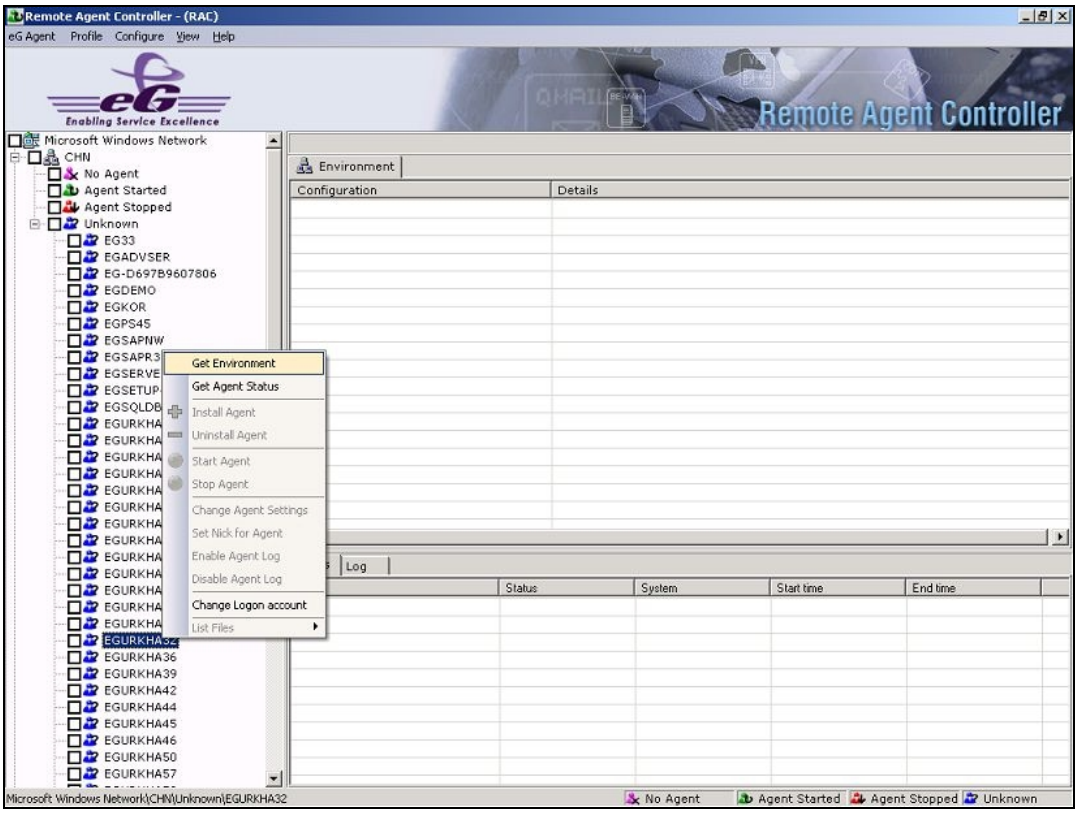

Figure 2.32: Getting environment of a host before discovery

10. If your target environment is small, or if you are looking to determine the status of specific agents alone, then you can attempt to manually retrieve the status information of individual agents. To do so, first, select the agent host from the **Unknown** node in the tree structure, right-click on it, and choose the **Get Agent Status** option from the menu (see Figure 2.33).

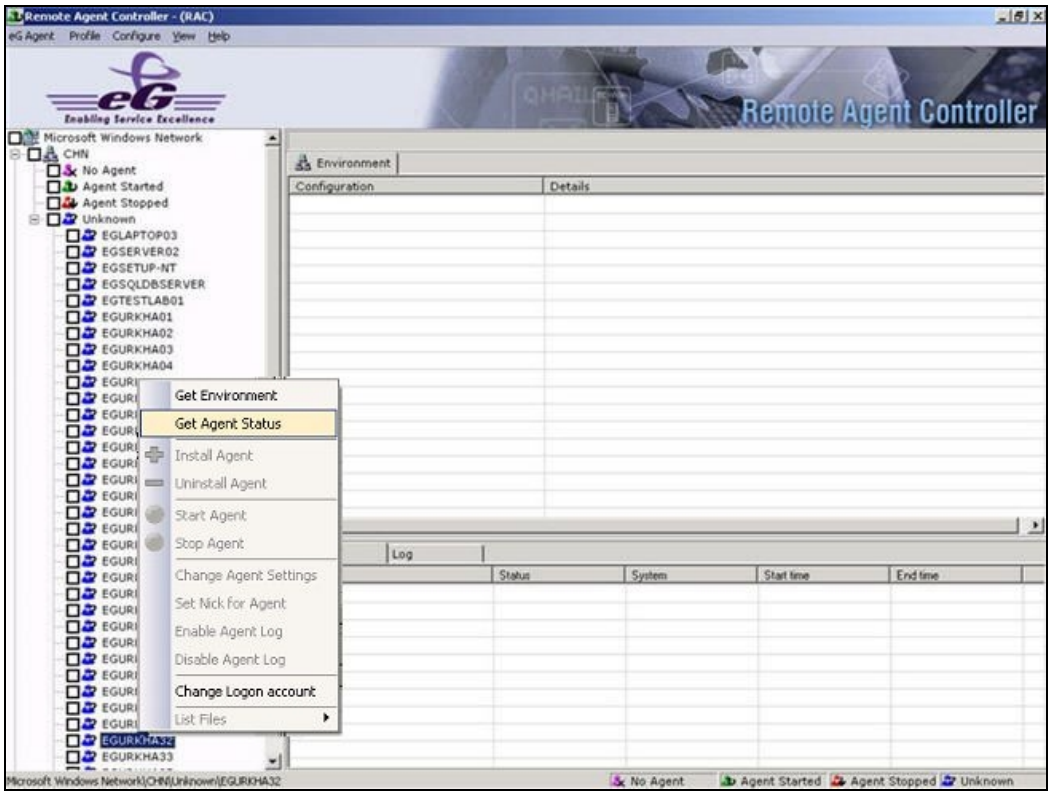

Figure 2.33: Getting the agent status

11. If RAC succeeds in connecting to the chosen host, then it automatically retrieves the agent status and indicates the same by adding the host to the relevant 'status sub-node' (**Agent Started**, **Agent Stopped**, or **No Agent**) (see Figure 2.34).

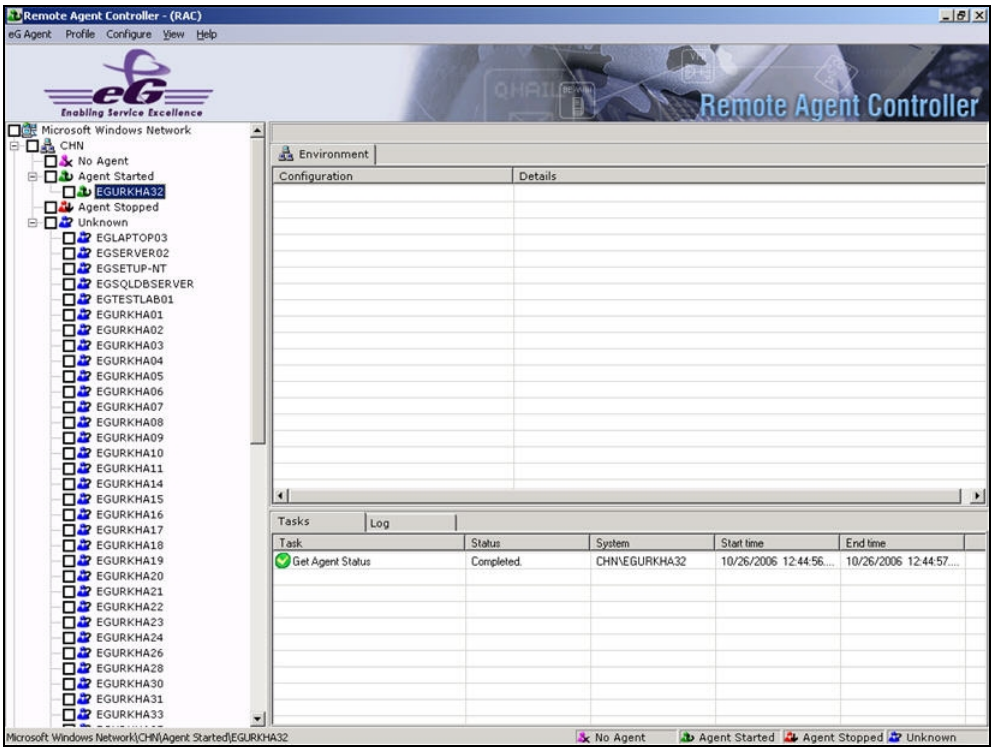

Figure 2.34: The status of a particular agent has been retrieved

12. In a fairly small-sized infrastructure therefore, you can repeat this procedure for connecting to and retrieving status information from individual hosts. However, in large environments comprising of a multitude of components, such a procedure is both cumbersome and time-consuming. Administrators of these environments naturally, would like RAC to discover all the hosts in the environment and the status of the hosts, simultaneously. To ensure this, select the **Preferences** option from the **Configure** menu, click on the **General** option in the left pane of the **Preferences** dialog box, and select the **Find the status of the eG Agent on discovery** check box (see Figure 2.35). By default, this check box is unselected.

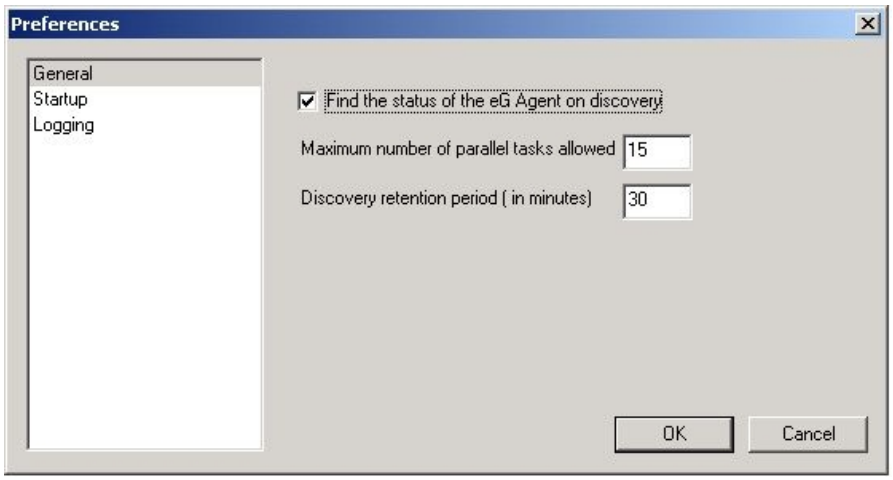

Figure 2.35: Enabling status discovery

13. Then, click the **OK** button to save the changes.

14. If you now attempt to rediscover the hosts in the environment, RAC will not only discover the hosts, but also organize them according to the agent status (see Figure 2.36).

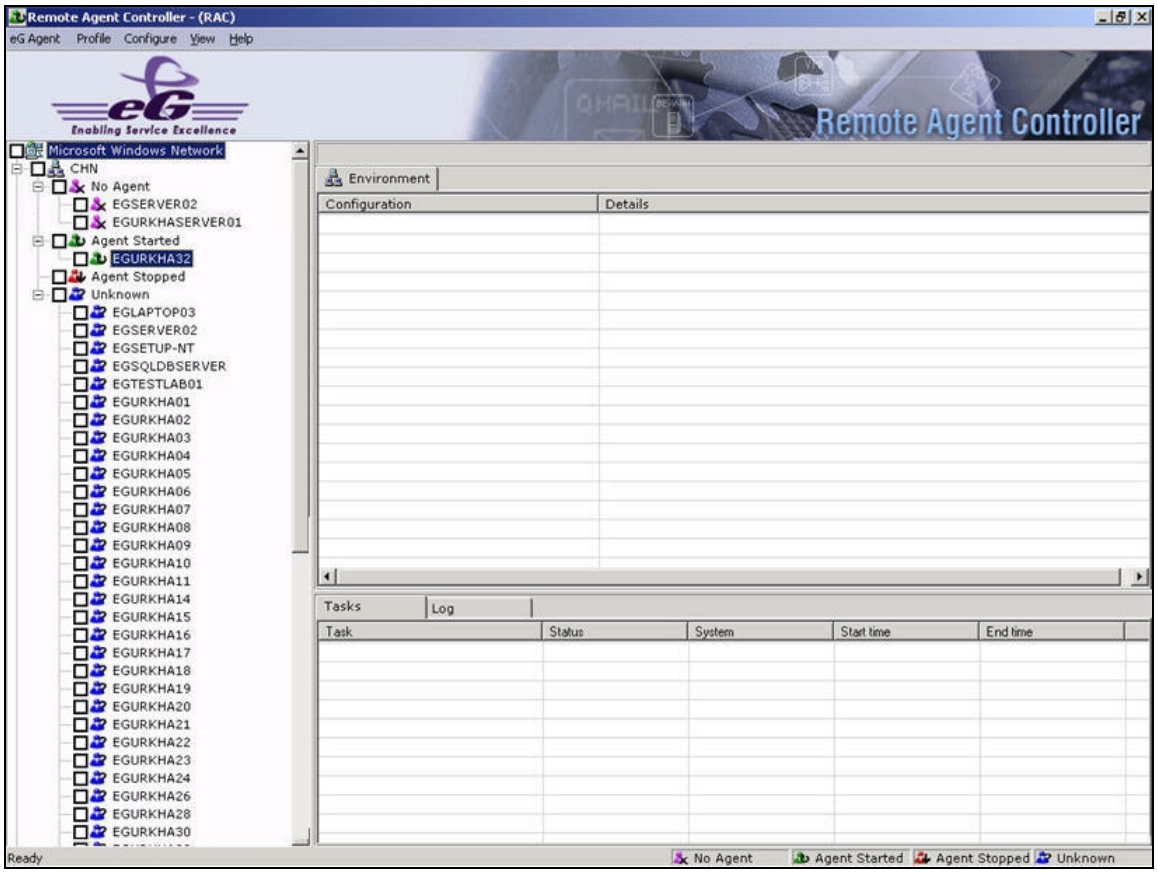

Figure 2.36: Discovering hosts and status

15. Subsequently, you will find hosts grouped under the **No Agent**, **Agent Started** and **Agent Stopped** nodes. Besides the above, some domains also include a node named **Unknown**. The **Unknown** group typically includes hosts to which RAC is unable to connect. Normally, RAC will not be able to connect to a host under the following circumstances:

    a. RAC uses the hidden shares – **Admin$** and **IPC$** - for performing the remote control activities. While the **Admin$** facilitates the discharge of administrative duties, the **IPC$** allows inter-process communication. If these hidden shares are disabled on a target host, then RAC cannot establish a connection with that host.

    b. If the user executing RAC does not have access to a host, then such a host cannot be accessed by RAC.

16. If situation (i) applies, then all you need to do is to enable the **Admin$** and **IPC$** shares on the respective hosts, and start discovery again to have these hosts discovered. To enable the shares,

use the **net share Admin$** and **net share IPC$** commands from the command prompt of the corresponding host.

17. Situation (ii) implies that the login user of the RAC host does not have access to a few systems in the target infrastructure. Owing to the lack of access privileges, the discovery process could not discover the exact status of the agent hosted by those machines. To ensure that RAC has the right to access all the hosts in a domain, you will have to logout of the RAC host, login once again as the **domain administrator**, start RAC, and then start discovery. Alternatively, you can switch logins from RAC itself using the **Change Log on account** option provided by RAC. This option can be used at the domain-level and/or the system-level.

18. In order to enable RAC to connect to almost all the hosts in a domain, you will have to use the **Change Log on account** option at the domain-level. To achieve this, first, select the node representing the domain from the tree-structure in the left pane, right-click on the domain, and choose the **Change Log on account** option from the menu (see Figure 2.37).

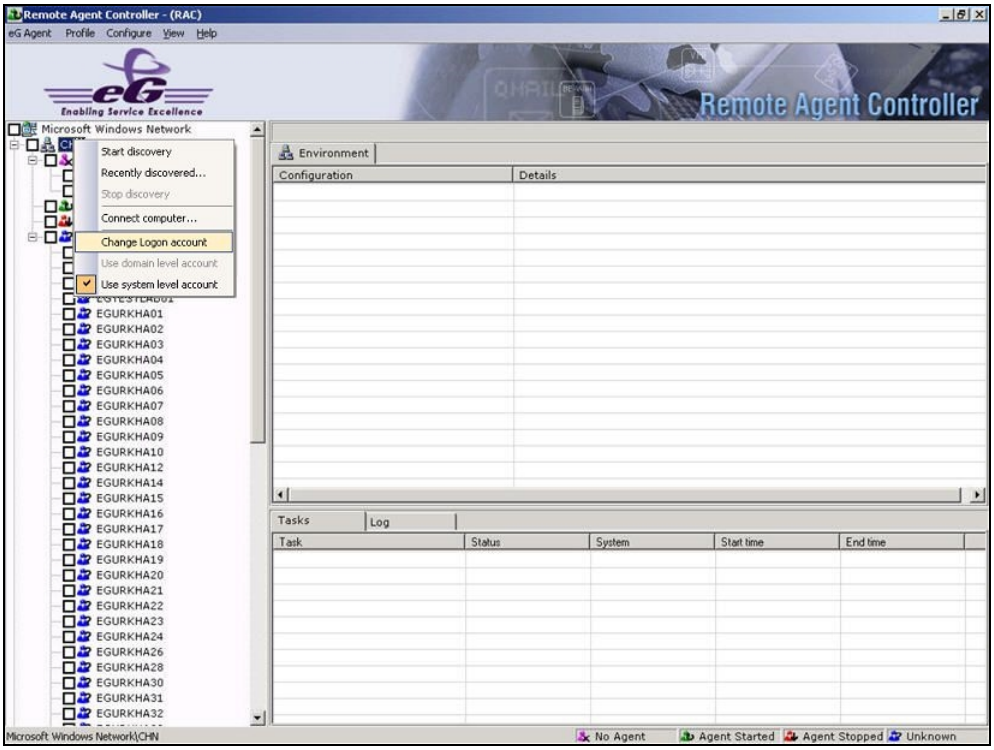

Figure 2.37: Selecting the Change Log on account option at the domain-level

19. Figure 2.38 will then appear, using which the login credentials of the domain administrator can be provided.

Figure 2.38: Specifying the login credentials of the domain administrator

20. Once you change the logon account, proceed to rediscover the hosts in that domain using the **Start discovery** option from the shortcut menu that appears upon right-clicking the domain name (see Figure 2.29).

21. During rediscovery, RAC will attempt to login to each of the hosts in the domain using the login credentials that were set at the domain-level. Once discovery completes, the hosts which RAC can now access are automatically removed from the **Unknown** list and moved to one of the other groups according to the agent status (see Figure 2.39).

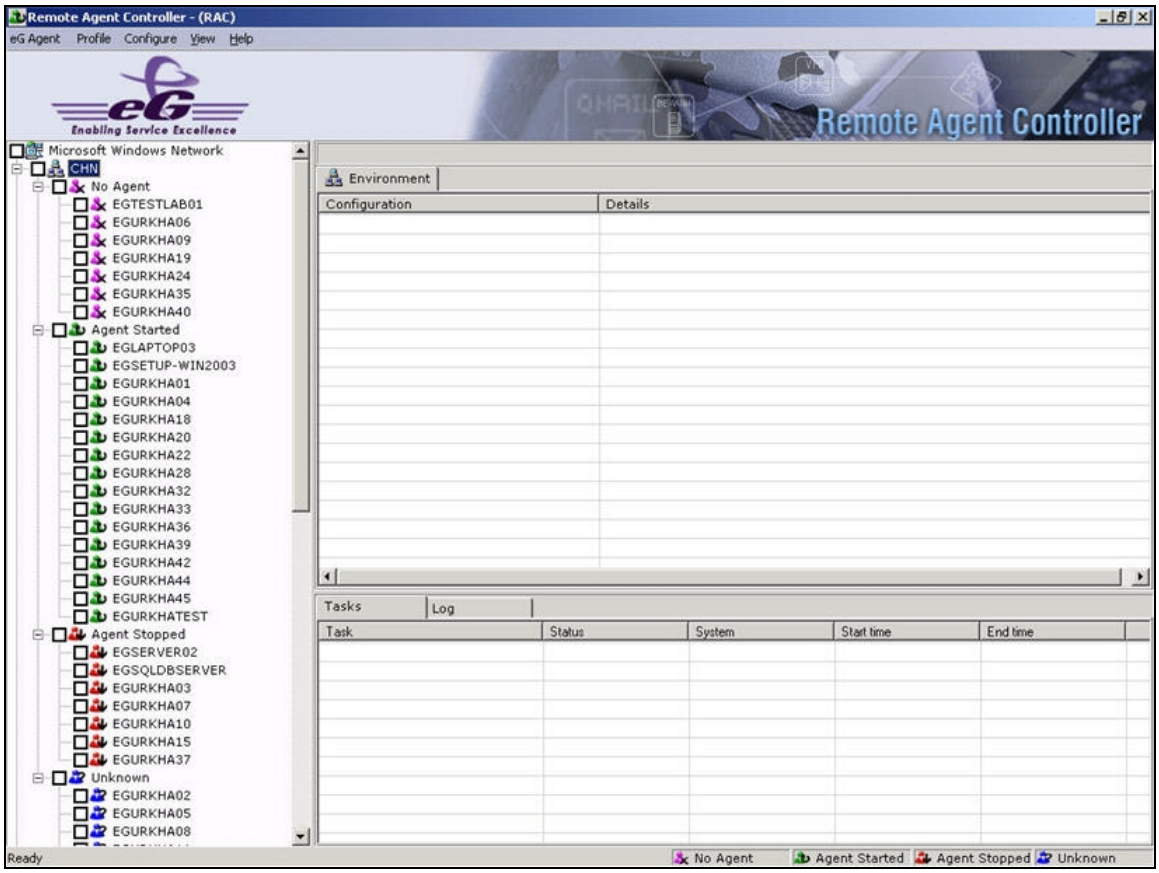

Figure 2.39: The hosts in the Unknown group moved to other groupings

22. On the other hand, if you need access to only specific hosts in the **Unknown** list, then it is recommended that you use a system-level user account, instead of a domain-level account. A system-level account refers to a user account that has the right to access a particular system/host only, and not the entire domain. To define a system-level account, first, select a particular host from the **Unknown list**, right-click on it, and then pick the **Choose Log on account** option (see Figure 2.40).

