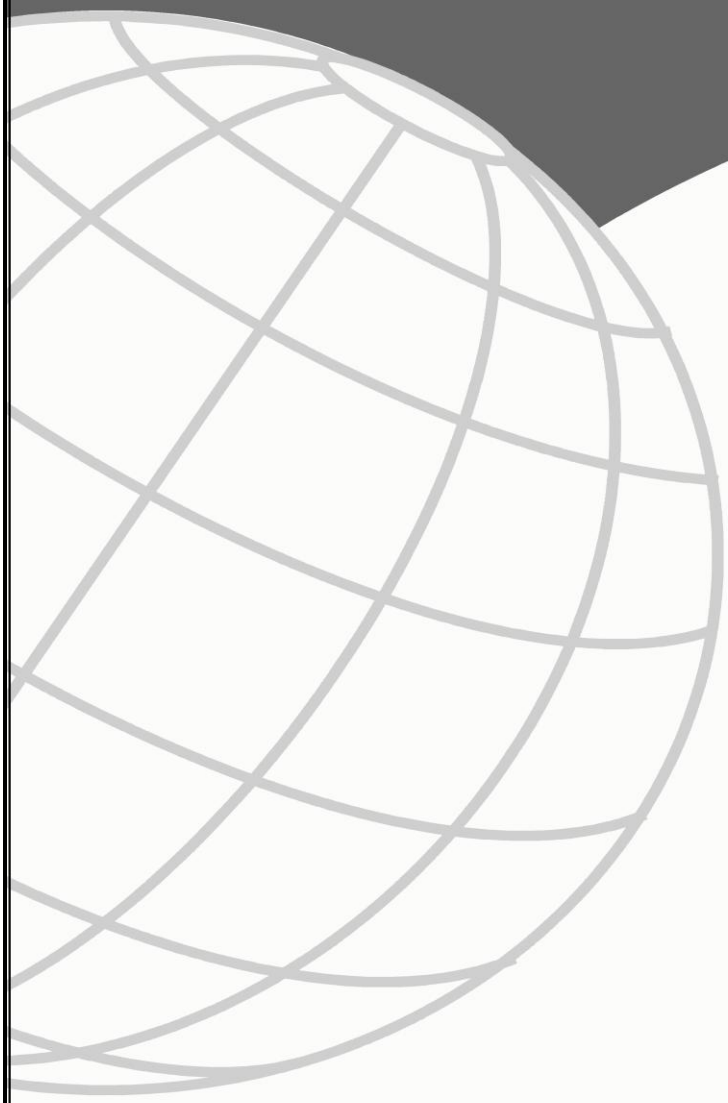

Enabling Service Excellence

Monitoring Microsoft Virtual Servers

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations, Inc. eG Innovations, Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

The copyright in this document belongs to eG Innovations, Inc. Complying with all applicable copyright laws is the responsibility of the user.

Table of Contents

MONITORING MICROSOFT VIRTUAL SERVERS **1**

1.1 How does eG Enterprise Monitor the MS Virtual Server? 2
1.2 Pre-requisites for Obtaining the "Inside View" of VMs on an MS Virtual Server 3
1.2.1 *Enabling ADMIN$ Share Access on the Guest Operating Systems* *3*
1.2.2 *Installing and Configuring the eG VM Agent* *9*
1.3 The Operating System Layer 12
1.3.1 *VirtualServerMemory Test* *13*
1.4 The Network Layer 14
1.5 The Tcp Layer 15
1.6 The VM Processes Layer 15
1.6.1 *VsEventLog Test* *16*
1.7 The Windows Service Layer 20
1.8 The Outside View of VMs Layer 20
1.8.1 *Virtual Machine Details Test* *21*
1.8.2 *Virtual Machine Status Test* *25*
1.9 The Inside View of VMs Layer 27
1.9.1 *VsgDiskSpace Test* *28*
1.9.2 *VsgDiskActivity Test* *30*
1.9.3 *System – Guest Test* *34*
1.9.4 *Tcp - Guest Test* *37*
1.9.5 *TcpTraffic - Guest Test* *39*
1.9.6 *WindowsMemory - Guest Test* *42*
1.9.7 *VsgNetworkTraffic – Windows Test* *46*
1.10 Correlation between Applications in a Virtualized Environment 49
1.11 Troubleshooting 51

CONCLUSION **61**

Chapter 1

Monitoring Microsoft Virtual Servers

Virtual Server 2005 R2 is a cost-effective server virtualization technology engineered for the Windows Server System™ platform. As a key part of any server consolidation strategy, Virtual Server increases hardware utilization and enables organizations to rapidly configure and deploy new servers. It improves operational efficiency in consolidating infrastructure, applications, and branch office server workloads, consolidating and re-hosting legacy applications, automating and consolidating software test and development environments, and reducing disaster impact.

Virtual Server 2005 R2 is a multithreaded application that runs as a system service, with each virtual machine running in its own thread of execution; I/O (input/output) occurs in child threads. Virtual Server 2005 R2 derives two core functions from the host operating system: 1) the underlying host operating system kernel schedules CPU resources, and 2) device drivers of the host operating system provide access to system devices. The Virtual Server 2005 R2 Virtual Machine Monitor (VMM) provides the software infrastructure to create virtual machines, manage instances, and interact with guest operating systems. Figure 1 illustrates the Virtual Server 2005 R2 architecture.

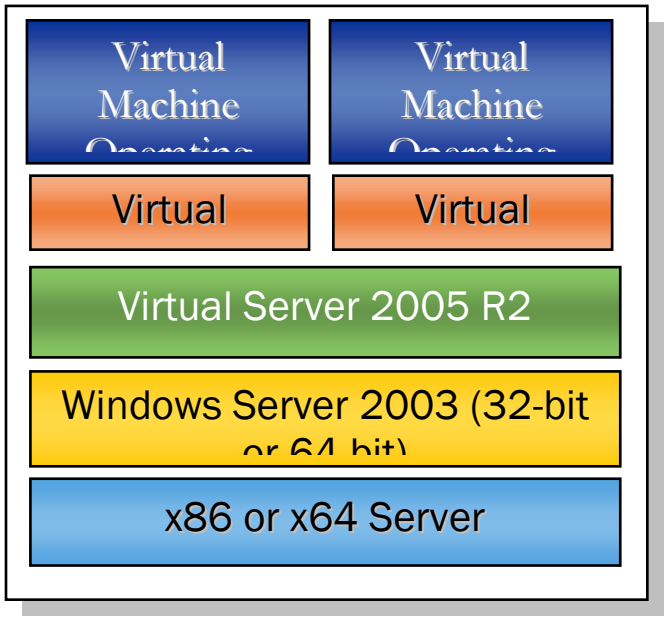

Figure 1: Virtual Server architecture

As the individual VMs on a Microsoft Virtual server share the CPU resources and device drivers of the host, resource contention at the host can degrade the performance of the VMs and the applications executing on them. At the same time, resource-intensive processes/applications executing on one/more guests can also erode the resources allocated to the guests and consequently affect application health. If one/more of these virtualized applications are participating in the delivery of a critical end-user service, then slowdowns experienced by the applications can adversely impact the service quality. Service operators should therefore carefully observe the resource usage of guests both from within and outside the guests, and accordingly fine-tune resource allocations, so as to ensure the optimal performance of the virtual infrastructure and the business-critical service riding on it.

eG Enterprise offers a 100% web-based *Microsoft Virtual Server 2005* (see Figure 2) monitoring model, which provides 'In-N-Out' monitoring of the Microsoft Virtual Server. A single eG agent deployed on the virtual server is capable of monitoring the resource usage of the guests in relation to the physical resources available to the virtual server host (which makes up the "outside" view). The same agent can also send probes into the individual virtual machines to monitor how effectively each guest uses the allocated resources (this makes up the "inside" view). Both these views enable administrators to proactively identify potential resource inadequacies, while accurately isolating the root-cause of the resource crunch – is it the virtual server host? or is it owing to one/more guests?