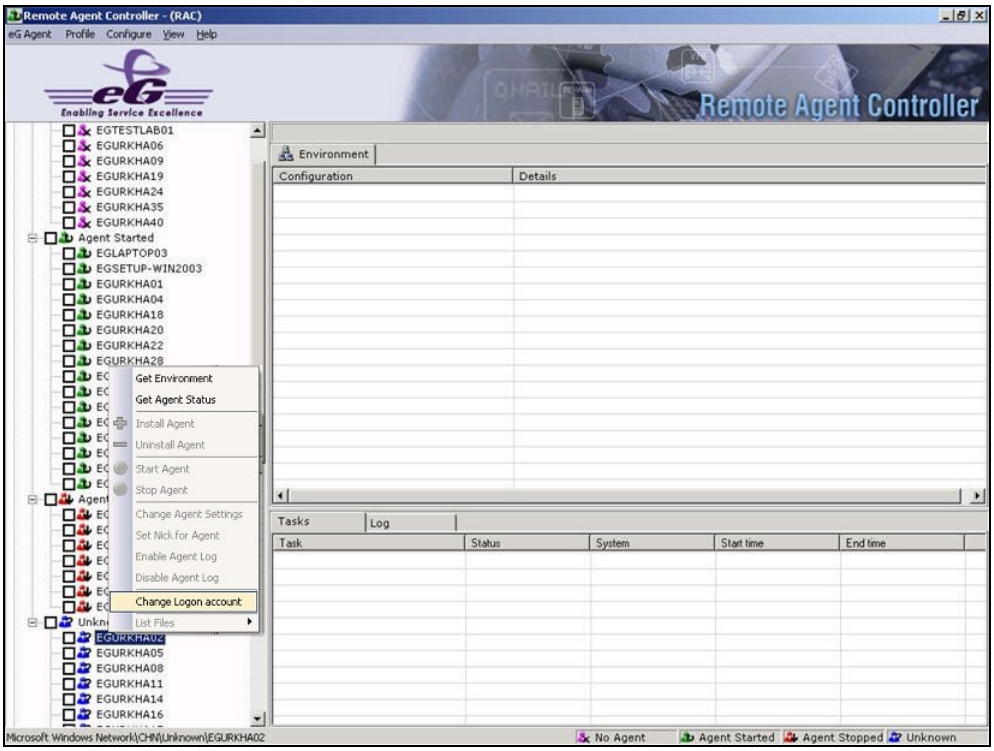

Figure 2.40: Using the Change log on account at the system level

23. Figure 2.41 will appear where valid credentials for logging into the chosen host need to be provided.

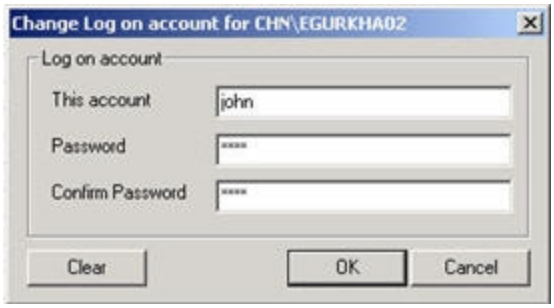

Figure 2.41: Providing the login credentials for a system-level user account

Note:

To simply get the environment information or agent status from a **Windows 2008** (32-bit or 64-bit) / **Windows Vista** / **Windows 7 / Windows 8 / Windows 2012** host, you may either use a domain administrator account or that of any valid user to that system.

However, prior to remotely installing, starting, stopping, or uninstalling an eG agent on any of the above systems, it is mandatory that you choose the **Change Log on account** option at the system-level, and make sure that the credentials you provide in Figure 2.41 are that of an *administrator* to that system, and not just a valid system user. In this case, you will also need to make sure that the aforesaid *system administrator* account is added to the **Log on as a service** list of the target Windows 2008/Vista/7/8/2012 host.

24. After the user account is set, as before, run discovery to connect to the host.

25. If a domain-level account as well as a system-level account is available, then RAC uses both the accounts in sequence, during discovery. In other words, whenever discovery is run, RAC first checks for the existence of a system-level account for the hosts in the target environment. If such an account is available, then RAC uses that account to login to the hosts. If no such account is available, then RAC proceeds to check for the existence of a domain-level account. If a user account has been defined at the domain-level, then RAC uses the credentials of the account to communicate with the hosts in the domain. If you so desire, you can instruct RAC to use only the system-level account while discovering the hosts in a domain. To do so, select the domain node from the tree-structure in the left pane, right-click on it, and select the **Use system level account** option (see Figure 2.42). When this is done, a 'tick' mark appears against the **Use system level account** option, indicating that only the system-level account will be used during discovery (see Figure 2.43). To disable this option later, just select it once again from the shortcut menu of Figure 2.43.

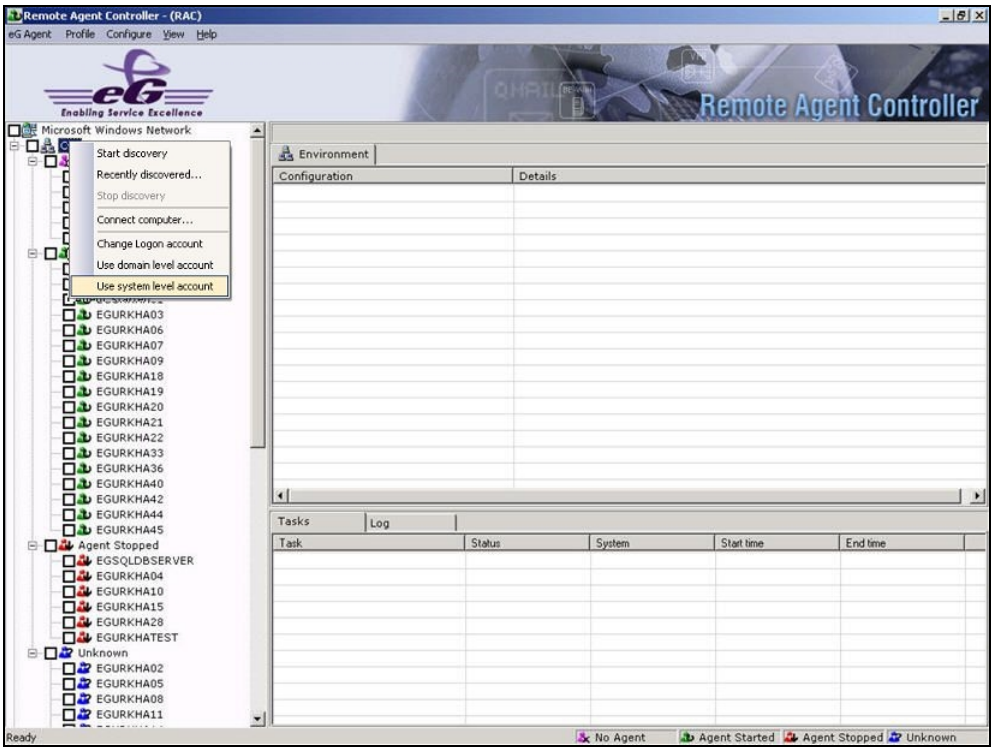

Figure 2.42: Using the system level account

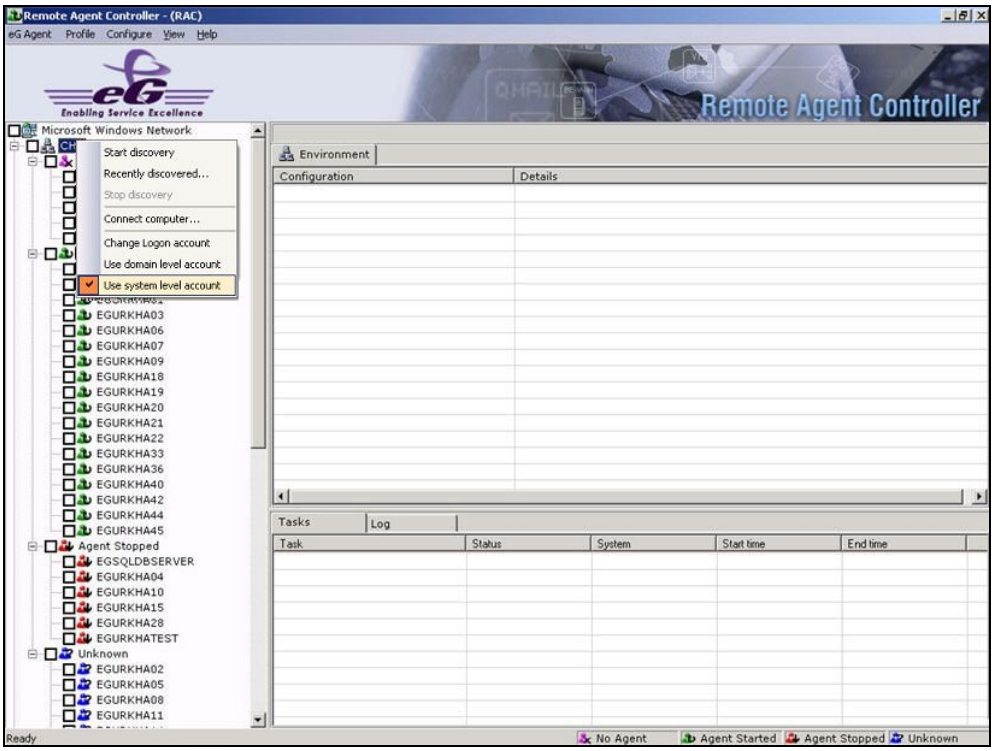

Figure 2.43: The tick mark against the system level option

26. Similarly, to enable only the domain-level account, select the **Use domain level account** option from the shortcut menu in Figure 2.44. Doing so ensures that a 'tick' mark appears against the **Use domain level account** option (see Figure 2.44). This indicates that all subsequent discoveries performed using RAC will use only the domain-level account for connecting to the hosts. To disable this option later, just select it once again from the shortcut menu of Figure 2.44.

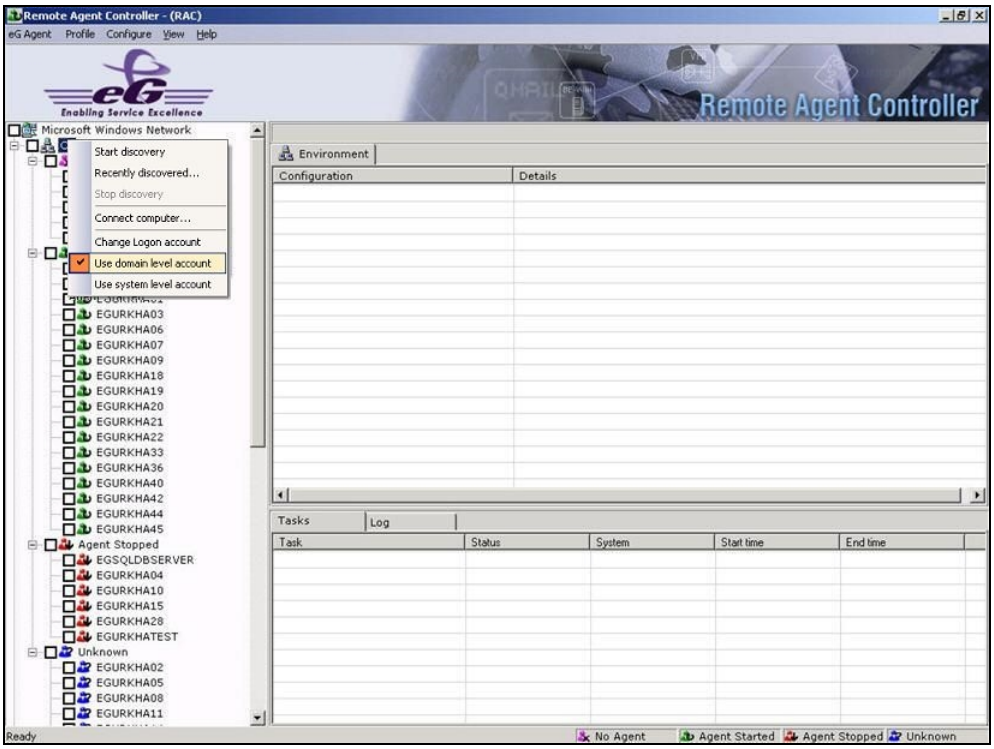

Figure 2.44: The tick mark against the domain-level option

27. Also, note that as soon as a domain-level or system-level account is defined, the corresponding "**Use . . .**" option automatically gets selected. Accordingly, if both domain-level and system-level accounts are present, then both the "**Use . . .**" options will be selected. If neither of these options is selected, then the access rights of the current RAC user will automatically apply during discovery.

Note:

RAC can discover across domains, but it can extract agent status information and other critical environment information from the hosts in only those domains that have a "trust relationship" with the RAC domain. Therefore, the hosts in a domain that does not have a trust relationship with the RAC domain will appear in the **Unknown** list only. To be able to connect to such hosts, you will have to set a user account at that domain-level or at the system-level of the individual hosts, and then rediscover the hosts in that domain.

2.7 Retrieving Recently Discovered Hosts

If, after discovering a number of hosts and their status, you inadvertently or otherwise exit RAC, then, upon logging back in, you would retrieve at least a few of the hosts that you last discovered using RAC, so that you do not spend too much time rediscovering. To achieve this, as soon as you start RAC, select the domain to which the hosts that you last discovered belong, right-click on the domain name, and choose the **Recently discovered** option from the shortcut menu (see 2.7).

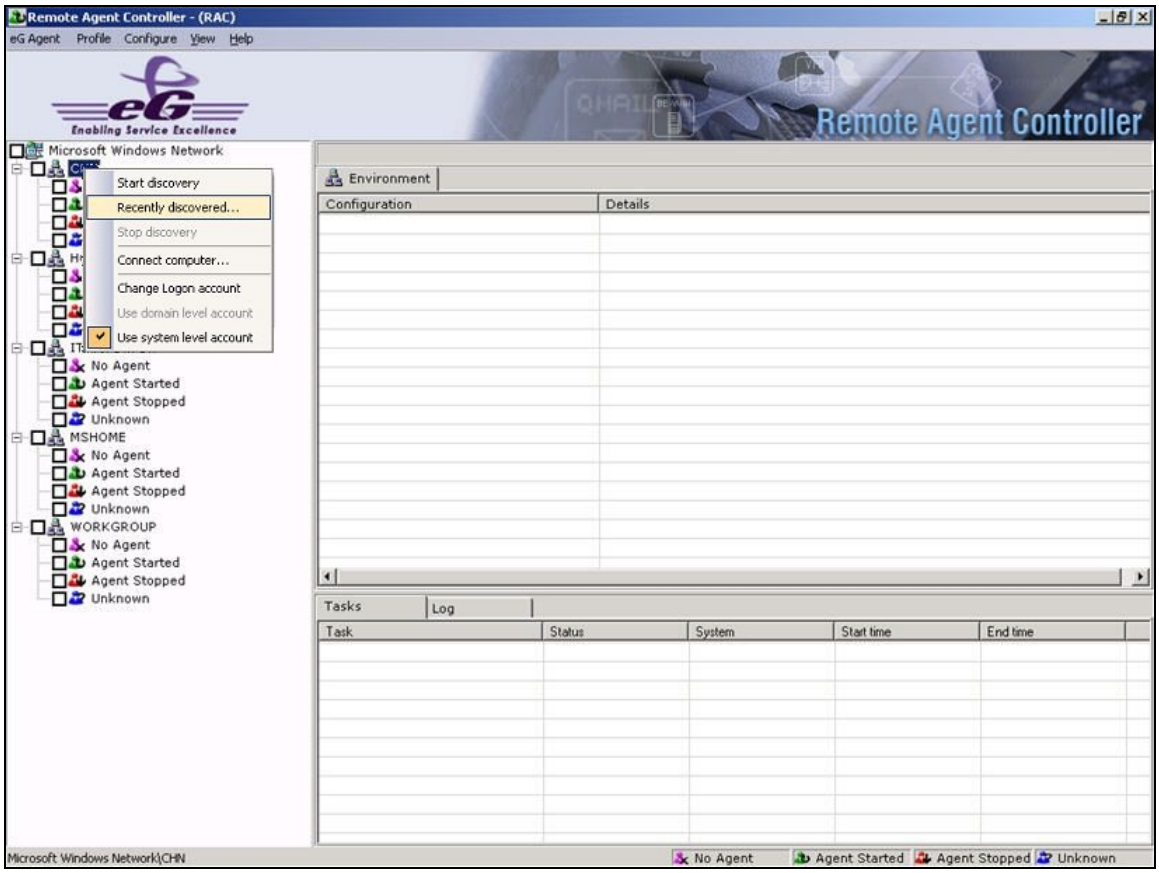

Figure 2.45: Retrieving last discovered hosts

If only 30 minutes have elapsed since you discovered the hosts, then, selecting the **Recently discovered** option enables RAC to quickly retrieve such hosts and group them according to their status (see Figure 2.46).

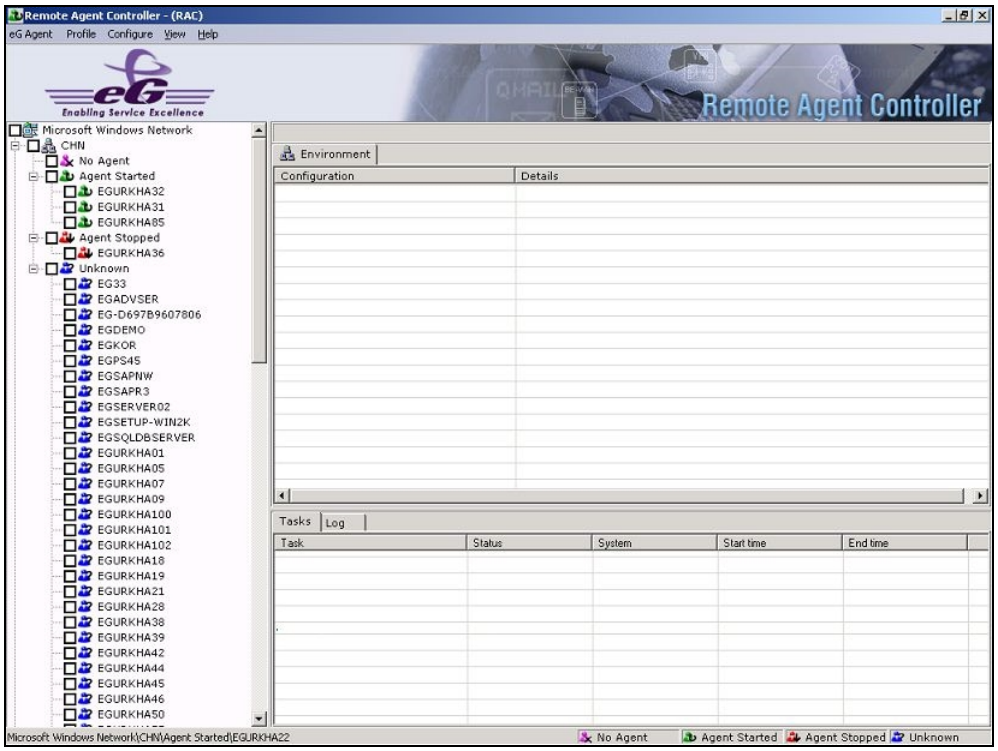

Figure 2.46: Retrieving the status of specific hosts

This is because, by default, RAC can retrieve the status information of only those hosts that were discovered half an hour ago. Any host that is discovered prior to the default duration, will have to be discovered yet again by running a rediscovery routine on the entire domain/across domains, or using the procedure discussed by Figure 2.33 and Figure 2.34 above. This default duration however, can be overridden. To do so, follow the Configure -> Preferences menu sequence, and reset the **Discovery retention period (in minutes)** displayed therein (default: 30) (see Figure 2.37). For instance, if you want the **Recently discovered** option to fetch the status of hosts that were discovered 1 hour ago, then set the retention period to **60** minutes.

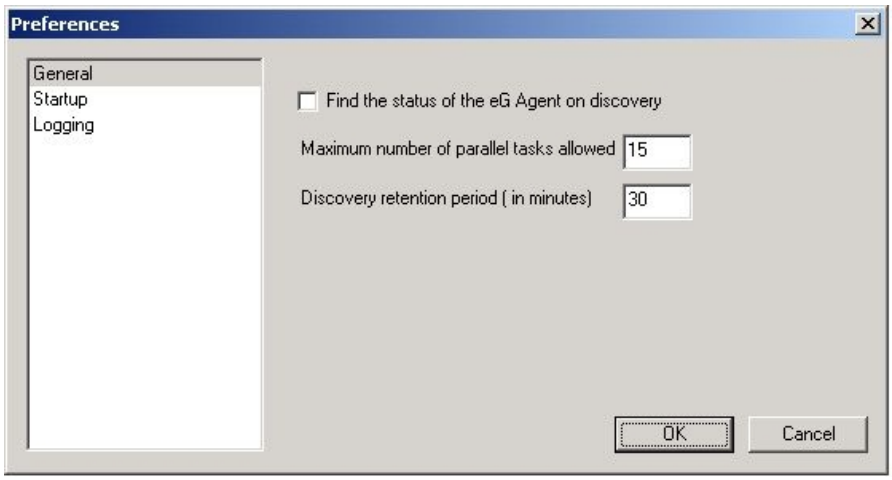

Figure 2.47: Specifying the discovery retention period

2.8 Viewing Environment Information

After discovering the target hosts, it is essential to determine whether the probable agent host fulfills the hardware and software pre-requisites for agent installation. In order to enable users to ascertain this, RAC allows users to connect to individual servers in the target environment, and obtain critical environment information from them. To do this, follow the steps given below:

1. In the tree-structure of the RAC console, hosts grouped under the **No Agent** node represent the probable hosts for agent installation. To view the information pertaining to one such host, select it, right-click on it, and select **Get Environment** from the shortcut menu (see Figure 2.48).

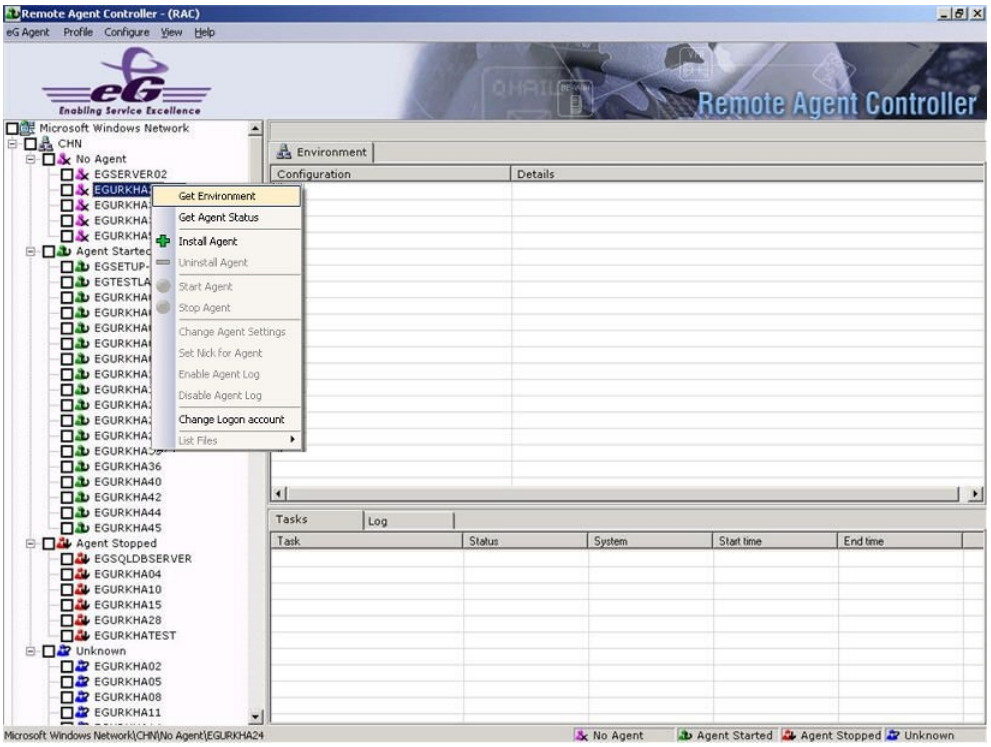

Figure 2.48: Getting the environment information of a host without any agent installed on it

2. Once an operation is triggered using RAC, Figure 2.49 appears indicating that the chosen operation (i.e., **Get Environment**, in this case) is in progress.

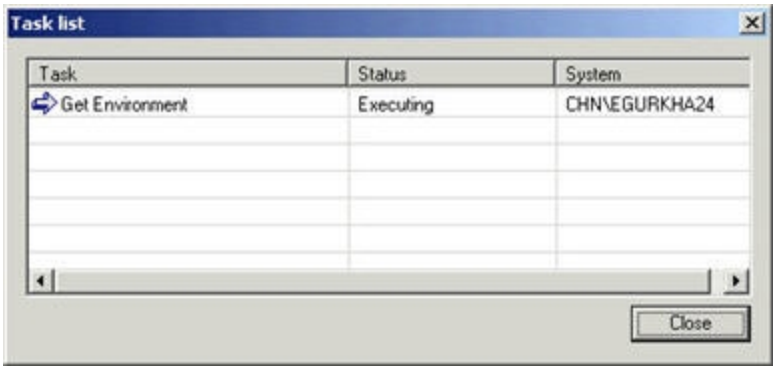

Figure 2.49: A dialog box indicating the progress of an operation

3. If the operation is successful, then the output of the operation will appear in the right pane of the RAC console. Accordingly, if RAC successfully reads the environment information of the host, then the details so extracted will be displayed in the right pane of the RAC console (see Figure 2.50). Also, the **Tasks** list at the bottom of the right pane will indicate the success/failure of the

operation Figure 2.50.

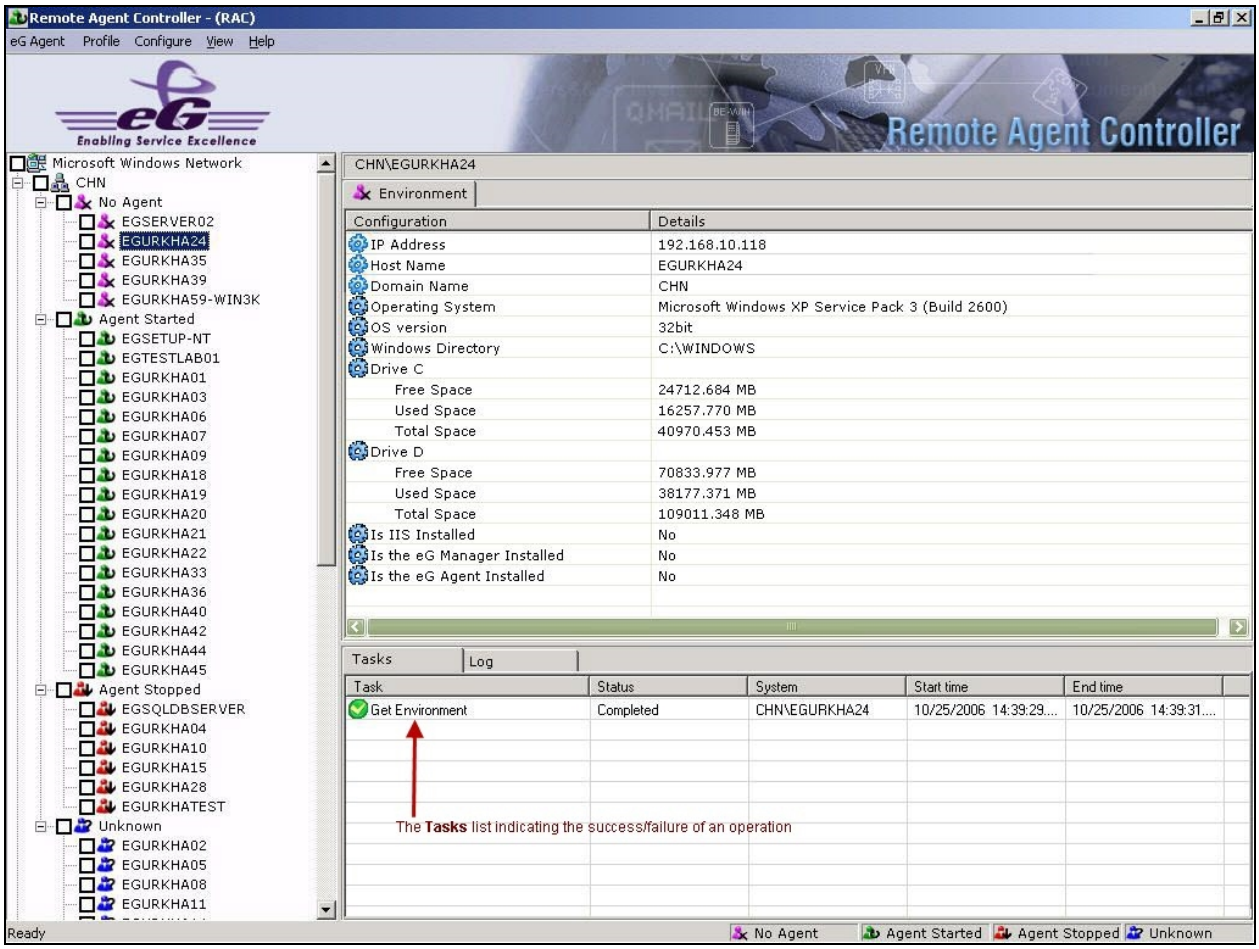

Figure 2.50: Environment information of the chosen host

4. Using the **Get Environment** option, RAC retrieves the following information about a probable agent host (see Figure 2.50):

   - Operating system of the host
   - The operating system version – i.e., whether 32-bit or 64-bit
   - The Windows directory of the host
   - Disk usage details for every disk drive on the host
   - Whether IIS is installed on the host or not
   - Whether an eG agent has been installed on the host or not
   - Whether an eG manager has been installed on the host or not

Using this information, you can ascertain whether a chosen system is qualified to host an agent, and then proceed to install an agent on it.

5. Similarly, to view the details pertaining to a system that already hosts an agent, expand the **Agent Started** or the **Agent Stopped** node in the tree-structure, select a host from within, right-click on it, and then choose the **Get Environment** option from the shortcut menu. Figure 2.51 will then appear.

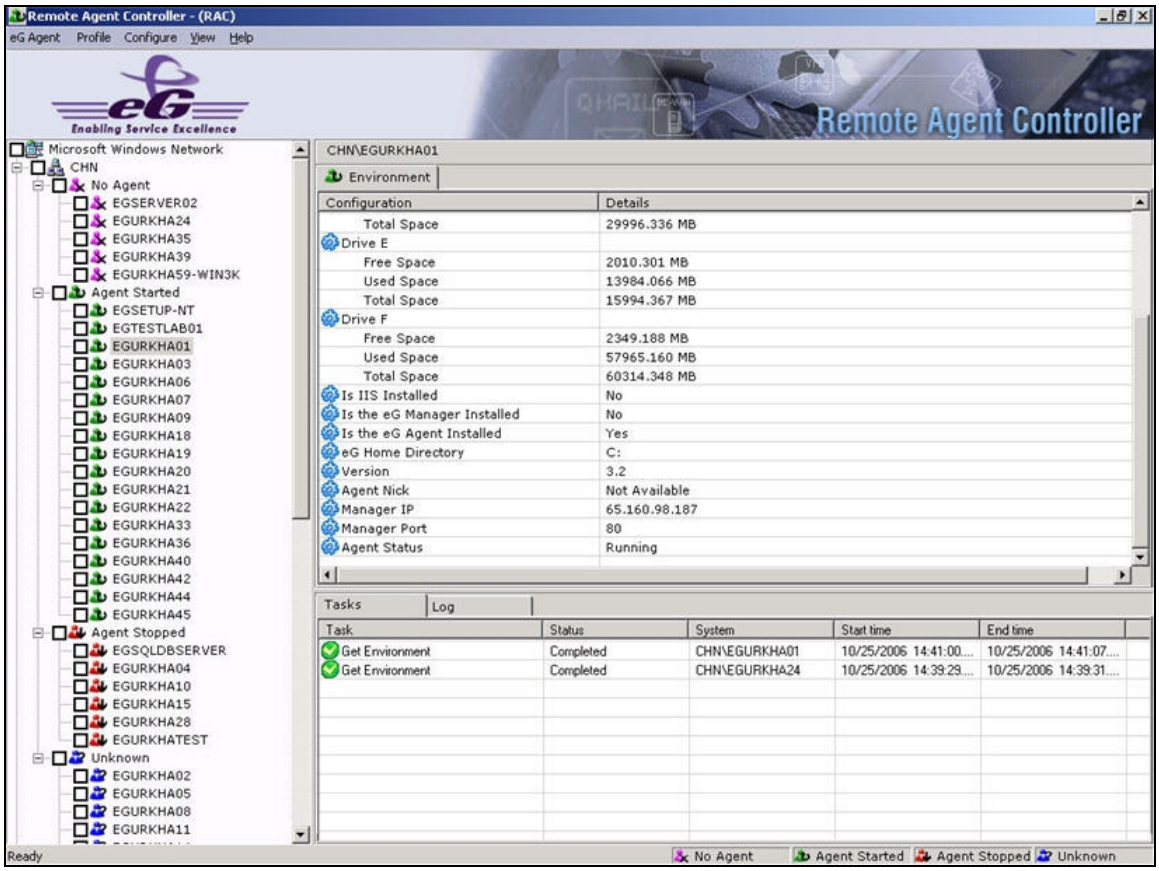

Figure 2.51: Viewing the environment information about a host with an agent on it

6. In the case of hosts where agents pre-exist, the environment information displayed in the right pane will additionally include agent information, such as the agent version, nick name(s) of the agent, the IP of the manager to which the agent reports, the port number of the manager, and the current agent status (whether running or not) (see Figure 2.51).

7. In a domain consisting of limited hosts, it is relatively easy to use RAC to view information about specific hosts. However, in case of large environments characterized by tens of thousands of hosts per domain, the challenges are greater; an RAC user might have to spend hours to locate a

particular host in a domain by scrolling up and down the tree-structure, and then connect to it. In order to enable the administrators of such environments to quickly locate specific hosts and instantly connect to them, RAC provides the **Connect computer** option. To use this option, select the domain to search from the tree-structure, right-click on it, and then select the **Connect computer** option from the pop-up menu (see Figure 2.52).

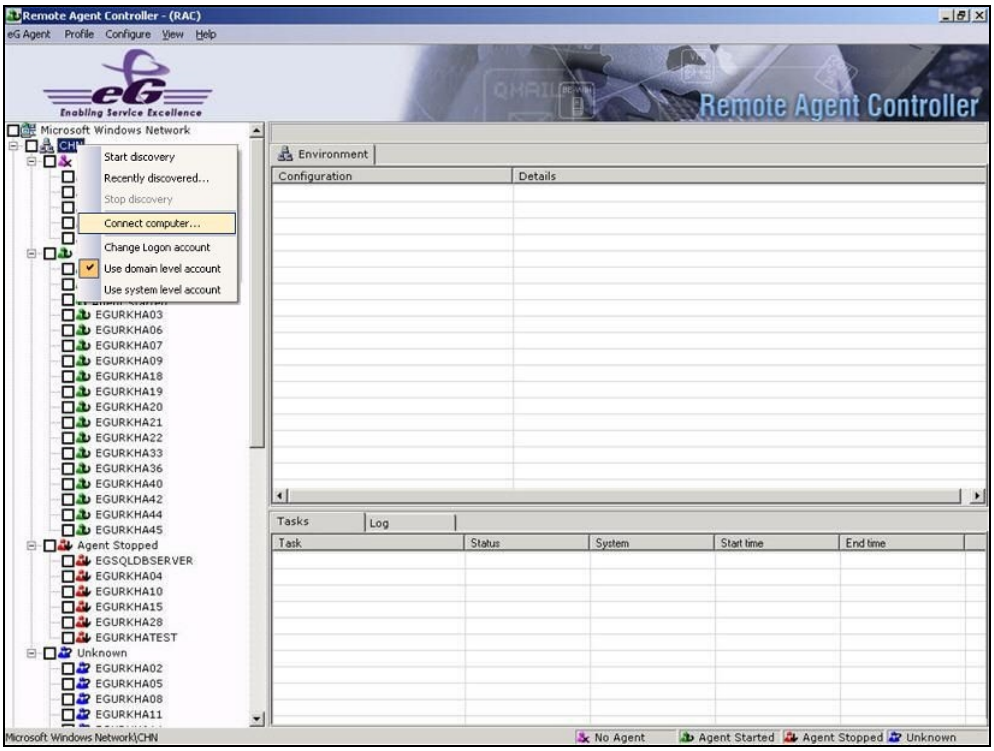

Figure 2.52: Selecting the Connect Computer option

8. When Figure 2.53 appears, provide the **Computer name** to search for, and then specify the user name and password using which RAC needs to connect to that computer. Finally, click the **OK** button.

Figure 2.53: Providing the details of the computer to locate

9. Once the **OK** button is clicked, RAC will begin searching for the specified computer. If found, control will automatically shift to that computer name in the tree-structure (see Figure 2.54). You can then use the **Get Environment** option to view the configuration information about the located host.

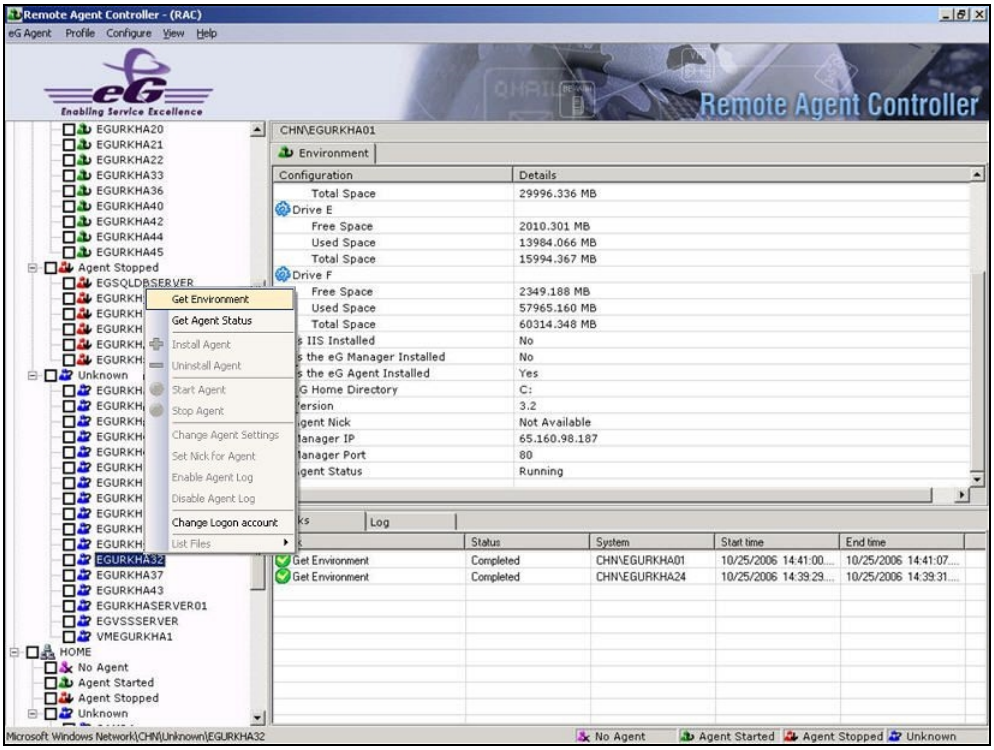

Figure 2.54: Viewing the information pertaining to the located computer

2.9 Defining Profiles

After viewing the information pertaining to a host in the **No Agent** list, one can figure out whether the host fulfills the pre-requisites for agent installation, and which disk partition has adequate free

space to support an agent. A profile can then be set accordingly. RAC allows profile definitions which typically comprise of the inputs for agent installation such as the install location, the manager IP/port, whether the agent is to be SSL-enabled or not, whether a Proxy server is required or not, etc. The chief benefit of profile definitions is that once set, a profile can be re-used by all agent installations that share the same input parameters. A profile can be defined either before or during agent deployment. To achieve the above, do the following:

1. Select the **Add/Change Profiles** option from the **Profile** menu on the menu bar of Figure 2.54. Figure 2.55 will then appear, wherein a *default* profile will be listed. The settings defined within this profile, will, by default, apply to all agent installations performed by RAC. By default, RAC creates a directory named **EgInstall** in the C drive of a host and tries to install an agent therein. The **Install Directory** column of Figure 2.55 displays this location only.

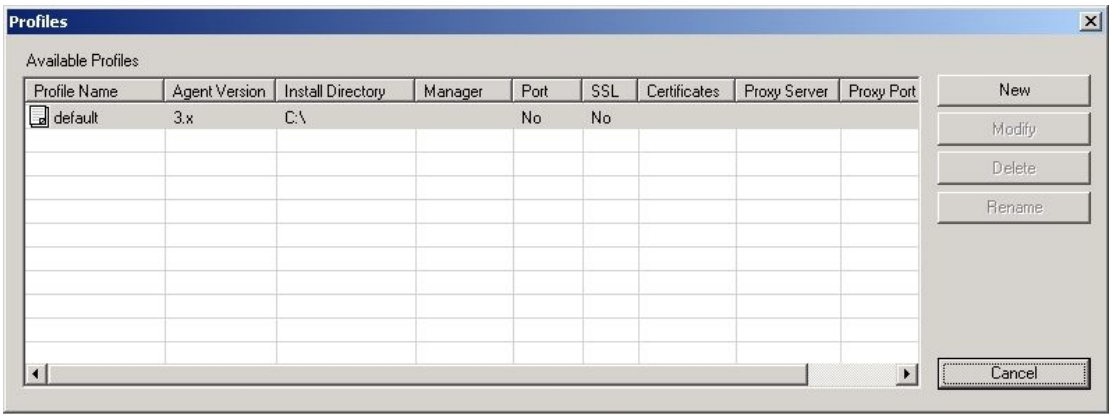

Figure 2.55: The default profile

2. The *default* profile cannot be deleted, but you have to modify the *default* profile so as to configure the IP/host name and Port of the eG manager to which all the eG agents installed using RAC will have to report. Any attempt made to create a new profile without modifying the *default* profile will result in an error that will be displayed in the **Tasks** list in the right pane.
3. To modify the default profile, select the profile from Figure 2.55 and then click the **Modify** button in Figure 2.55.

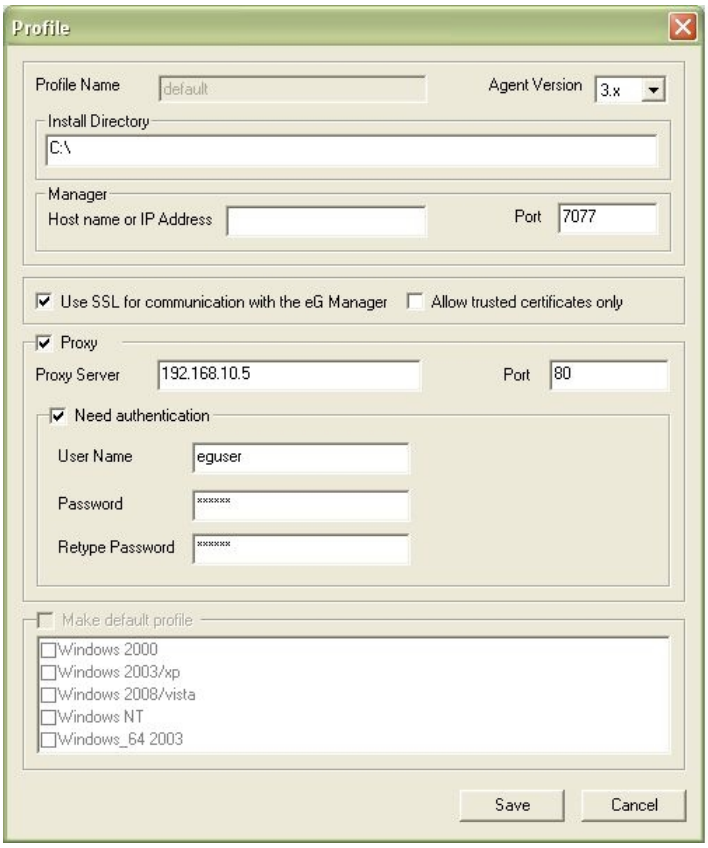

Figure 2.56: Modifying the default profile

4. Figure 2.56 then appears wherein the **Host name or IP address** and **Port** of the eG manager need to be provided. By default, these fields will remain unconfigured for the *default* profile. Remember that the eG manager specification provided here will automatically apply to all the profiles created using RAC. You can change the **Install Directory** for the *default* profile, if so required.

5. Also, from the **Agent Version** list in Figure 2.56, select the version of eG agent that the *default* profile should install on a remote host. By default, *3.x* is the **Agent Version** chosen for the *default* profile. The other options are *4.x* and *5.x*.

   Note:

   While installing a Windows 2008 (32-bit or 64-bit) agent, Windows Vista, Windows 7, or a Windows 2003 64-bit agent, ensure that the **Agent Version** chosen is *4.x* or *5.x* and not *3.x*, as the remote installation will not work otherwise; this is because, the agent installable for version *3.x* does not provide support for Windows 2008 (32-bit and 64-bit), Windows Vista, Windows 7,

or Windows 2003 64-bit platforms. Likewise, when installing a Windows 8/Windows 2012 agent, ensure that the **Agent Version** chosen is only *5.x*; this is because, agents of version *3.x* and *4.x* do not provide monitoring support to Windows 8 / Windows 2012 systems.

6. To automatically SSL- enable the agents to be installed remotely, select the **Use SSL communication with the eG Manager** check box. To ensure that the agent allows only trusted certificates, select the **Allow trusted certificates only** check box.
7. If the agent-manager communication takes place via a proxy server, then the default settings of the Proxy server can be provided in Figure 2.56 by selecting the **Proxy** check box. Doing so will enable the text boxes below the **Proxy** check box, wherein the proxy **Server IP** and **Port** are to be provided.
8. If authentication is required for the proxy server, then enable the **Need authentication** option and provide the **User Name** and **Password** that will be authenticated by the proxy server. To confirm the password, enter it again in the **Retype Password** text box.
9. Save the changes by clicking on the **Save** button in Figure 2.56.
10. Finally, save the changes by clicking on the **Save** button. This will lead to Figure 2.55.
11. If need be, you can configure additional profiles, by clicking on the **New** button in Figure 2.55. Figure 2.57 will then appear, using which the new profile can be created (see Figure 2.57).