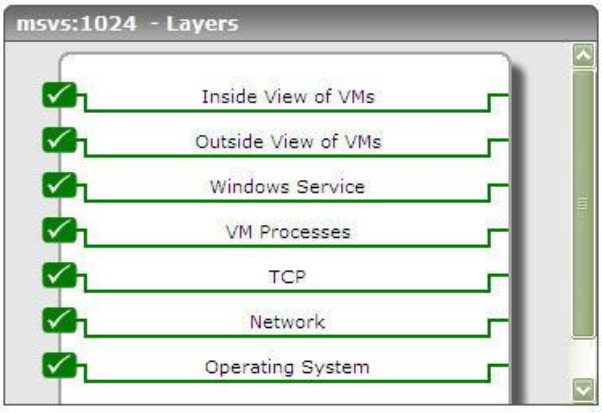

Figure 2: Layer model of the Microsoft Virtual Server

The eG agent deployed on the virtual server executes a variety of the tests on the host and the guests, and extracts a plethora of statistics pertaining to the health of the virtual server host and its VMs. These tests and the metrics they report are mapped to the layers depicted by Figure 2 above.

1.1 How does eG Enterprise Monitor the MS Virtual Server?

eG Enterprise prescribes an **agent-based approach** to monitor the Microsoft Virtual Servers. A single eG agent deployed on the MS Virtual Server host extracts critical statistics pertaining to the health of the host using perfmon counters. The same agent automatically discovers the guests on the Virtual Server, reports the powered-on status of each guest so discovered, and also reports *outside view* metrics indicating how well each VM uses the physical resources of the host.

For obtaining the *inside* view, the eG agent, by default, remotely communicates with every VM on the server. To establish this remote connection, the eG agent needs to be configured with *domain administrator* privileges. However, administrators of highly secure environments might not be in favor of the idea of exposing the *domain administrator* credentials. For such environments, eG Enterprise

provides a specialized **eG VM Agent**; this agent, when deployed on each VM on the server, allows the eG agent to connect to a VM **without domain administrator privileges** and extract the *inside view*.

The next section discusses the pre-requisites that need to be fulfilled to enable the eG agent to obtain the *inside view*, with and without the eG VM agent.

1.2 Pre-requisites for Obtaining the "Inside View" of VMs on an MS Virtual Server

As already mentioned, the eG agent, by default, establishes a remote connection (using NetBIOS) with each VM on an MS Virtual Server to extract the *inside view*. If the *inside view* is to be obtained using this default mechanism, then the following pre-requisites need to be fulfilled:

- The **ADMIN$** share should be enabled for all virtual guests being monitored and the administrative account must have permissions to this share drive. Refer to Section 1.2.1 for a step-by-step procedure to achieve this.
- To enable the eG agent to communicate with the guest operating systems, an administrative account login and password (either a local account or a domain account) must be provided when configuring the eG monitoring.

On the other hand, if the **eG VM Agent** is to be used for obtaining the *inside view*, then the only pre-requisite here is that the **eG VM Agent** be deployed on each VM to be monitored. The steps for installing and configuring the **eG VM Agent** are detailed in Section 1.2.2.

1.2.1 Enabling ADMIN$ Share Access on the Guest Operating Systems

If the **ADMIN$** share is not available on any virtual guest, create the share using the procedure detailed below:

1. Open the Windows Explorer on the virtual machine, browse for the corresponding **Windows** directory in the C drive, right-click on it, and select the **Sharing** option from the shortcut menu.
2. If the **ADMIN$** share does not pre-exist on the Windows guest, then Figure 3 appears indicating the same.

Figure 3: The ADMIN$ share does not exist

On the other hand, if the **ADMIN$** share pre-exists, Figure 4 appears. In such a case, first, remove the **ADMIN$** share by selecting the **Do not share this folder** option from Figure 4 and clicking the **Apply** and **OK** buttons. After this, you will have to repeat step 1 of this procedure to open Figure 3. Then, proceed as indicated by step 3 onwards.