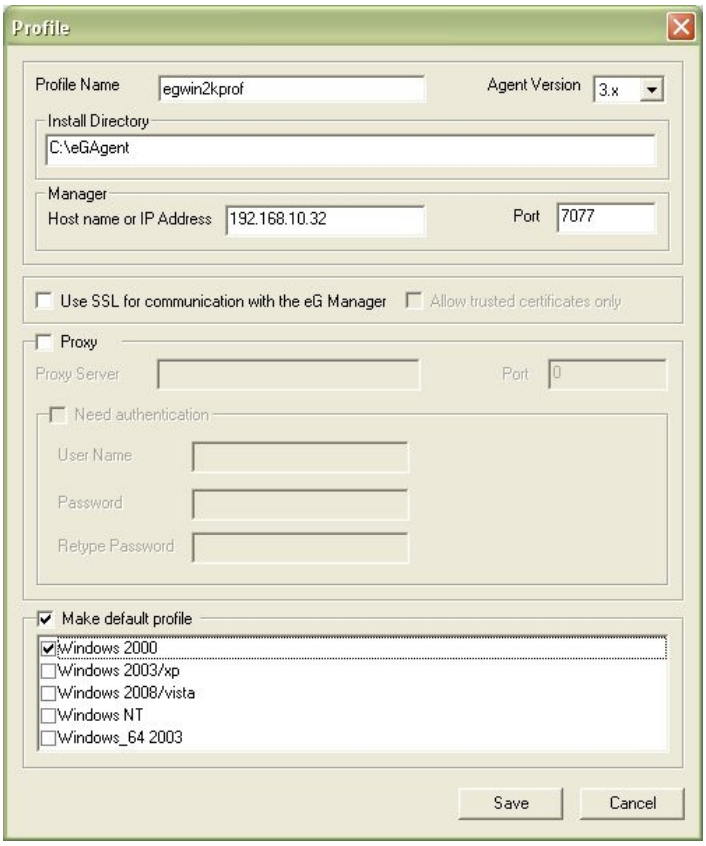

Figure 2.57: Creating a new profile

12. For new profiles, an additional **Make default profile** option is provided (see Figure 2.57). Selecting this check box will allow you to make the newly created profile as the default profile for specific operating systems. To do so, click on the check boxes preceding the required Windows operating systems in Figure 2.57.
13. Finally, click the **Save** button to register the changes.
14. Figure 2.58 will then appear displaying the newly created profile.

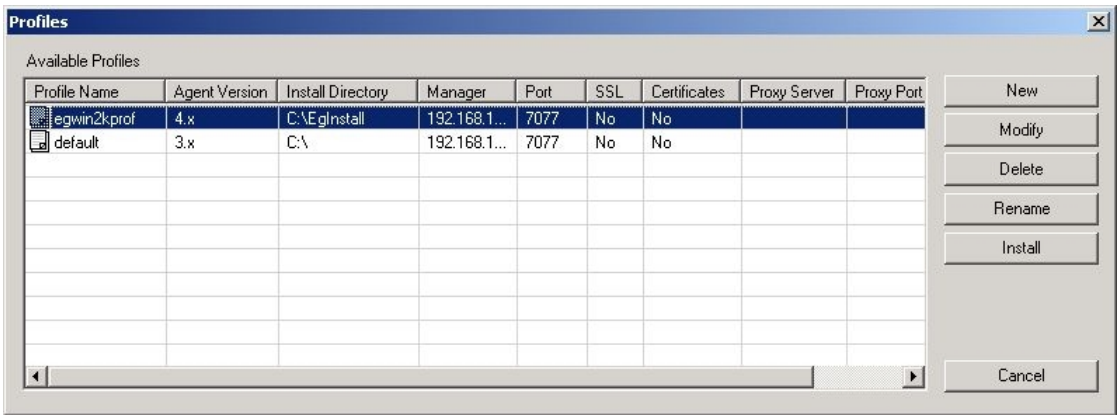

Figure 2.58: Newly created profile being displayed

15. New profiles can be deleted using the **Delete** button and renamed using the **Rename** button in Figure 2.58.

16. Click **Cancel** in Figure 2.58 to return to the RAC console.

2.10 Remotely Installing eG Agents

Once all the pre-requisites listed above are fulfilled, follow the steps discussed below to install an agent remotely using the eG remote agent controller:

1. In the RAC console, you will find that the group that tops the tree structure in the left pane of the console is the **No Agent** group, which lists all the hosts in the domain without agents installed on them. To install an agent on one of the listed hosts, first, select a host from the **No Agent** group, right-click on it, and select **Install Agent** from its shortcut menu (see Figure 2.59).

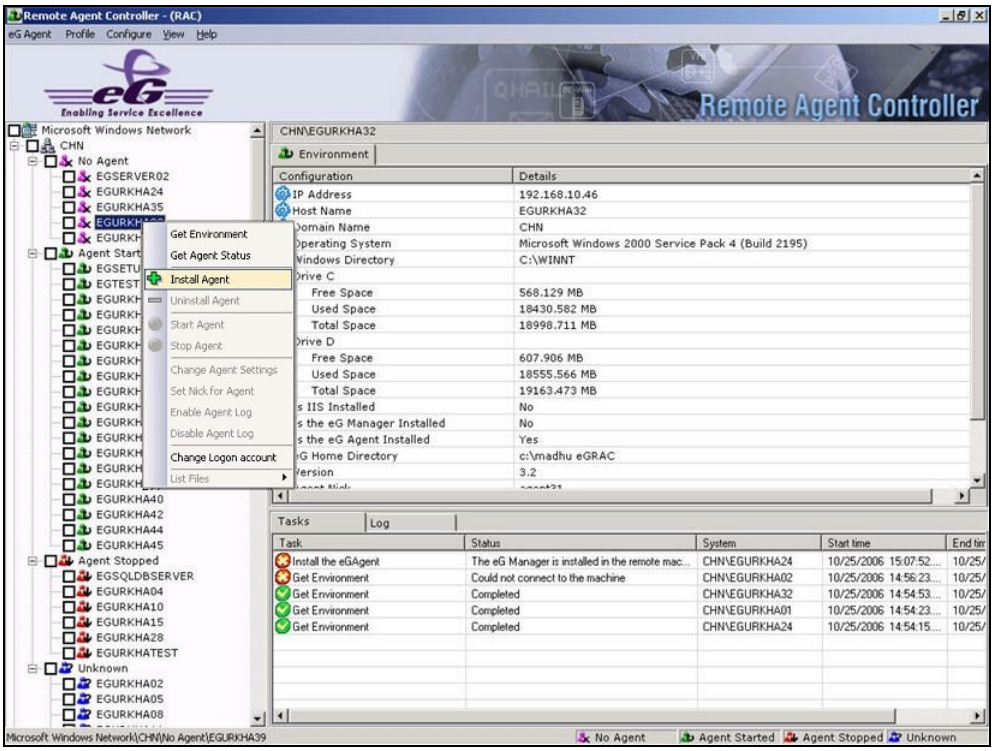

Figure 2.59: Installing an agent

2. RAC then prompts you to confirm agent installation on the chosen host (see Figure 3.33). Click **Yes** here to confirm the installation.

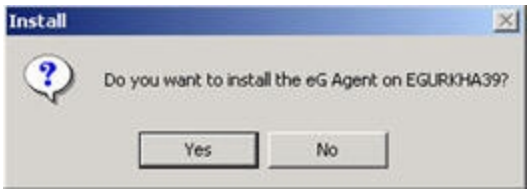

Figure 2.60: A message box requesting your confirmation to install an agent on the chosen host

3. Then, pick a profile from Figure 2.61 that appears. If the operating system on which the agent is being installed has a corresponding default profile specification, then that entry will be automatically 'marked for selection' in the **Profiles** dialog box as depicted by Figure 2.61. At this juncture too, profiles can be added, modified, renamed, or deleted.

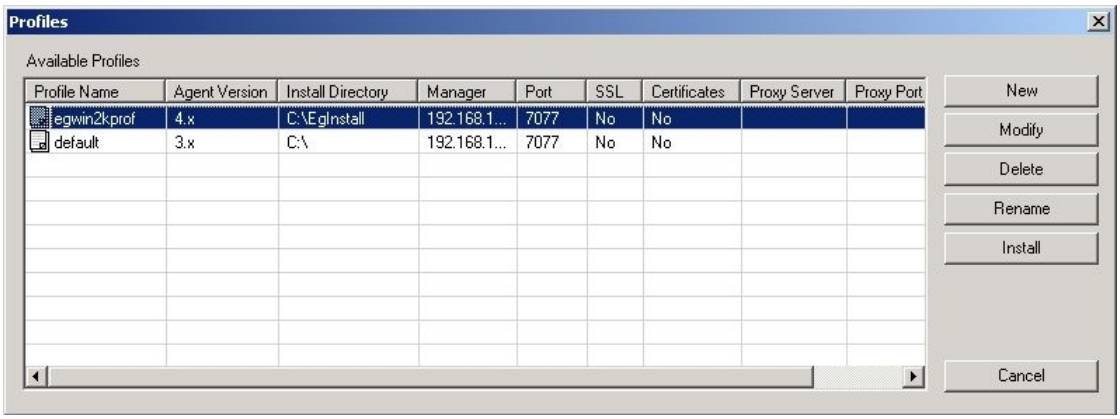

Figure 2.61: List of available profiles

4. Select a profile from Figure 2.61 by clicking on it, and then click on the **Install** button therein to install the eG agent in the location represented by the chosen profile.
5. Once the agent is installed successfully, Figure 2.62 will appear wherein you will find that the host on which the agent has been installed has moved from the **No Agent** node to the **Agent Stopped** node.

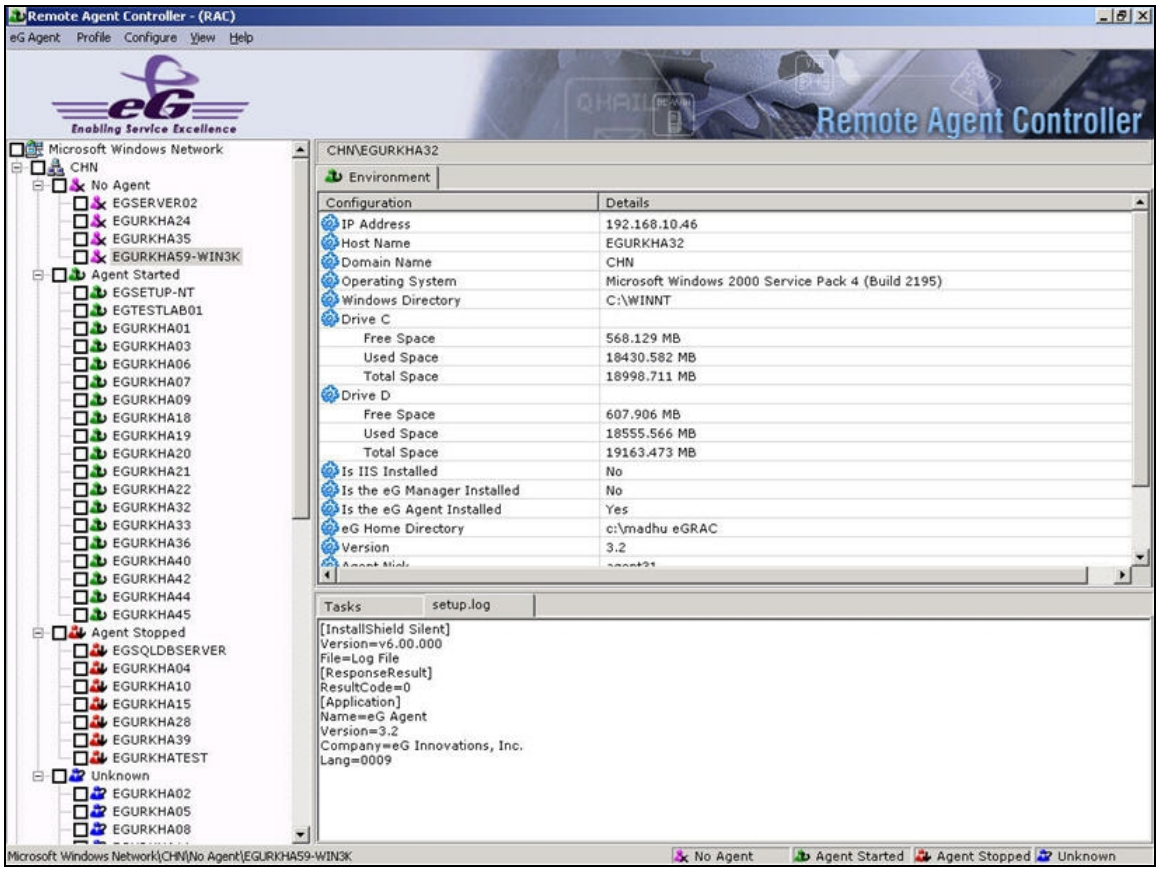

Figure 2.62: The RAC console after agent install

6. The **setup.log** section of the right pane (see Figure 2.62) reports the agent details.

7. Administrators of large infrastructures again are sure to find the individual agent installation rather cumbersome. To cater to their special needs, RAC facilitates multi-tasking. In other words, if you want to install agents on multiple hosts at the same time, you can do so very easily using RAC. To achieve this, first select the targets for installation from the **No Agent** group by clicking on the corresponding check boxes (see Figure 2.63). If all the agents under **No Agent** need to be selected, then simply select the **No Agent** check box. Once the targets are marked, select the **No Agent** sub-node, right-click on it, and choose the **Install Agent** option from the menu (see Figure 2.63).

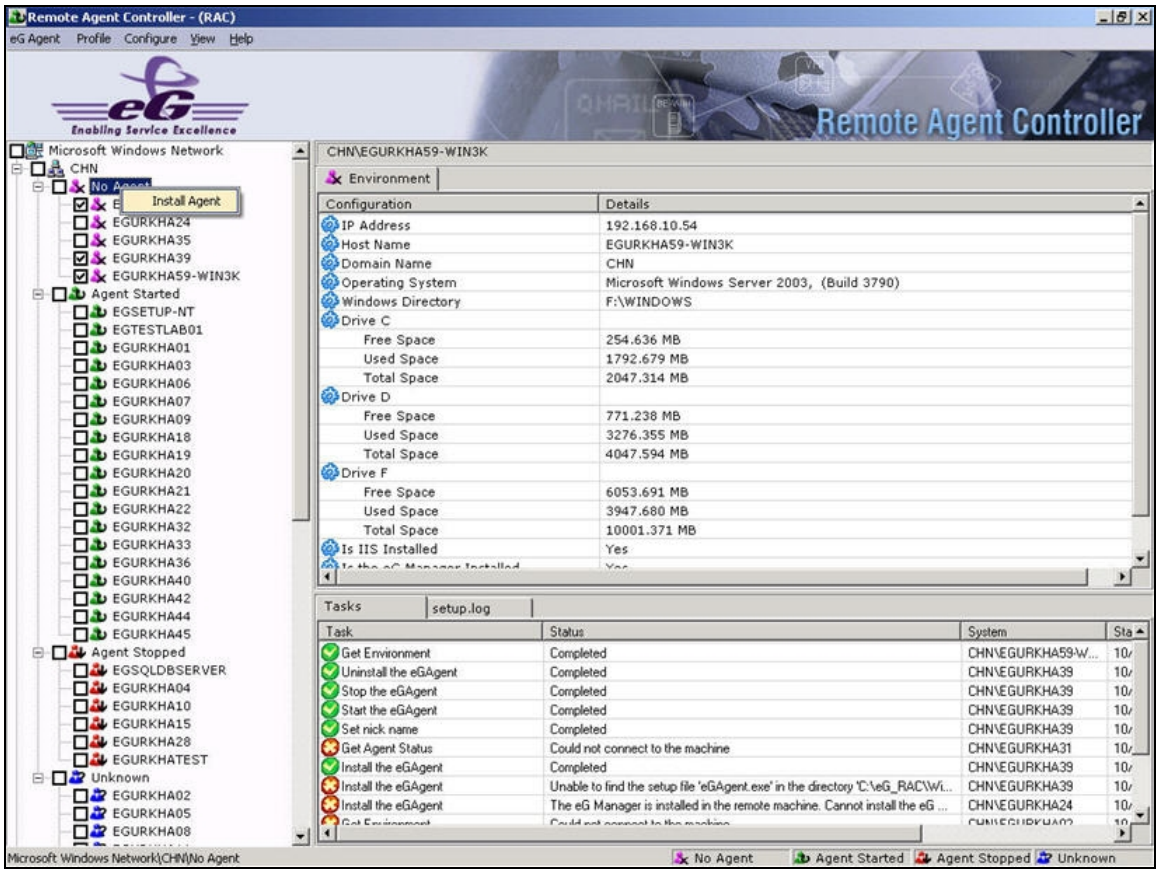

Figure 2.63: Installing agents on multiple hosts simultaneously

8. Figure 2.64 then appears using which you can modify your selection.

9. Right-clicking anywhere within the **Machines** section of Figure 2.64 invokes a shortcut menu that allows you to make quick modifications to the selections (see Figure 2.65).

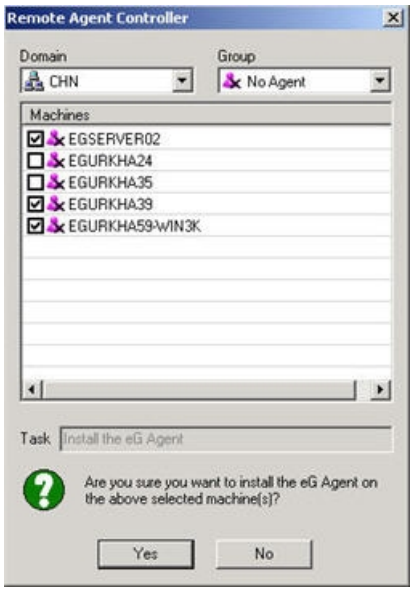

Figure 2.64: Modifying the multiple selection

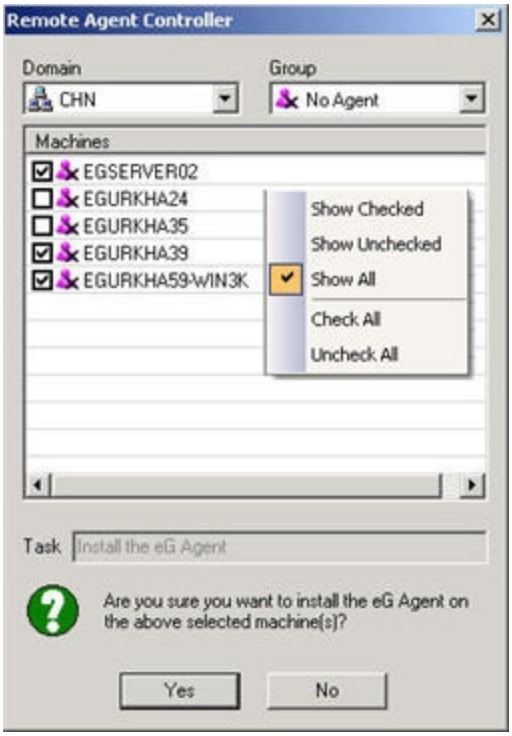

Figure 2.65: Shortcut menu within

10. By default, the **Show All** option is selected in the shortcut menu of Figure 2.65. This indicates that this window, by default, displays all the target hosts under the chosen node (in this case, it is

the **No Agent** node), regardless of whether or not the hosts are marked for installation. To select all the displayed hosts, use the **Check All** option in the shortcut menu of Figure 2.65. To unselect all the displayed hosts, choose the **Uncheck All** option. To view only the selected hosts, use the **Show Checked** option, and for viewing the deselected hosts alone, pick the **Show Unchecked** option.

11. After making the necessary modifications, click on the **Yes** button in Figure 2.65 to begin installing the eG agent on the selected hosts.

12. Next, like every other remote install, select the **Profile** to be used (see Figure 2.66) and click on **Install** to begin installation.

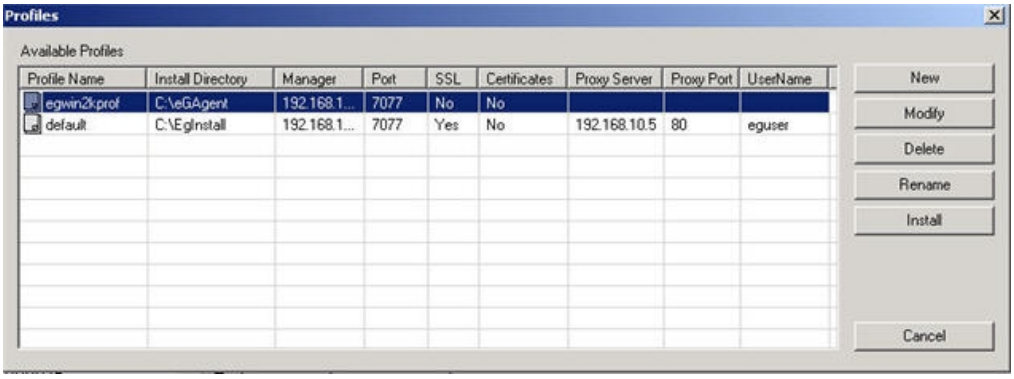

Figure 2.66: Selecting a profile for the multiple installation

13. Similarly, you can start, stop, and even uninstall multiple agents simultaneously.

14. By default, a maximum of 15 parallel tasks can be performed by RAC. You can, if you so desire, change this default value to suit the specific needs of your infrastructure. To do so, first, select the **Preferences** option from the **Configure** menu. Then, select the **General** option from the left pane of the **Preferences** dialog box, and provide a value of your choice in the **Maximum number of parallel tasks allowed** box (see Figure 2.67).

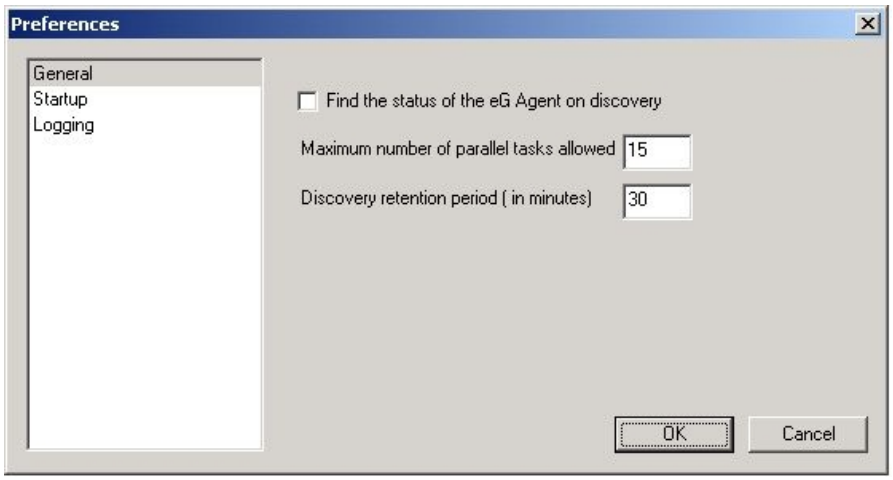

Figure 2.67: Specifying a value for the number of parallel tasks permitted

15. Finally, click the **OK** button to save the changes.

2.11 Remotely Setting a Nick Name for an eG Agent

Instead of remembering the IP address/ host name of an agent host, users can assign one or more nick names to the host and manage all applications on the host using the same name. The RAC console enables users to assign nick names to agents that have been installed using RAC.