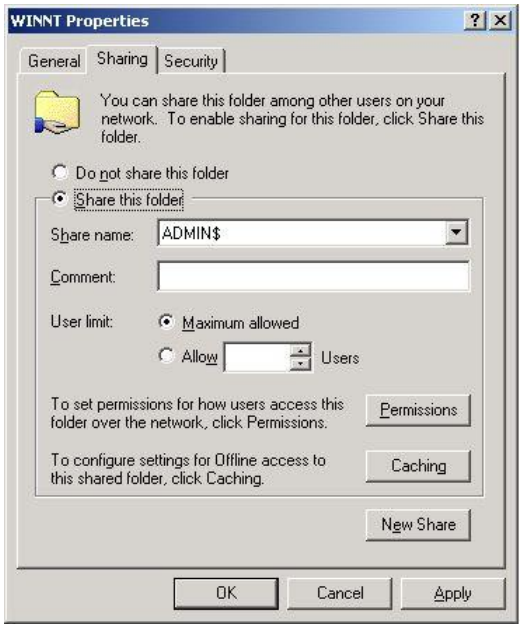

Figure 4: Admin$ share pre-exists

3. To create (or re-create) the **ADMIN$** share, select the **Share this folder** option from Figure 3, and provide **ADMIN$** share against the **Share name** text box (see Figure 5).

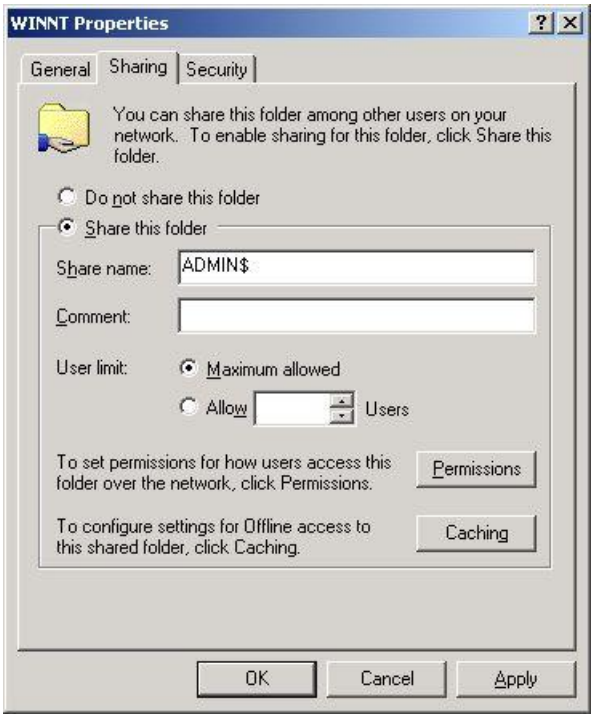

Figure 5: Creating the ADMIN$ share

4. Next, to enable the eG agent to communicate effectively with the Windows guest, you need to ensure that the permission to access the **ADMIN$** share is granted to an administrative user (local/domain); also, the **credentials of this user should be passed while configuring the eG monitoring capabilities** - i.e., while configuring the VMware tests. To grant the access permissions, click on the **Permissions** button in Figure 5.

5. By default, the **ADMIN$** share can be accessed by **Everyone** (see Figure 6). To grant access rights to a specific administrative (local/domain) user, select the **Add** button in Figure 6. When Figure 7 appears, select the domain to search from the **Look in** list. The valid user accounts configured on the chosen domain then appear in the box below. From this box, choose the administrator's account and click on the **Add** button to add the chosen user account to the box below the **Add** button.

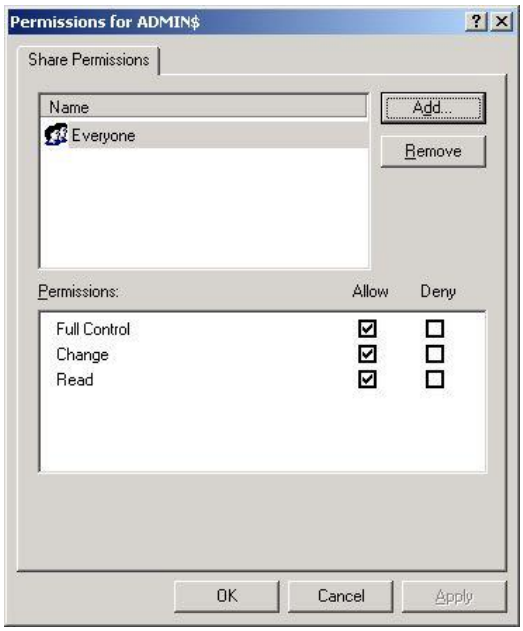

Figure 6: Clicking the Add button

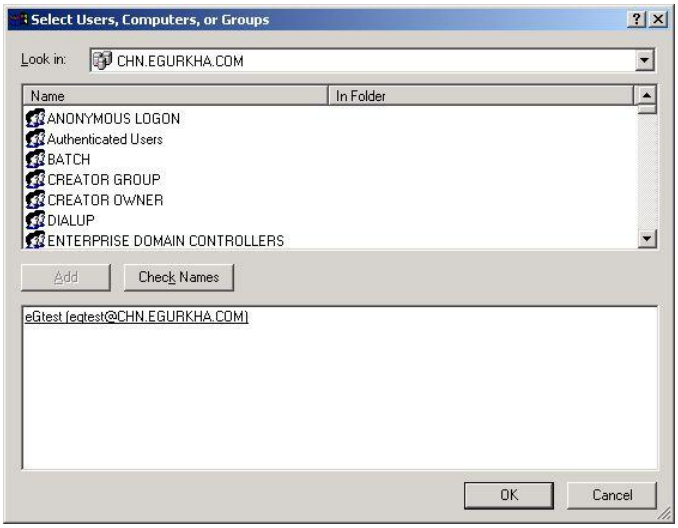

Figure 7: Selecting the administrative user to whom access rights are to be granted

6. Finally, click the **OK** button. You will then return to Figure 6, where the newly added administrator account will appear (see Figure 8).

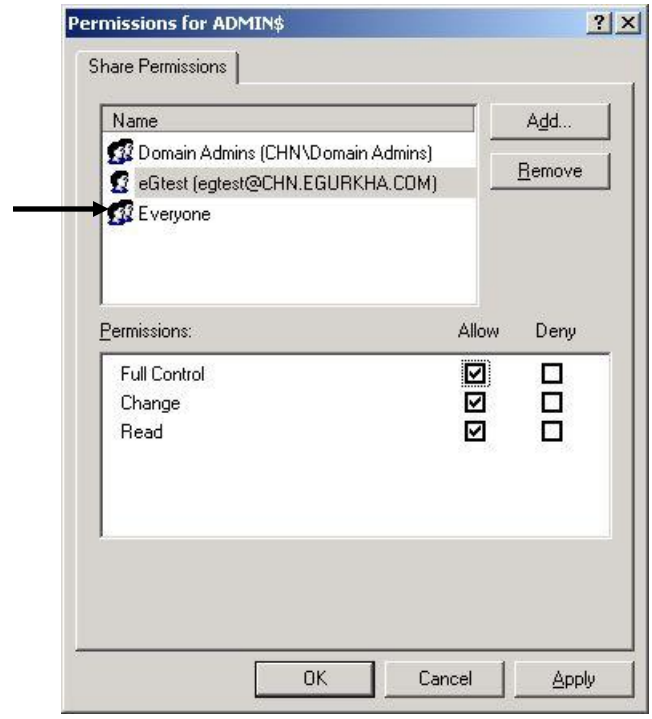

Figure 8: The administrator account granted access permissions

7. Select the newly added administrator account from Figure 8, and then, using the **Permissions** section, grant the administrator **Full Control**, **Change**, and **Read** permissions.
8. Finally, click the **Apply** and **OK** buttons in Figure 8 to register the changes.
9. Once you return to Figure 5, click on the **Security** tab (see Figure 9) to define the security settings for the **ADMIN$** share.