To assign a nick name to an installed agent, do the following:

1. An agent that has just been installed will appear below the **Agent Stopped** node in the tree structure in the left pane of Figure 2.68. From within this node, select the agent to which a nick name has to be set, right-click on it, and choose the **Set Nick for Agent** option (see Figure 2.68).

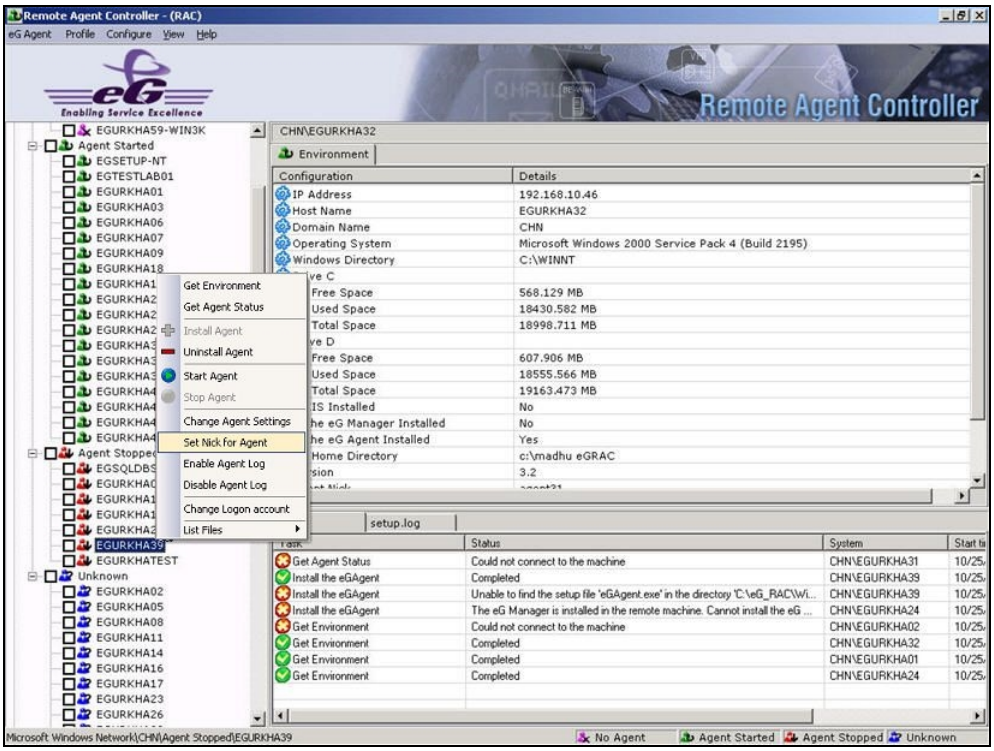

Figure 2.68: Setting a nick name for an eG agent

2. In the **Nick Name** text box that appears (see Figure 2.69), specify the nick name to be set for the chosen agent. Multiple nick names can be provided as a colon-separated (:) list.

Figure 2.69: Setting a nick name for an agent

3. Finally, click the **Set** button in Figure 2.69 to save the changes.

2.12 Remotely Starting/Stopping an eG Agent

To start agents using the eG RAC, do the following:

1. From the hosts listed under the **Agent Stopped** node in the tree structure in the left pane of Figure 2.70, select the agent to be started, right-click on it, and choose the **Start Agent** option (see Figure 2.70).

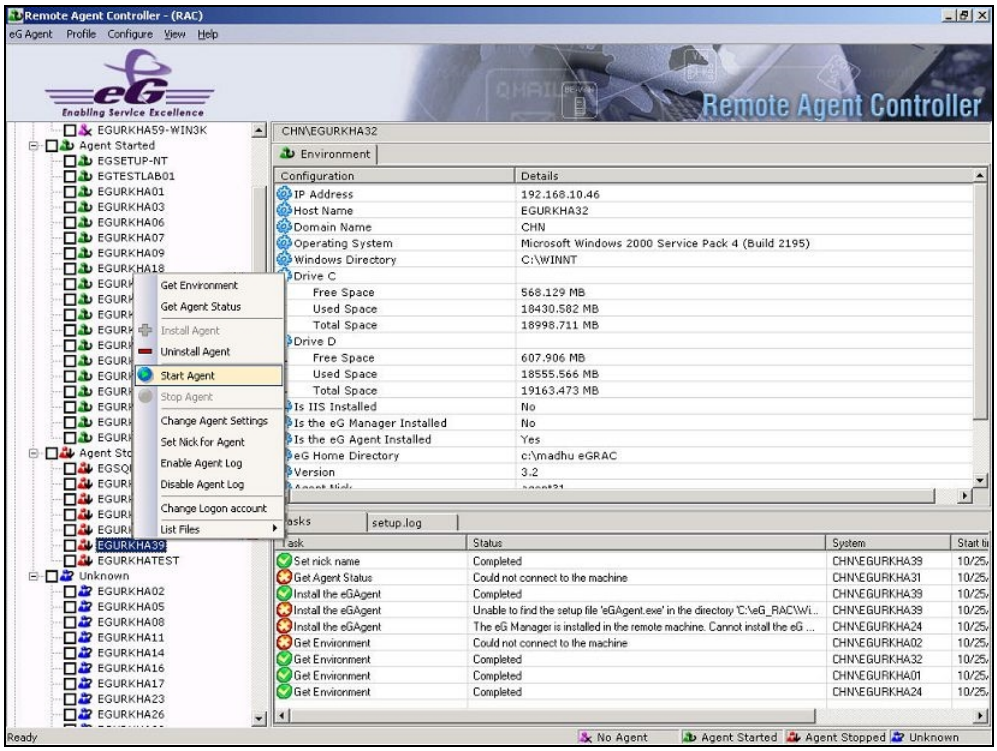

Figure 2.70: Starting an eG agent remotely

2. If the agent starts successfully, the **Tasks** list will indicate the success of the operation (see Figure 2.71), and the agent that was started will move to the **Agent Started** group of the left pane (see Figure 2.71).

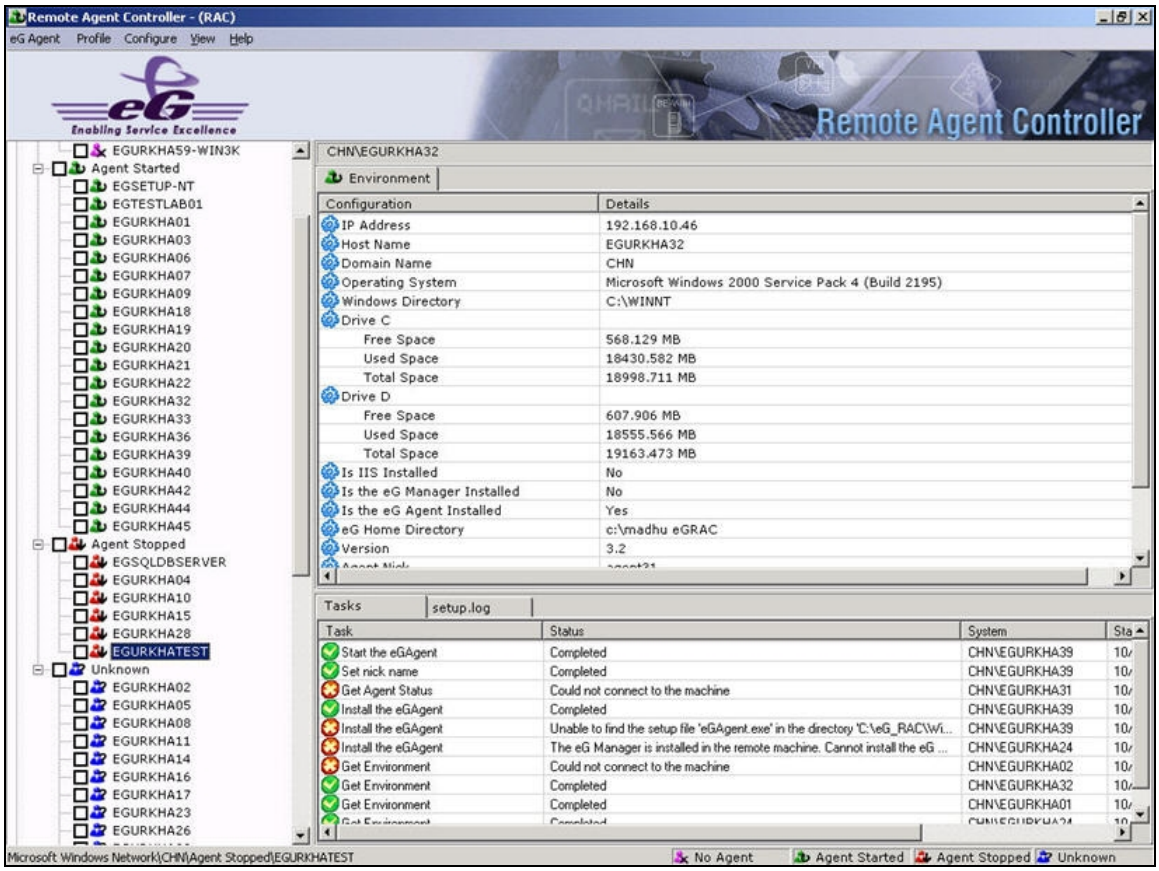

Figure 2.71: Successful starting the eG agent

To stop an agent, do the following:

1. From the hosts listed under the **Agent Started** node in the tree structure in the left pane of Figure 2.72, select the agent to be stopped, right-click on it, and choose the **Stop Agent** option (see Figure 2.72).

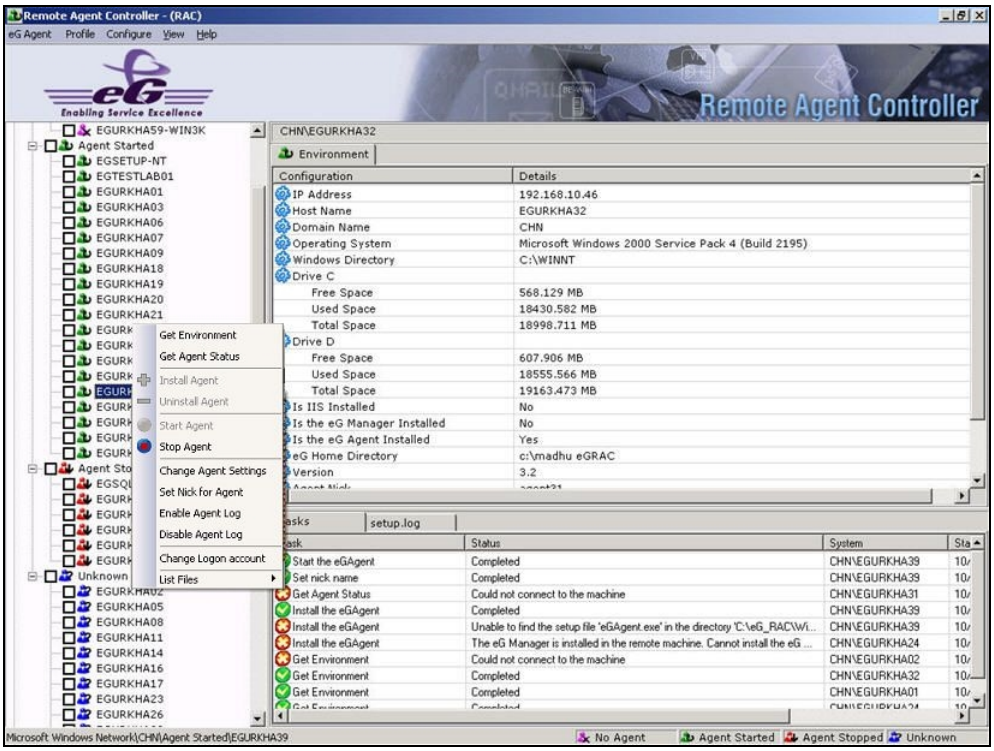

Figure 2.72: Stopping an eG agent remotely

2. If the agent stops successfully, the agent that was stopped will move to the **Agent Stopped** group of the left pane (see Figure 2.73).

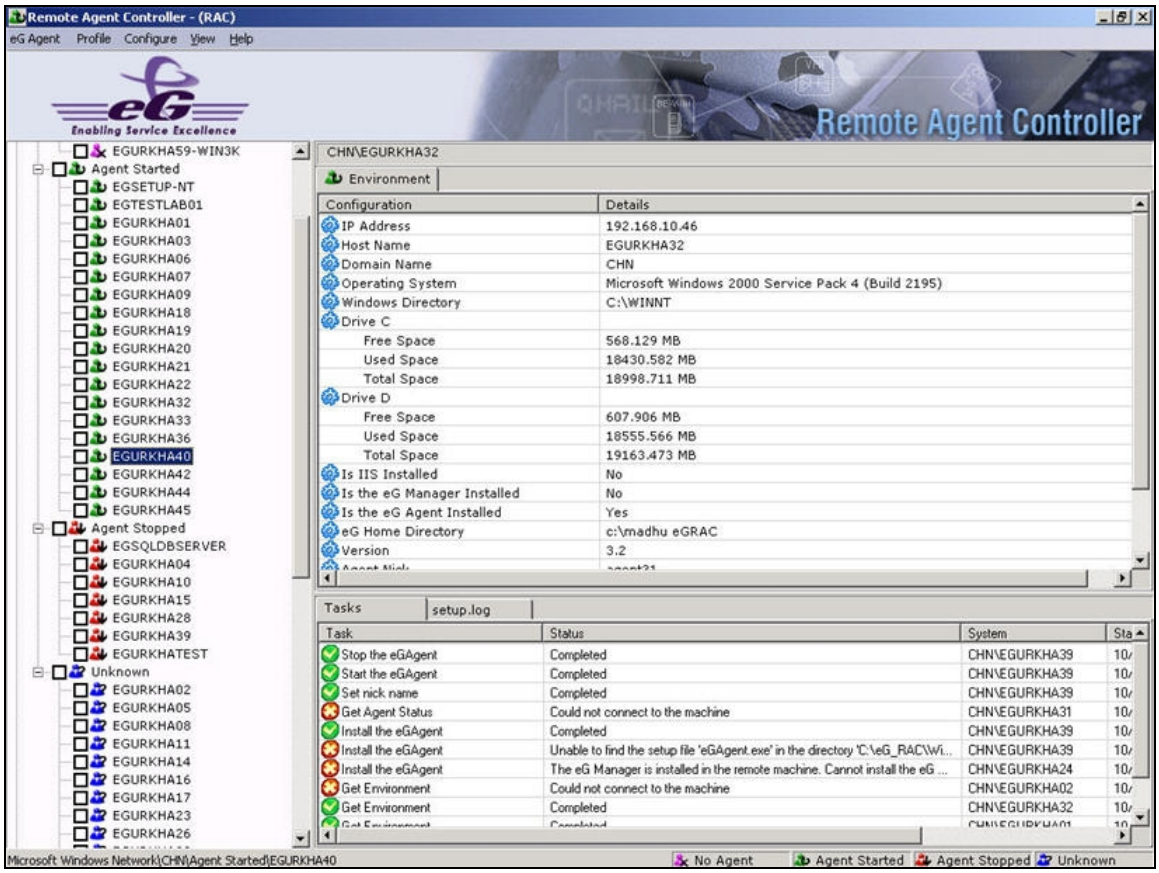

Figure 2.73: Successful stopping the eG agent

2.13 Remotely Changing Agent Settings

RAC enables administrators to instantly change critical agent settings without having to re-install the agent. To perform this, follow the steps given below:

1. Select the agent to be changed from the left pane of the RAC console, right-click on it, and then pick the **Change Agent Settings** option from the shortcut menu that appears (see Figure 2.74).

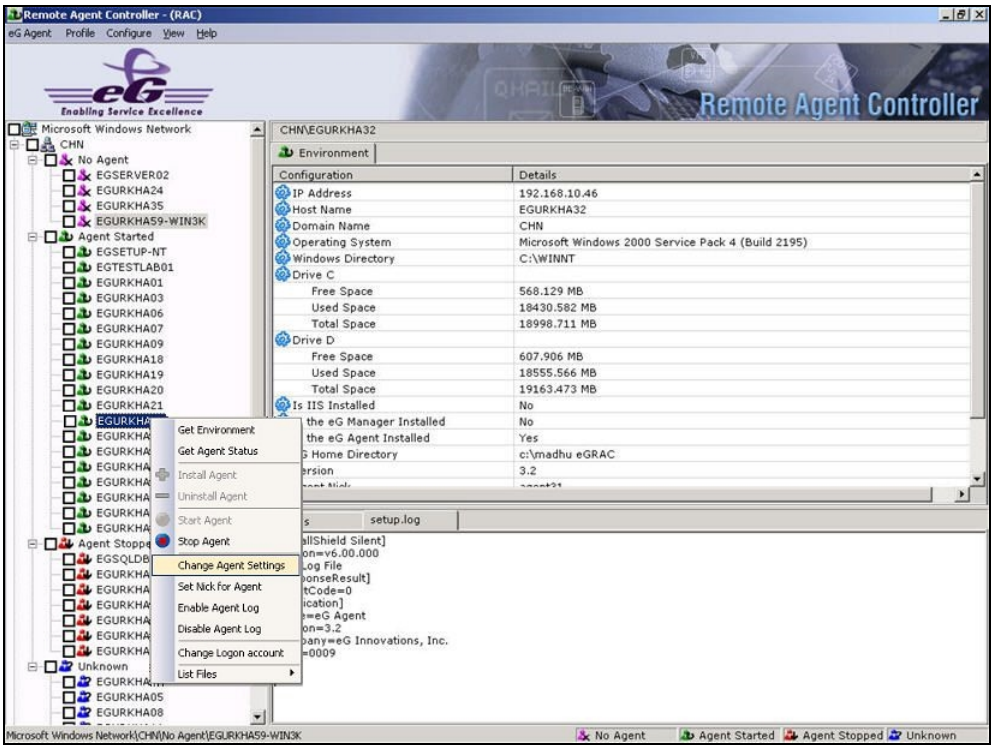

Figure 2.74: Selecting the Change Agent Settings option

2. Figure 2.75 then appears using which you can make the agent report to a different manager by providing the **Host name or IP Address** of the new manager and its **Port**. Similarly, you can also SSL-enable the eG agent by selecting the **Use SSL for communication with the eG Manager** check box. Finally, click the **OK** button.

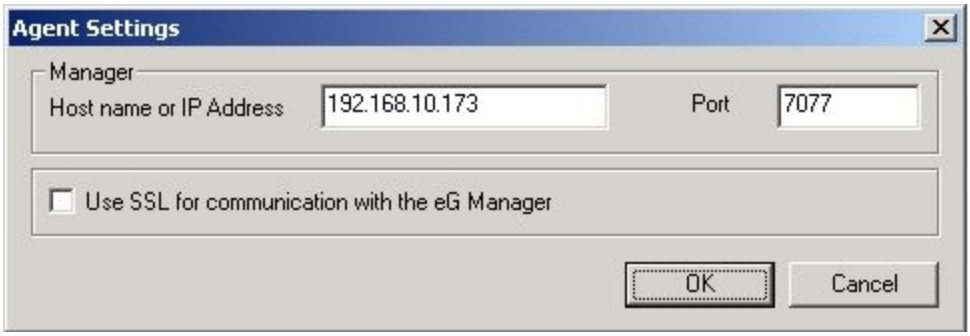

Figure 2.75: Changing the agent settings

2.14 Remotely Uninstalling an eG Agent

To uninstall agents using the eG RAC, do the following:

1. If the agent to be uninstalled is currently running, then select the agent from within the **Agent Started** node. If the agent is not operational presently, then it will appear as a sub-node of the **Agent Stopped** node. In such a case, select the agent from under the **Agent Stopped** node. Then, right-click on the agent and select the **Uninstall Agent** option from its shortcut menu (see Figure 2.76).

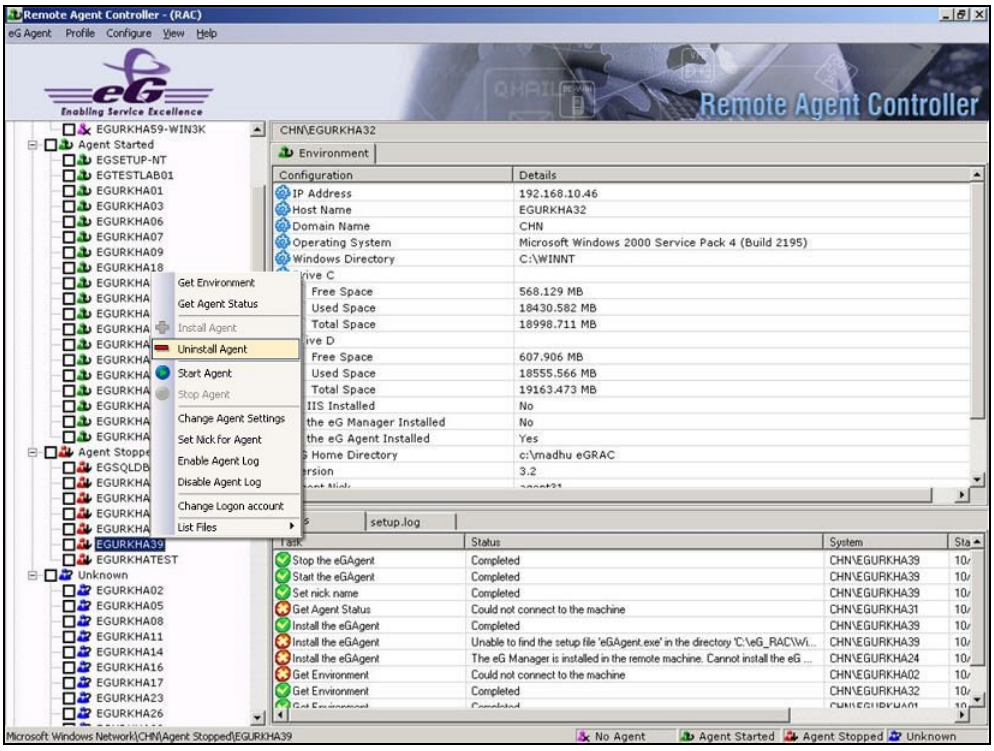

Figure 2.76: Remotely uninstalling an eG agent

2. Figure 2.77 will then appear requesting your confirmation to uninstall the agent. Click **Yes** here to proceed.

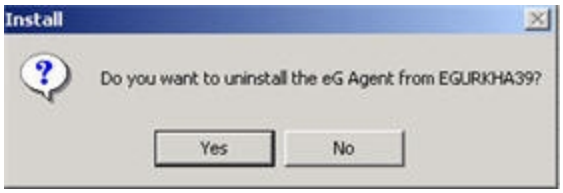

Figure 2.77: Confirming the agent uninstallation

3. If the agent is uninstalled successfully, the host from which the agent was uninstalled will automatically move to the **No Agent** group of the left pane (see Figure 2.78).

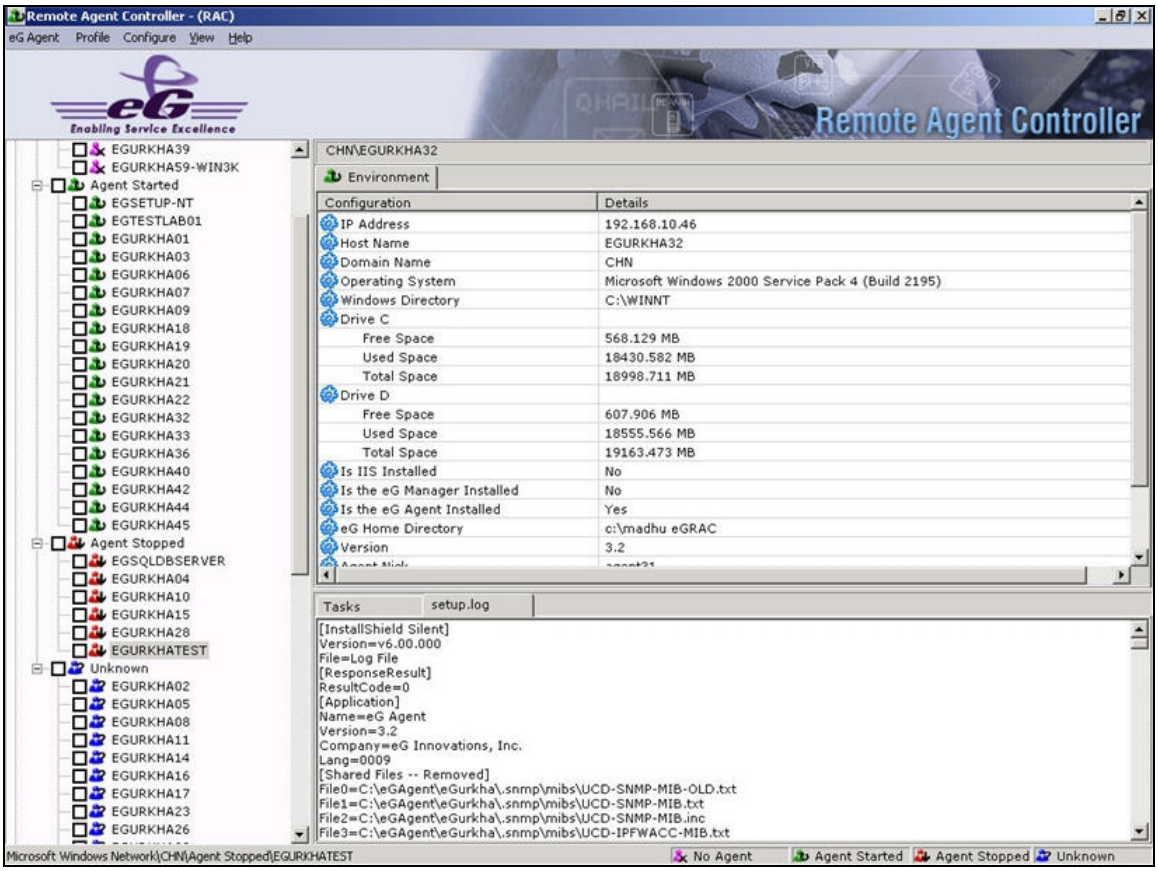

Figure 2.78: Successfully uninstalling the eG agent

2.15 Other Features of the RAC

Besides the utilities already discussed, the following functions can also be performed using RAC:

- Task list manipulations
- Refreshing the entire network
- Viewing the error log and the **eg_agents.ini** file
- Logging every RAC operation/command

This section deals with each of these functions in great detail.

2.15.1 Working with the Tasks List

The **Tasks** list at the bottom of the right pane of Figure 2.76 serves as an effective indicator of the success/failure of every operation triggered using RAC. Also, in the event of failure of an operation,

the **Status** column (see Figure 2.76) of the **Tasks** list throws light on why the operation failed, so that the corrective action can be promptly initiated.

You can view the tasks currently in progress (see Figure 2.79) in a separate dialog box for more clarity, by selecting **Task List** from the **View** menu on the RAC menu bar.

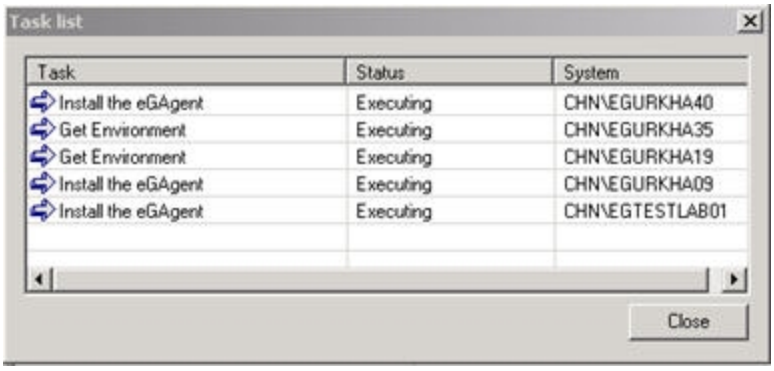

Figure 2.79: Viewing the current tasks list

If the **Tasks** list in the right pane becomes too crowded, then you can remove all the entries from the list by right-clicking inside the **Tasks** tab, and selecting the **Clear** option from the pop-up menu (see Figure 2.80). Then, click the **Yes** button to confirm clearing the tasks list (see Figure 2.81).

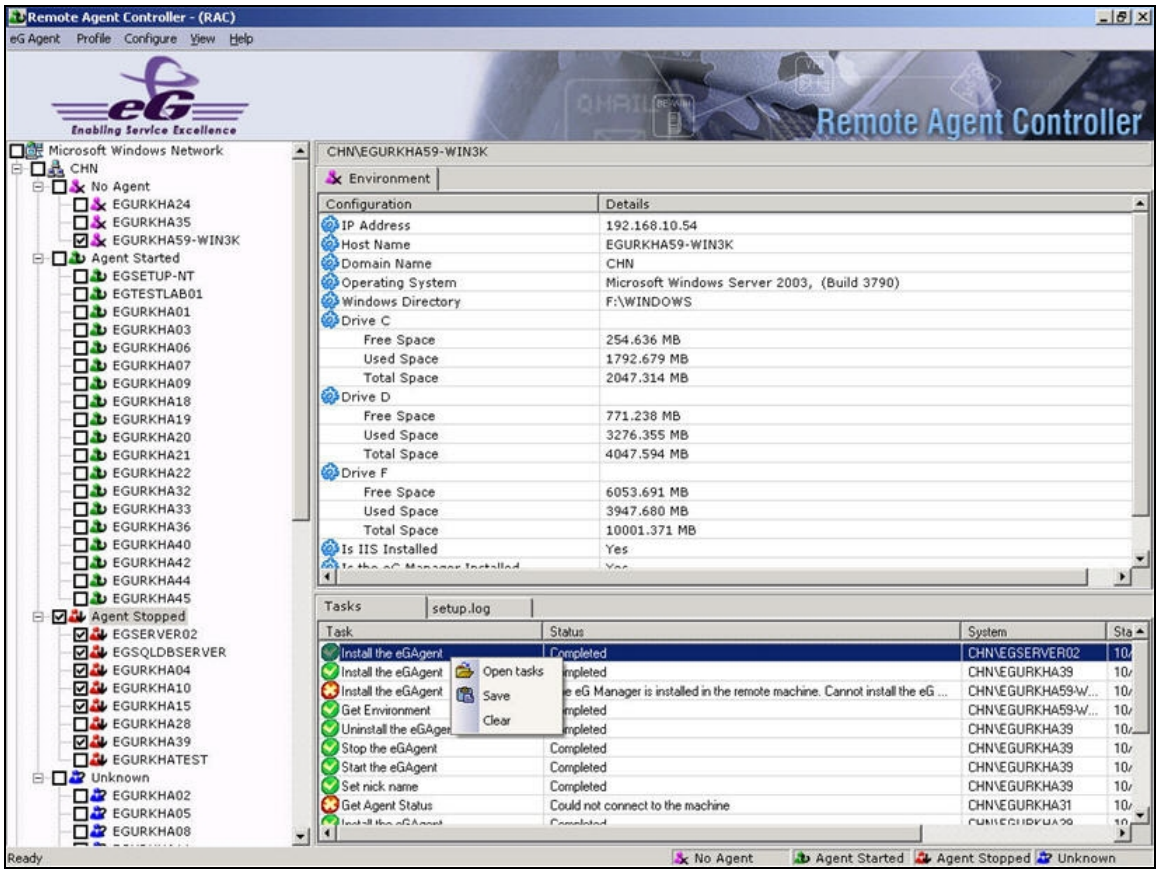

Figure 2.80: Selecting the Clear option from the shortcut menu inside the task list

Figure 2.81: Confirming clearing the task list

Similarly, you can save the task list entries for future reference, by selecting the **Save** option from the shortcut menu that appears upon right-clicking on the insides of the **Tasks** list (see Figure 2.82).

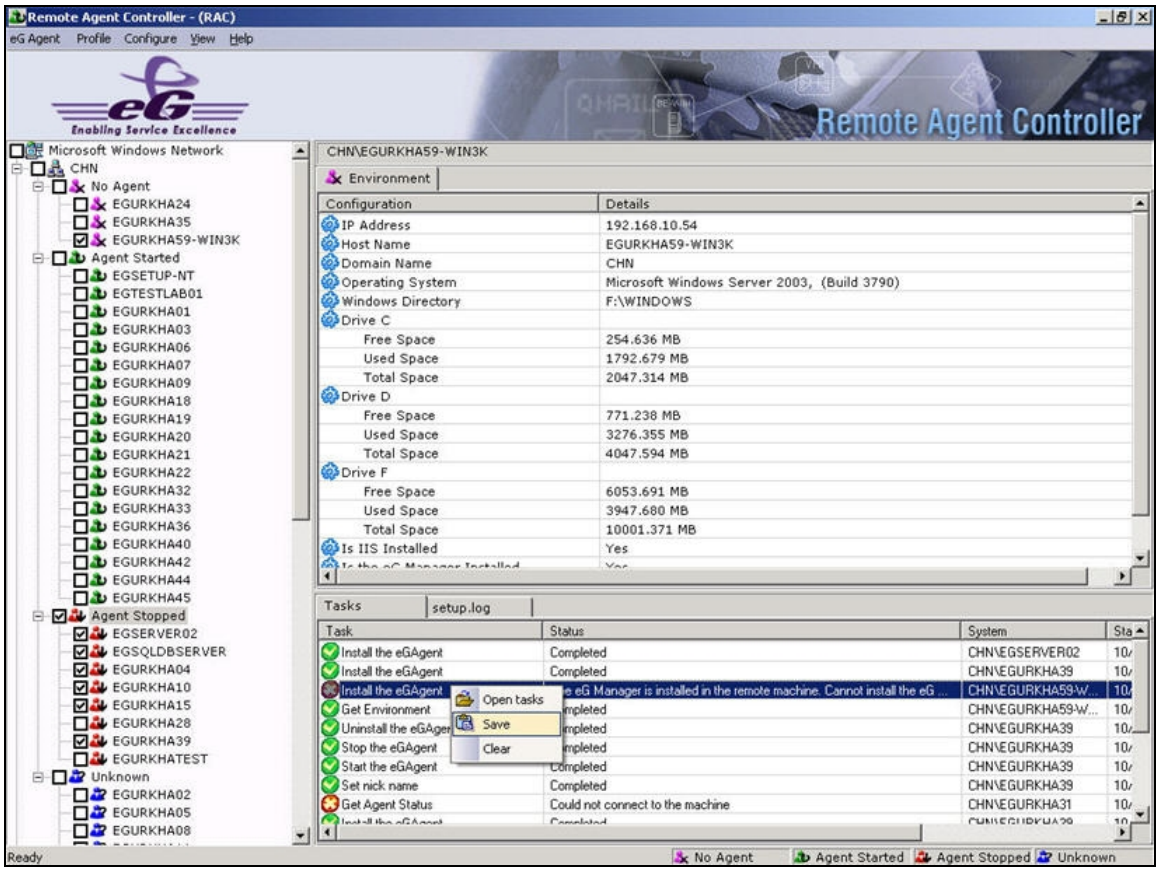

Figure 2.82: Selecting the Save option from the task list menu

A task list is typically saved as a ***.task** file. To open a saved task list sometime later, use the **Open tasks** option in the shortcut menu that appears when you right-click within the **Tasks** tab (see Figure 2.83), and then select the task file to be opened.

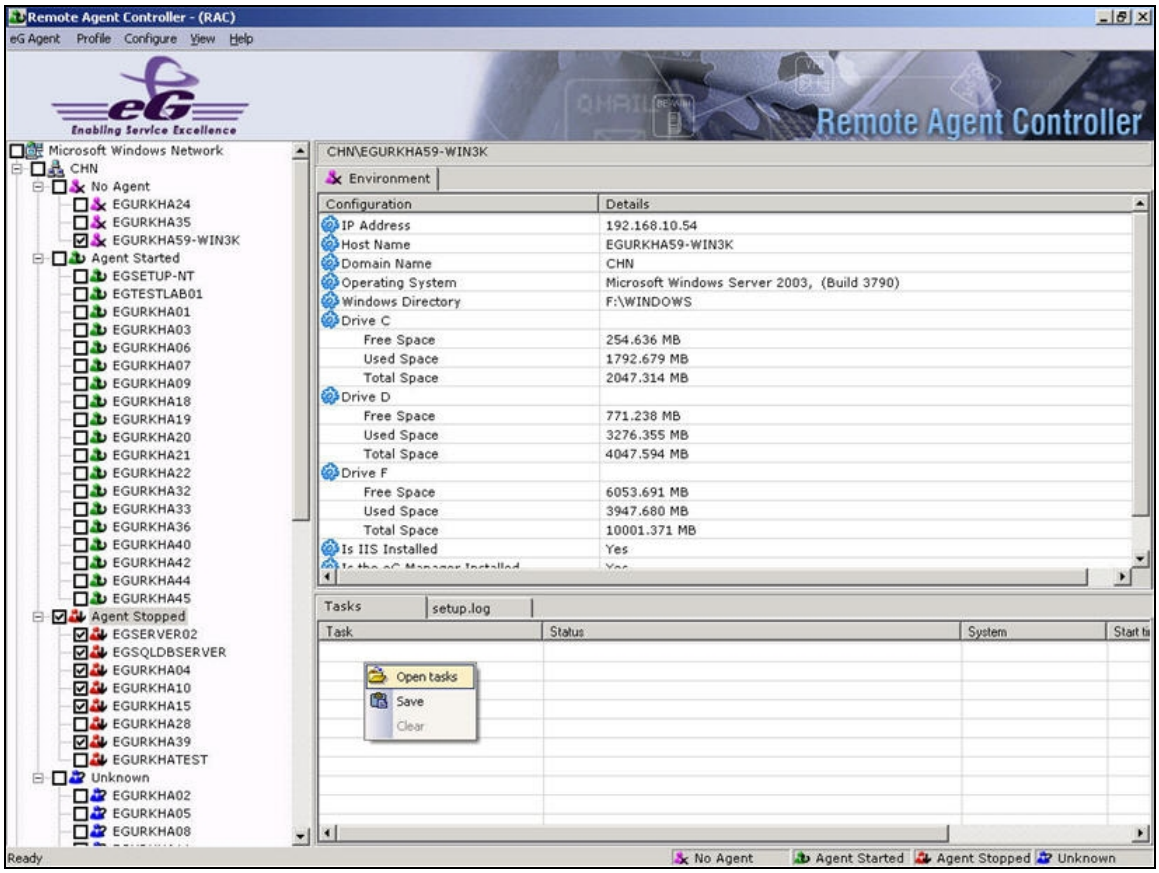

Figure 2.83: Selecting the Open tasks option

Some RAC users however, might find the manual saving of task lists rather inconvenient. For their benefit, on a daily basis, RAC automatically records the details (including status) of all tasks that users have performed to a file, and stores these 'dated' files in the **<EG_RAC_INSTALL_DIR>\data** folder. Typically, these files are named after the *date* to which the tasks pertain. For example, to view the details of all user-initiated tasks on RAC on December 20, 2007, simply double-click on the file named *12_20_2007*, in the **<EG_RAC_INSTALL_DIR>\data** folder (see Figure 2.84).

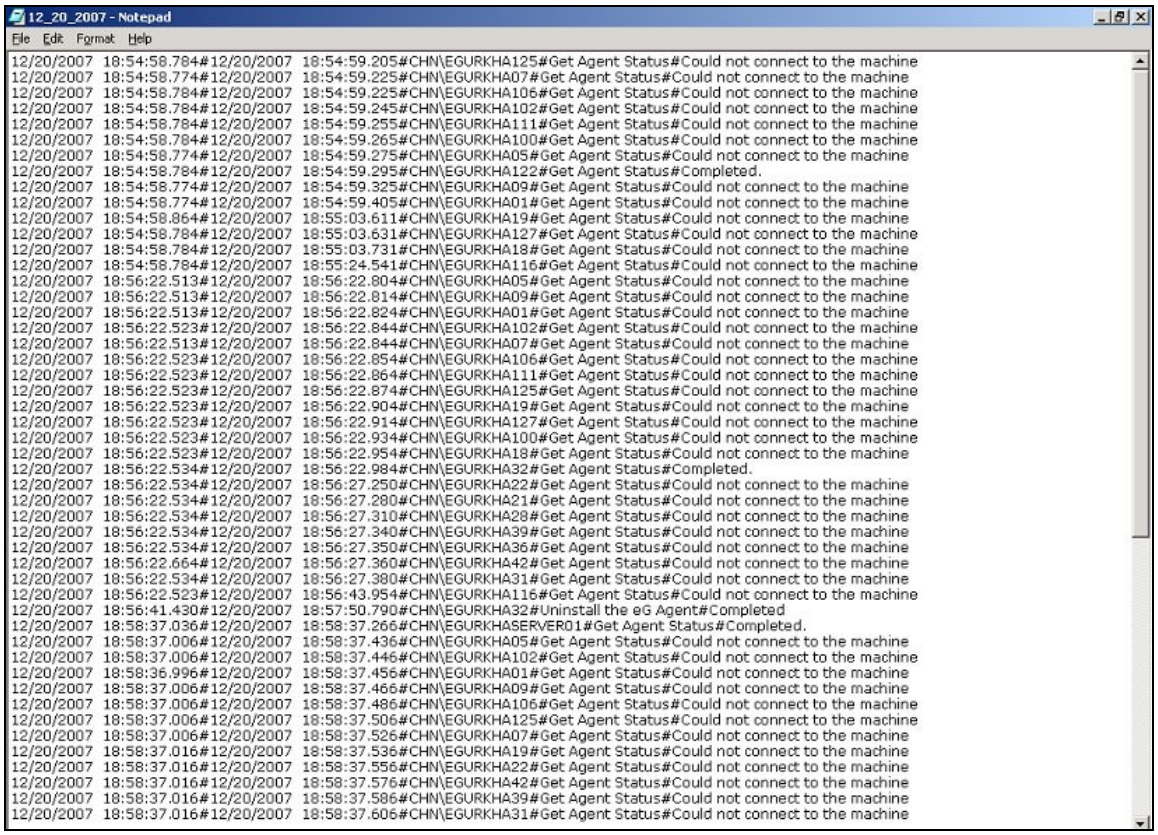

Figure 2.84: Details of tasks executed on December 20, 2007

2.15.2 Refreshing the Network

If you so desire, you can refresh the entire monitored network, so that the tree-structure in the left pane of the RAC console reflects recent changes in the monitored environment - this could be addition of new domains/hosts to the target environment, or the deletion of existing domain/hosts To refresh the network, select the **Refresh Network** option from the **eG Agent** menu option (see Figure 2.85).

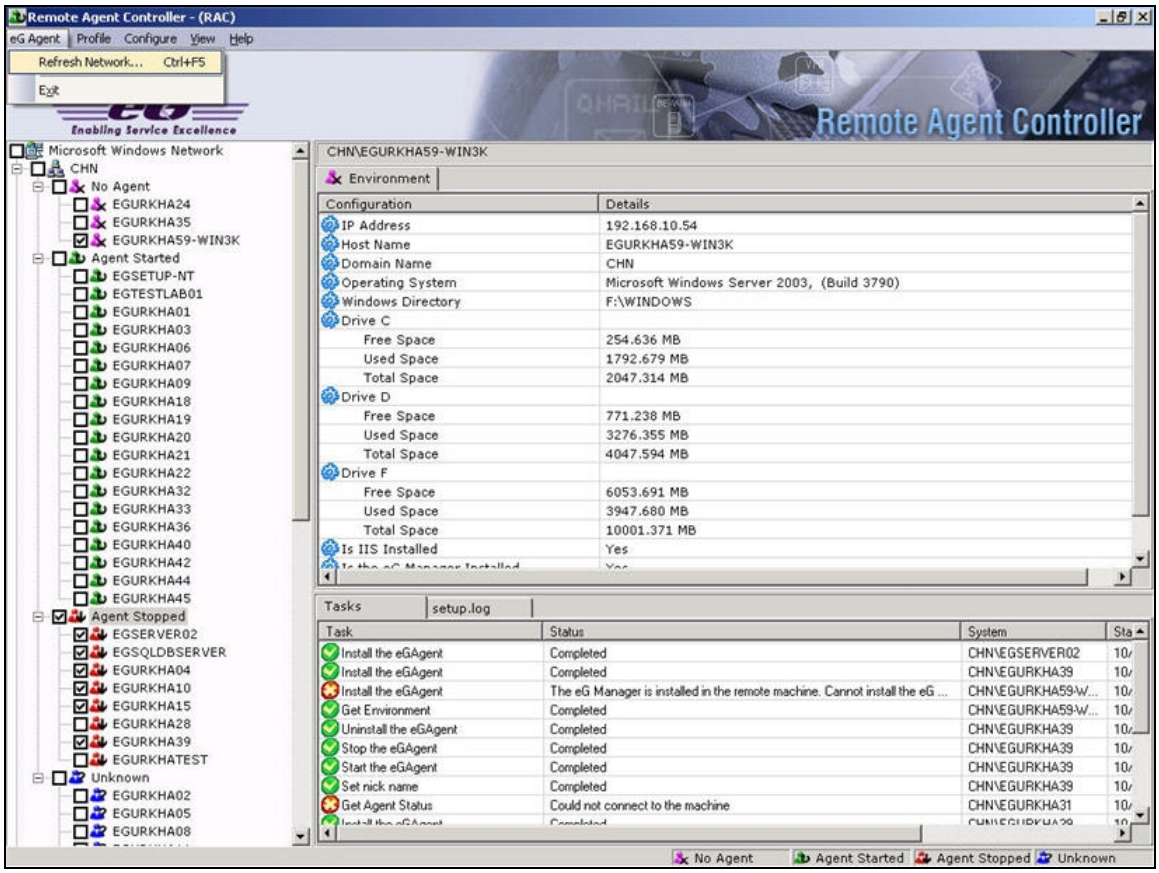

Figure 2.85: Refreshing the network

Note:

If you are not looking to determine status changes across the environment, but are only interested in the current state of specific hosts in the environment, then, you need not run an elaborate **Refresh Network** routine. Instead, simply select the host from the tree-structure, right-click on it, and pick the **Get Agent Status** option to view its current status.

2.15.3 Enabling Logging of Agent Operations and Viewing Agent Logs

Logging enables you to track agent-related activities, and to trap errors (if any) that might occur while performing such activities, so as to facilitate further diagnosis. RAC allows you to remotely enable/disable logging for specific agents. To enable logging, select the agent host from the **Agent Started** or **Agent Stopped** nodes in the tree-structure in the left pane of RAC, right-click on it, and then select the **Enable Agent Log** option (see Figure 2.86). To disable logging, select the **Disable Agent Log** option from the shortcut menu of Figure 2.86.

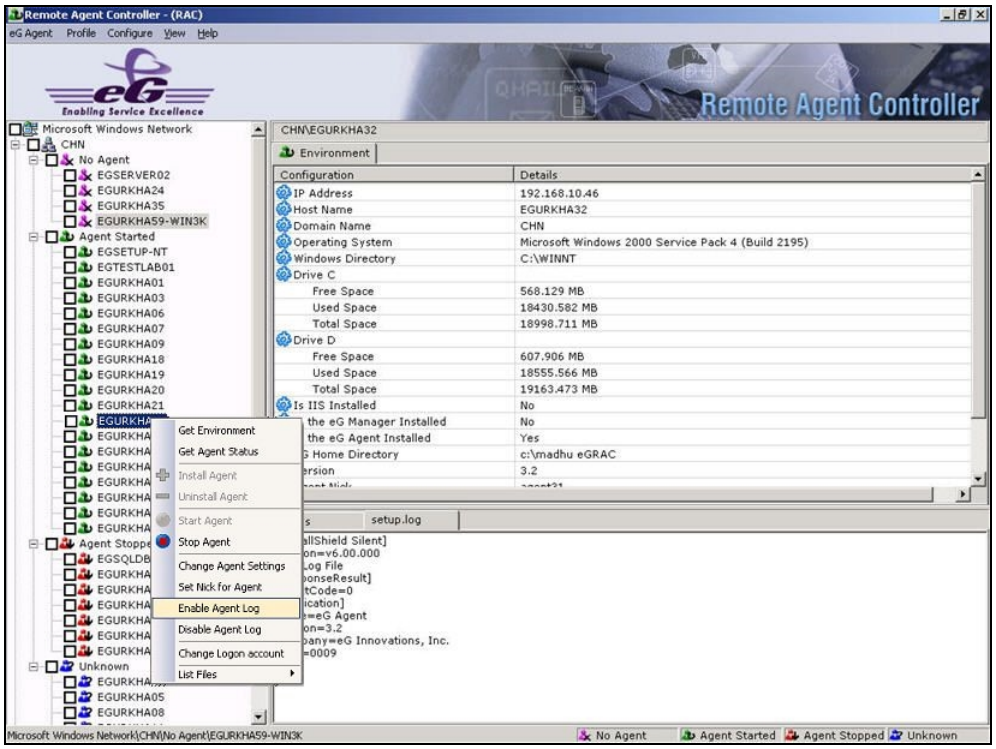

Figure 2.86: Enabling logging

As soon as logging is enabled for an agent, an **agentout** file is created in the **<EG_INSTALL_DIR>\agent\logs** directory, to which every subsequent agent operation is logged. Similarly, an **error_log** file is also created in the same directory, to which error information is written. To view these log files, first, select the agent host, and right-click on it. In the shortcut menu that appears, move your mouse pointer of the **List Files** option, and then pick the **Log Directory** option from the **List Files** menu that appears (see Figure 2.87).

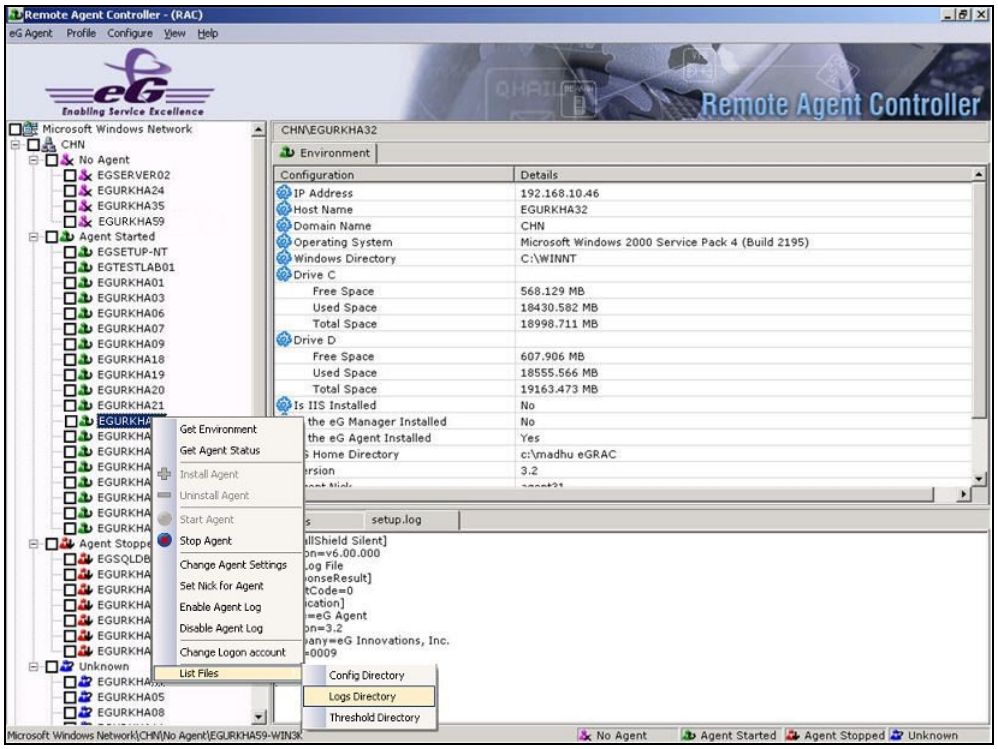

Figure 2.87: Selecting the Log Directory option

Figure 2.88 then appears, listing the contents of the **Log Directory**.

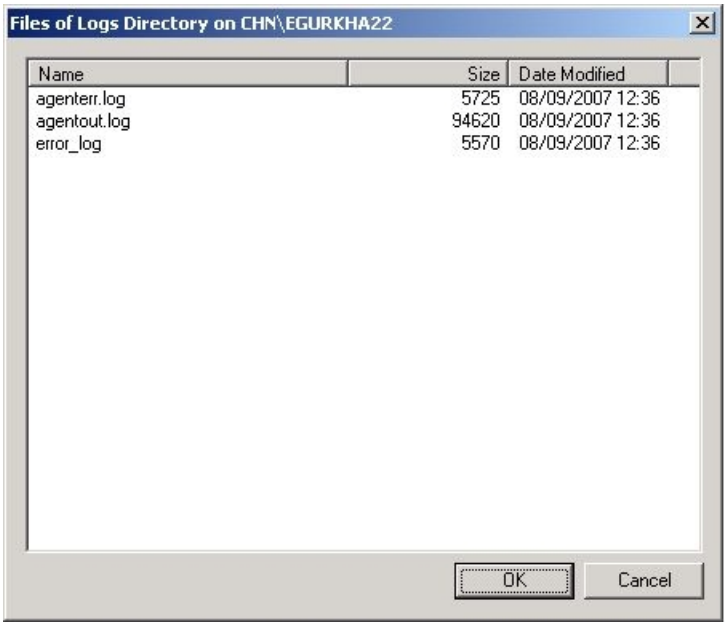

Figure 2.88: Viewing the contents of the Log Directory

To view any of the log files listed therein, simply double-click on the file name in Figure 3.62. For instance, to view the **error_log**, double-click on it. Doing so leads you back to the RAC console. In the right pane of the console, you can view the contents of the **error_log** (see Figure 2.89). **Note that RAC does not allow users to modify the displayed contents.**

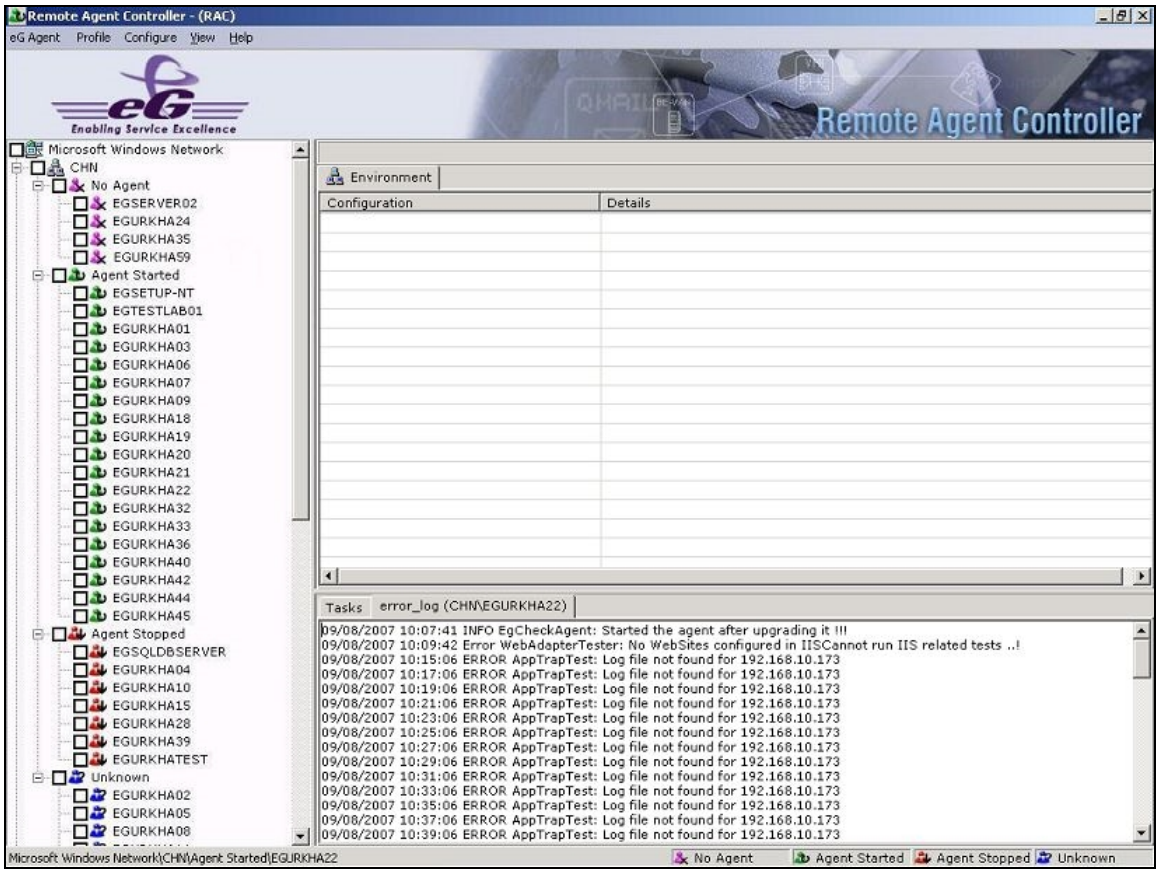

Figure 2.89: Viewing the contents of the error_log

2.15.4 Viewing Agent Configuration

RAC also provides administrators with remote access to the configuration information pertaining to a chosen agent. To view an agent's configuration, select the agent host from the left pane of the RAC console, right-click on it, and then move your mouse pointer over the **List Files** option in the shortcut menu that appears. Next, select the **Config Directory** option from the **List Files** menu (see Figure 2.90).

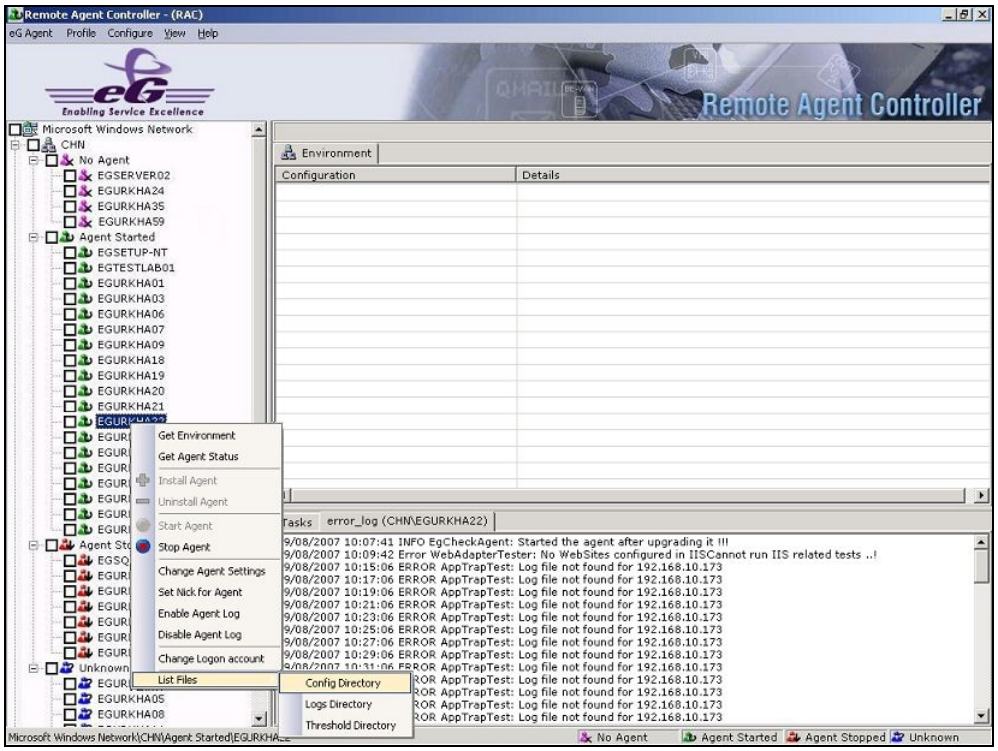

Figure 2.90: Figure 3.76: Selecting the Config Directory option

Doing so invokes Figure 2.91, which displays the files within the **Config Directory** of the agent.

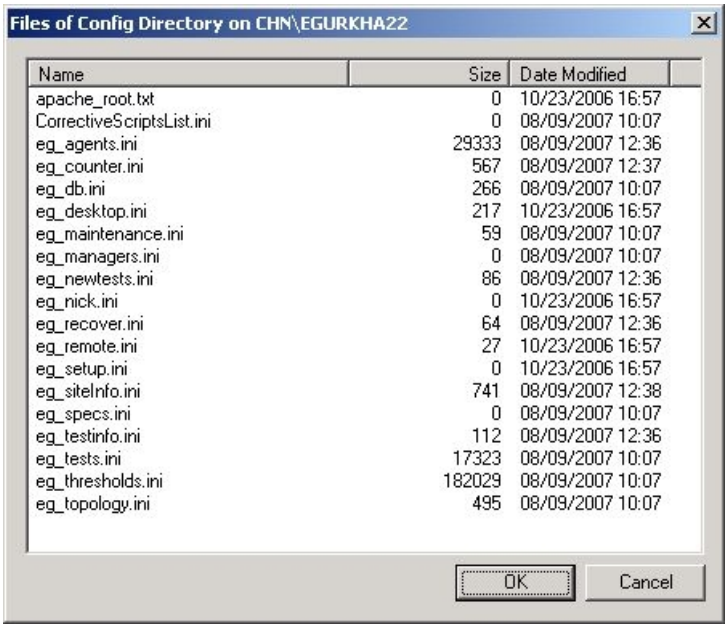

Figure 2.91: Figure 3.77: Viewing the contents of the Config Directory

To view the contents of a particular config file, double-click on the file name in Figure 2.91. Figure 2.92 then appears, displaying the relevant contents. **Note that RAC does not allow users to modify the displayed contents.**

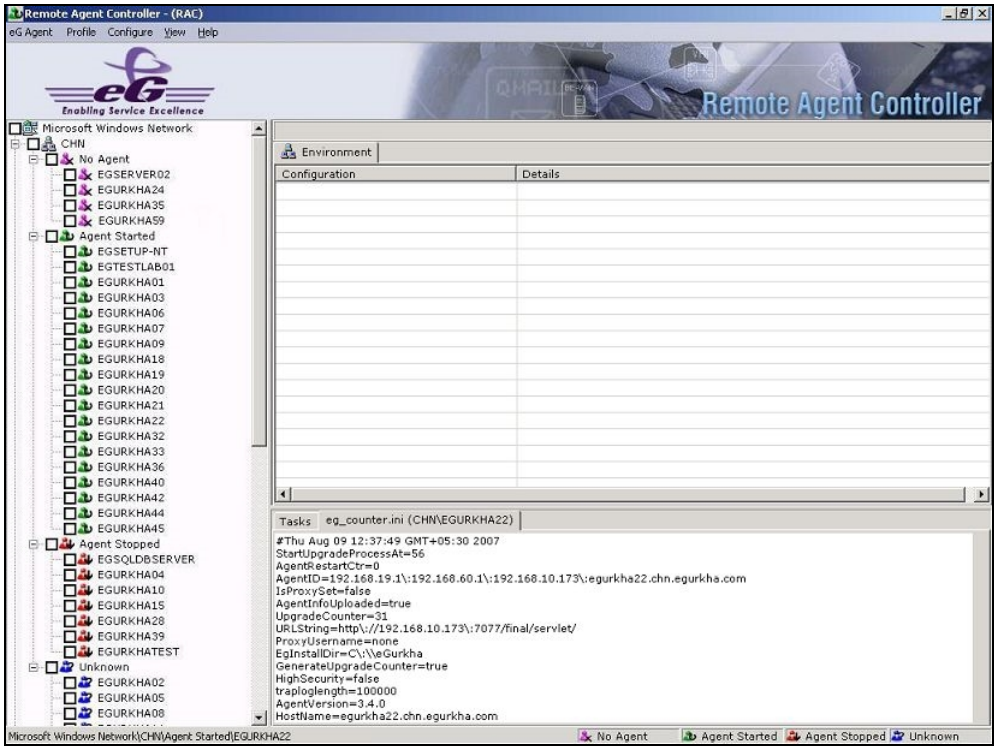

Figure 2.92: Viewing the contents of a config file

2.15.5 Viewing Threshold Computations

The eG agent downloads the pre-configured threshold settings from the eG manager, compares the set threshold limits with actual measure values that it collects from the monitored target, and reports deviations (if any) to the eG manager.

RAC enables administrators to remotely track the threshold computations for various tests that are executed by an eG agent. To achieve this, first, select the agent host from the left pane of the RAC console and right-click on it. Then, move your mouse pointer over the **List Files** option in the shortcut menu that appears, and select the **Threshold Directory** option from the **List Files** menu (see Figure 2.93).

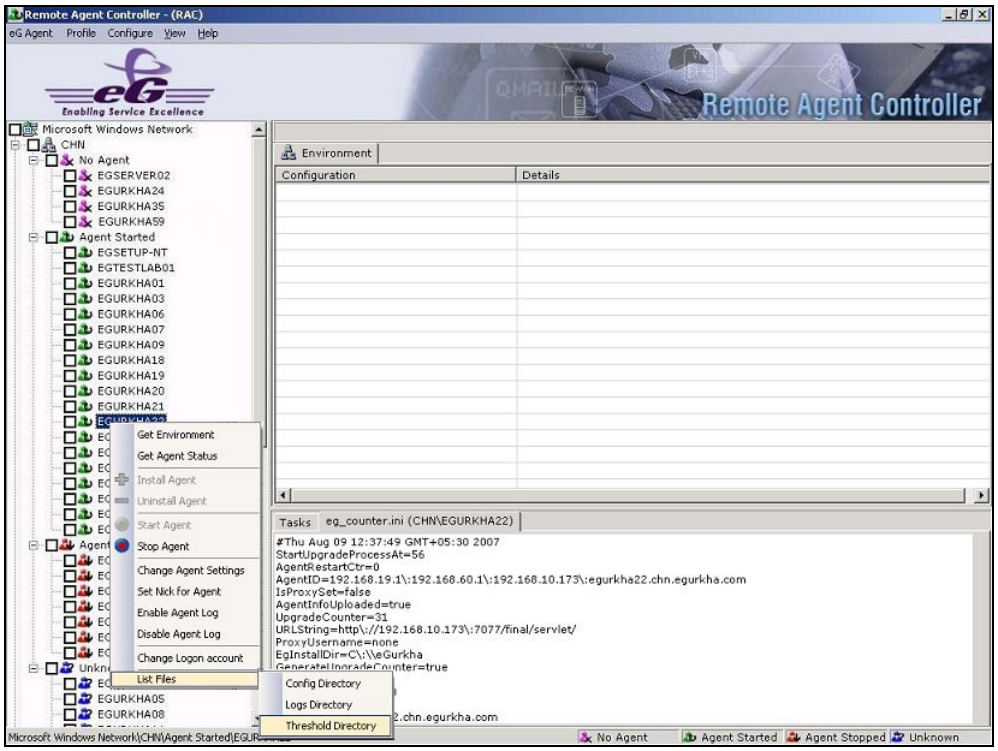

Figure 2.93: Figure 3.79: Selecting the Threshold Directory option

Figure 2.94 then appears listing the files that the **Threshold Directory** contains.

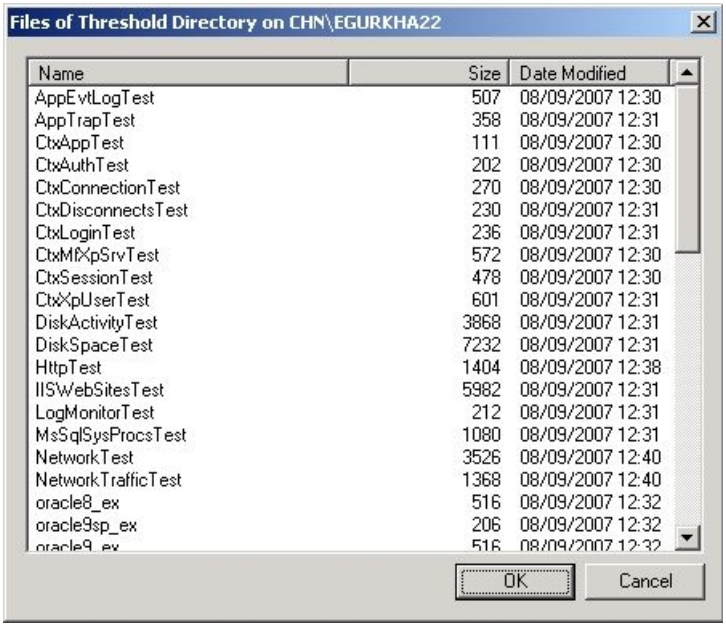

Figure 2.94: Contents of the Threshold Directory

Every file listed in Figure 2.95 corresponds to a test that the eG agent executes on a monitored server. To view the contents of a file, double-click on it. Figure 2.95 appears displaying the contents of the chosen file. **Note that RAC does not allow users to modify the displayed contents.**

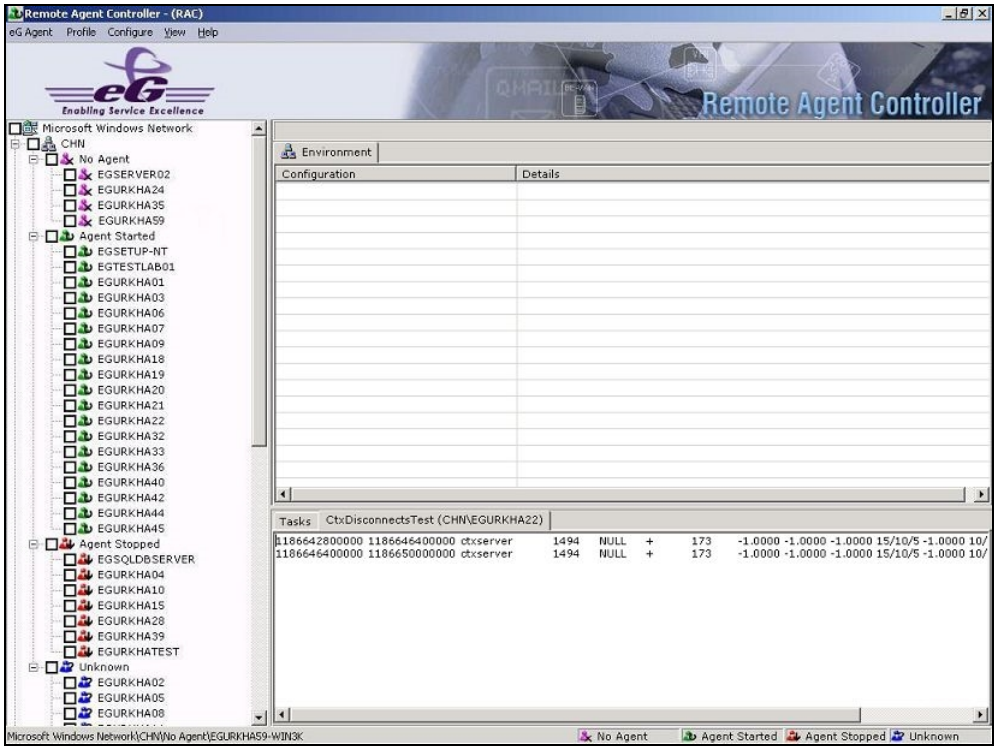

Figure 2.95: Contents of a Threshold file

2.15.6 Logging RAC Operations/Commands

By default, every operation performed using RAC and the errors that occur in the process are logged in a log file named **eg_output.log** in the **<RAC_INSTALL_DIR>\bin** directory. If need be, you can disable the automatic logging by deselecting the **Enable Logging** check box in the **Logging** section of the **Preferences** dialog box (see Figure 2.96).

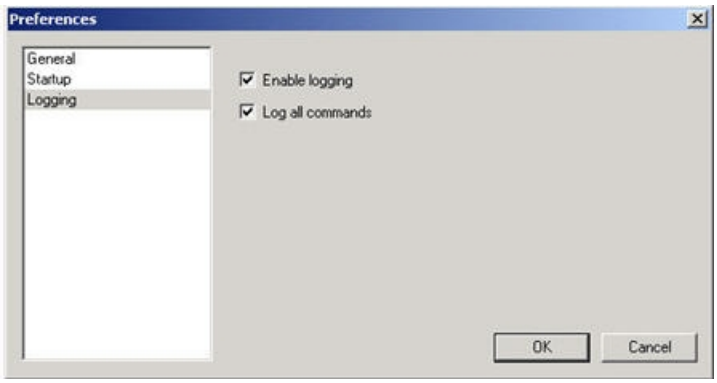

Figure 2.96: Enabling/disabling logging

Besides tasks, you can also log the individual commands executed by RAC and the success/failure status of each command in the log file. To enable this logging, select the **Log all commands** check box in Figure 2.96.

After enabling/disabling logging, click the **OK** button in Figure 2.96 to save the changes.

Chapter 2: Troubleshooting the Remote Agent Controller

2.16 Troubleshooting Domain Discovery Failure

If RAC is unable to discover hosts in some domains, then, check the following:

1. Check whether the domains that could not be discovered are backup domains. If so, note that RAC cannot discover such domains.
2. If the domains are not backup domains, then check the following:
   - Was RAC launched using the **Run as administrator** option? If not, then stop RAC, and start it again using the **Run as administrator** option.
   - Are the **Computer Browser**, **Server**, and **Workstation** services running on all domain controllers? If not, then start these services on the controllers.
   - Has Network Discovery been enabled on the Windows Firewall of all target Windows hosts in the undiscovered domains? If not, then follow the steps detailed in page to configure Windows Firewall to allow inbound network discovery.
   - Are there other third-party firewalls in the connectivity path to the problem domains? If so, do those firewalls allow network discovery as well? If not, then configure the third-party firewalls to allow network discovery through the following ports:

  - UDP 3702, 137, 138, 1900
  - TCP 5357, 5358, 445, 2869, 139
- Has network discovery been enabled on the RAC host? If not, make sure that the Windows Firewall on the RAC host has been configured to allow network discovery. For the procedure to achieve this, refer to Page of this document.
- Does the domain in which RAC operates have a trust relationship with the domains that could not be discovered? If not, then make sure that the trust relationship is established before attempting discovery.

2.17 Troubleshooting Host Discovery Failure

Sometimes, RAC may not be able to discover hosts within one/more domains. In such circumstances, check the following:

- Was RAC launched using the **Run as administrator** option? If not, then stop RAC, and start it again using the **Run as administrator** option.
- Are the **Computer Browser and Server** services running on the hosts that could not be discovered? If not, then start these services on those hosts.
- Before running discovery, did you use the **Change Logon Account** option in RAC to grant domain administrator privileges to RAC? This is imperative because, RAC will not be able to connect to a domain and discover its hosts without the privileges of the administrator of that domain. If you have not configured RAC with these privileges, then, use the **Change Logon Account** option to provide the credentials of the administrator of the domain for which hosts could not be discovered, and then run discovery.
- Has Network Discovery been enabled on the Windows Firewall of all target Windows hosts in the undiscovered domains? If not, then follow the steps detailed in page to configure Windows Firewall to allow inbound network discovery.
- Are there other third-party firewalls in the connectivity path to the problem domains? If so, do those firewalls allow network discovery as well? If not, then configure the third-party firewalls to allow network discovery through the following ports:
  - UDP 3702, 137, 138, 1900
  - TCP 5357, 5358, 445, 2869, 139

2.18 Troubleshooting Host Discovery Failure

Sometimes, RAC may not be able to discover hosts within one/more domains. In such circumstances, check the following:

- Was RAC launched using the **Run as administrator** option? If not, then stop RAC, and start it again using the **Run as administrator** option.
- Are the **Computer Browser and Server** services running on the hosts that could not be discovered? If not, then start these services on those hosts.
- Before running discovery, did you use the **Change Logon Account** option in RAC to grant domain administrator privileges to RAC? This is imperative because, RAC will not be able to connect to a domain and discover its hosts without the privileges of the administrator of that domain. If you have not configured RAC with these privileges, then, use the **Change Logon Account** option to provide the credentials of the administrator of the domain for which hosts could not be discovered, and then run discovery.
- Has Network Discovery been enabled on the Windows Firewall of all target Windows hosts in the undiscovered domains? If not, then follow the steps detailed in page to configure Windows Firewall to allow inbound network discovery.
- Are there other third-party firewalls in the connectivity path to the problem domains? If so, do those firewalls allow network discovery as well? If not, then configure the third-party firewalls to allow network discovery through the following ports:
    - UDP 3702, 137, 138, 1900
    - TCP 5357, 5358, 445, 2869, 139

2.19 Troubleshooting Failure of RAC to Install / Uninstall / Start / Stop Agents

If RAC fails to install/uninstall/start/stop an agent on a host, check the following:

1. Were you trying to install the eG agent on the eG manager host? If so, then note that the installation will fail, as you cannot use RAC to install an agent on the manager host. Such an agent can only be installed manually.
2. Is the target Windows host sized with the space requirement for the eG agent? If not, then the agent operation is bound to fail, owing to the lack of adequate space. In this case therefore, ensure that you resize the target with sufficient disk space.

3. Does the install drive you specified during a remote agent installation (i.e. the Profile that is chosen for the agent install) exists on the target host; if not, the install process will fail;
4. Was RAC launched using the Run as administrator option? If not, then stop RAC, and start it again using the Run as administrator option.
5. Are the Computer Browser and Server services running on the host in question? If not, then start these services on that host.
6. Before attempting an install/uninstall/start/stop of an eG agent on the host, did you use the Change Logon Account option in RAC to grant system administrator privileges to RAC for accessing the host? This is imperative because, RAC will not be able to perform any of these activities on a host without administrator privileges. If you have not configured RAC with these privileges, then, use the Change Logon Account option to provide the credentials of the system administrator of that host.
7. Have you added the system administrator account that you have used above to the Log on as a service list of the target Windows host? If not, then before granting system administrator privileges to RAC, make sure that you follow the steps below to add the system administrator account you intend to use, to the **Log on as a service** list of the target:
    - Login to the target Windows host.
    - Follow the Start -> Control Panel menu sequence on the host.
    - Double-click on the **Administrative Tools** option in the **Control Panel**, and click on the **Local Security Policy** option within (see Figure 2.97).

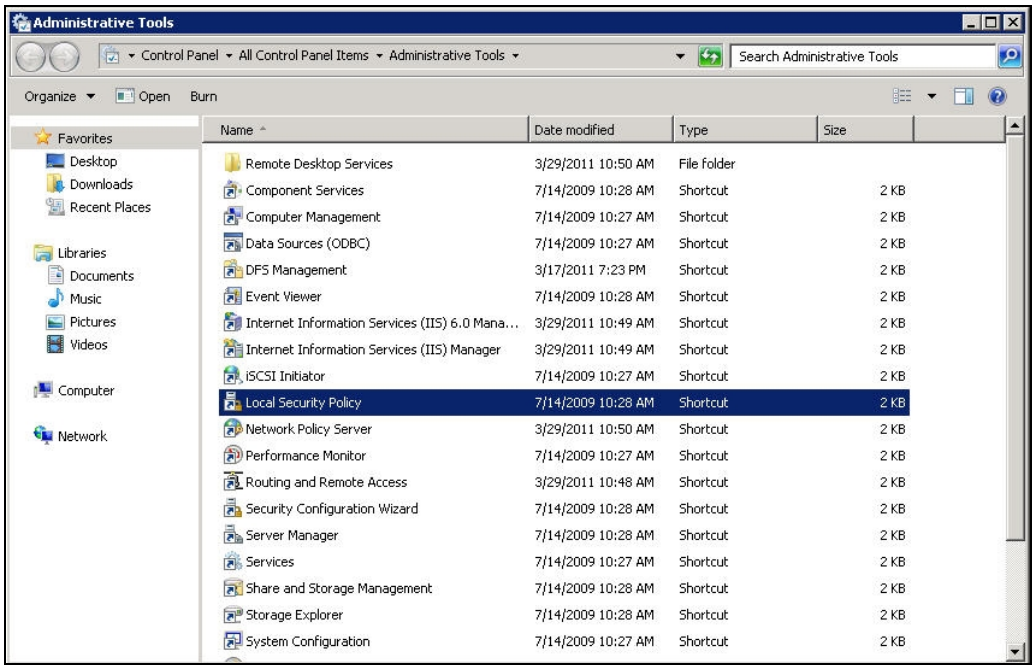

Figure 2.97: Clicking on the Local Security Policy option

- In left panel of Figure 2.98 that then appears, expand the **Local Policies** node and click on the **User Rights Assignment** sub-node within. The right panel will then change to list the policies (see Figure 2.98).

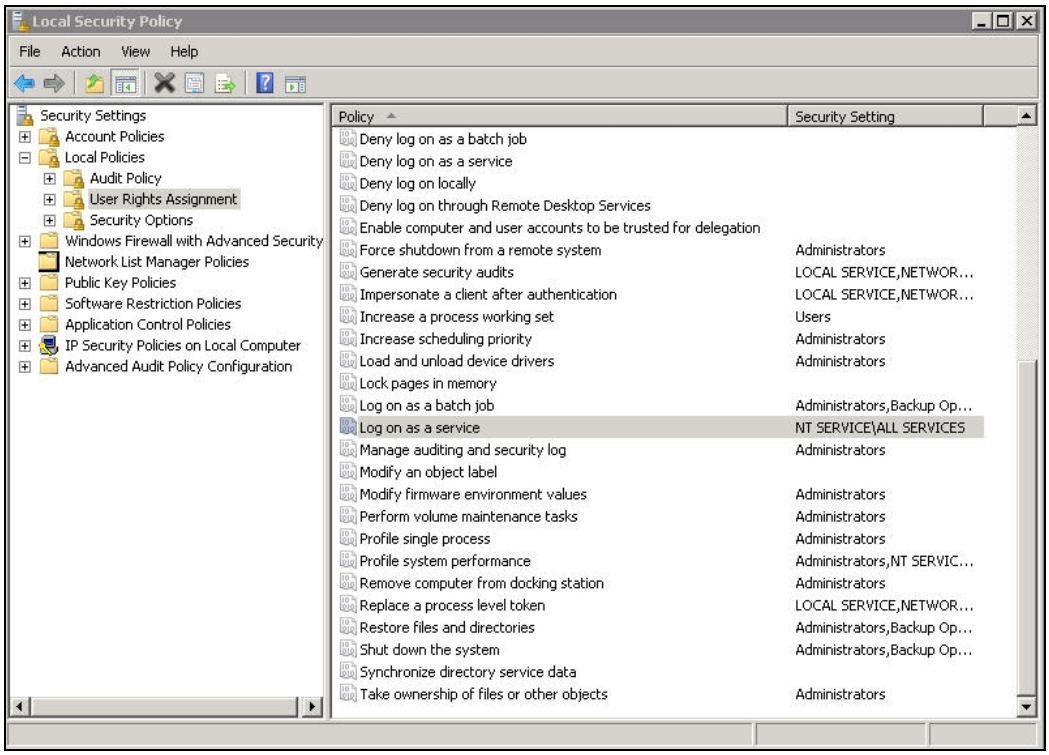

Figure 2.98: Viewing the User Rights Assignment policies

- Browse the policy list in the right panel to locate the **Log on as a service** policy (see Figure 2.98). Double-click on this policy.
- Figure 2.99 will then appear listing the user accounts with the **Log on as a service** privilege. If this list does not include the *system administrator* account that you intend using for remotely installing (or uninstalling/stopping/starting) an eG agent using RAC, then, proceed to manually add that account. For this, click on the **Add User or Group** button in Figure 2.99.

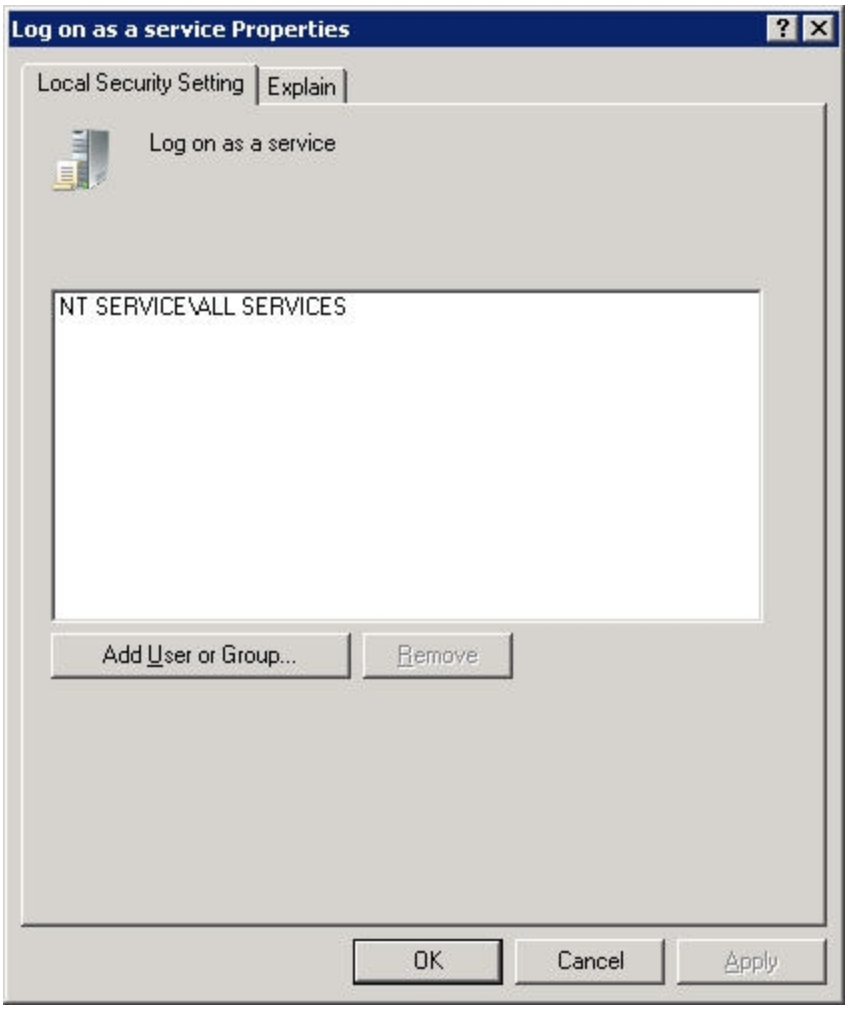

Figure 2.99: Adding a User or Group

- When Figure 2.100 appears, type the *system administrator's* user name in the format *domainname\username* in the **Enter the object names to select** text area, and click the **OK** button.

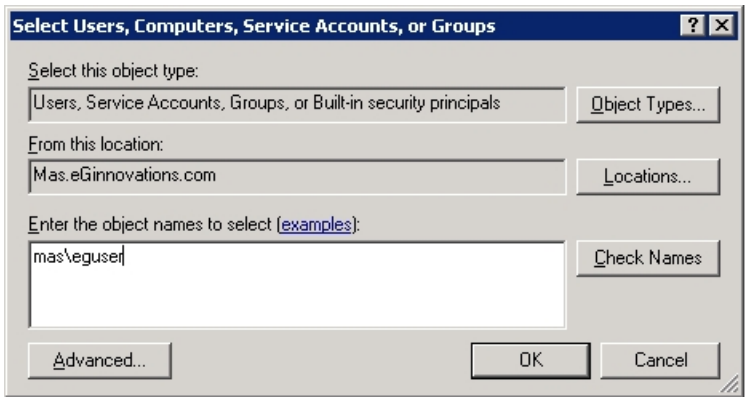

Figure 2.100: Adding the domainname\username of the user account being added

- Doing so will invoke Figure 2.101, where you will have to provide the credentials of the *system administrator* account being added. Then, click the **OK** button in Figure 2.101.

Figure 2.101: Providing the credentials of the user account being added

- Clicking the **OK** button in Figure 2.101 will lead you to Figure 2.102, where you will find that the *system administrator* account that you just added is available in the **Log on as a service** list. Click the **Apply** and **OK** buttons in Figure 2.102 to apply the changes.

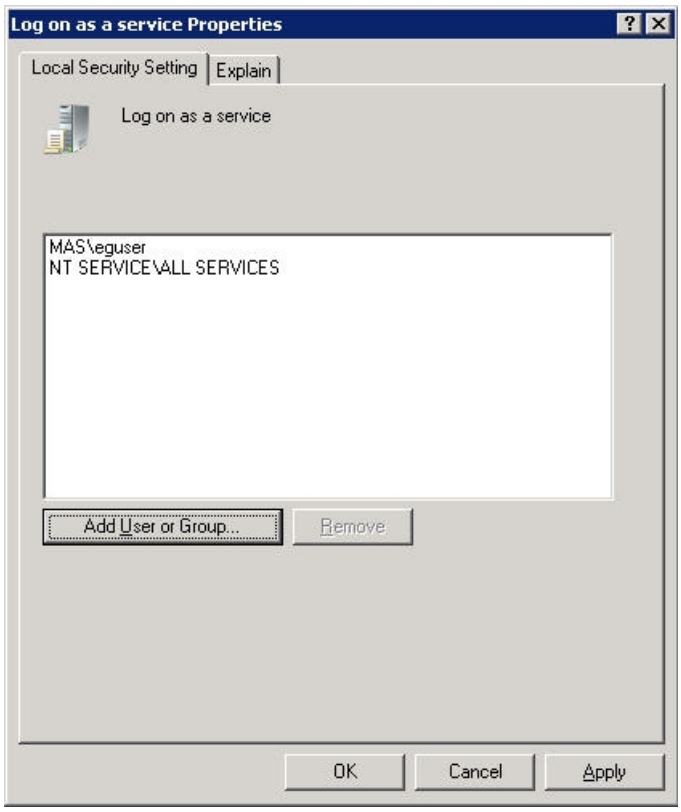

Figure 2.102: The newly added account available in the Log on as a service list

- Are the eG agent software and the **iss** files used for installing/uninstalling the agent available on the target host in the appropriate folder? The table below indicates where these files should be available on different versions of Windows, for remote operations to succeed.

Operating System	Location
Windows 2008 R2 32-bit	<EG_RAC_INSTALL_ DIR>\Windows 2008
Windows 2008 R2 64-bit	<EG_RAC_INSTALL_ DIR>\Windows_64 2008
Windows 2012 R2 32-bit	<EG_RAC_INSTALL_ DIR>\Windows 2012
Windows 2012 R2 64-bit	<EG_RAC_INSTALL_ DIR>\Windows_64 2012

8. Are the **ADMIN$** and **IPC$** shares on the target host accessible from the RAC host? If not, then agent installation/uninstallation will fail. To check whether these shares exist and are accessible, follow the simple steps discussed below:

- Login to the RAC host.
- To check whether the **ADMIN$** share, for instance, is available and accessible, from Start->Run, type **\\<IPAddress_of_RemoteHost\admin$**.
- If the **ADMIN$** share exists and the current login user is authorized to access the share, then you should be able to view the folder structure of the remote Windows host. In this case, you will not be prompted for authentication.
- If the **ADMIN$** share exists, but the current login user does not have access rights to the share, then the folder structure of the remote host will not appear. Instead, you will be prompted for valid login credentials.
- Provide the credentials of a user with rights to **ADMIN$** at the prompt. Upon authentication, you will be able to view the folder structure.
- On the other hand, if the **ADMIN$** share does not exist on the remote host, a message to that effect will appear.
- You can follow the same steps detailed above to check for the existence and accessibility of the **IPC$** share. The only difference would be to type **\\<IPAddress_of_RemoteHost\ipc$** in the **Run** box.
- If both these shares are not available, you will have to create them on the remote host. For that, do the following:
  - Login to the target system and go to the command prompt.
  - Type the command **net share**; this command will list all the default and user-configured shares on the system
  - If **ADMIN$** and **IPC$** are not listed, it is a definite indicator that the system does not consist of these shares.
  - To create these shares, issue the following commands one after another from the command prompt of the target Windows system:

    net share admin$
    net share IPC$