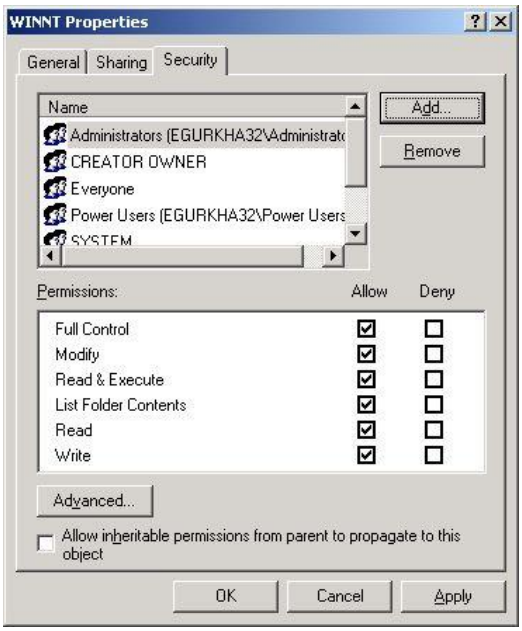

Figure 9: Defining the Security settings for the ADMIN$ share

10. Here again, you need to add the same administrator account, which was granted access permissions earlier. To do so, click the **Add** button in Figure 9, pick a domain from the **Look in** list of Figure 10, select the said administrator account from the domain users list below, and click the **Add** button (in Figure 10) to add the chosen account. Then, click the **OK** button in Figure 10.

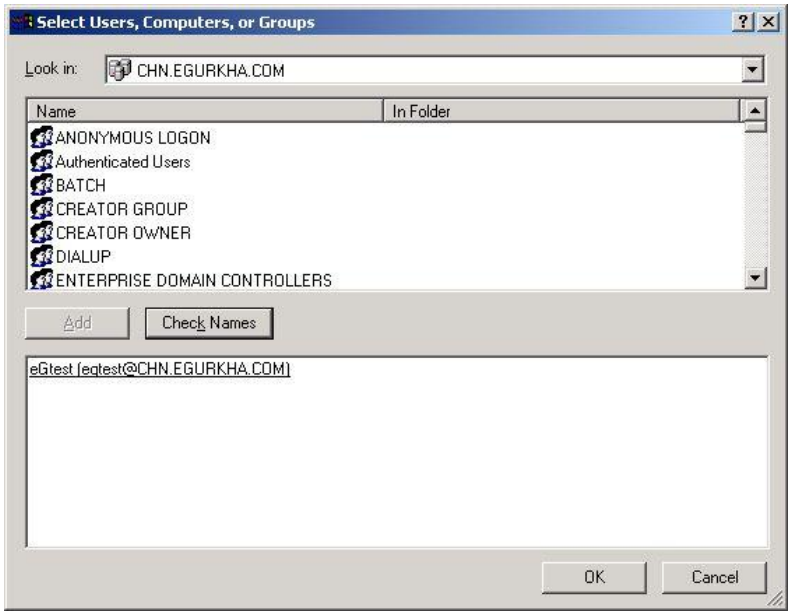

Figure 10: Adding the administrator account

11. This will bring you back to Figure 9, but this time, the newly added domain administrator account will be listed therein as indicated by Figure 11.

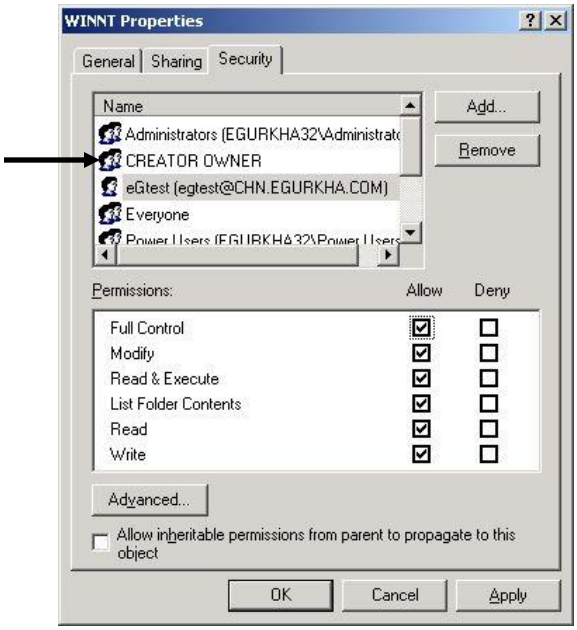

Figure 11: The Administrator account in the Security list

12. Finally, click the **Apply** and **OK** buttons in Figure 11.

1.2.2 Installing and Configuring the eG VM Agent

To install the eG VM agent on a guest, do the following:

1. Double-click on the **eGVMAgent.exe**.
2. Figure 12 then appears. Click on the **Next** button in Figure 12 to continue.

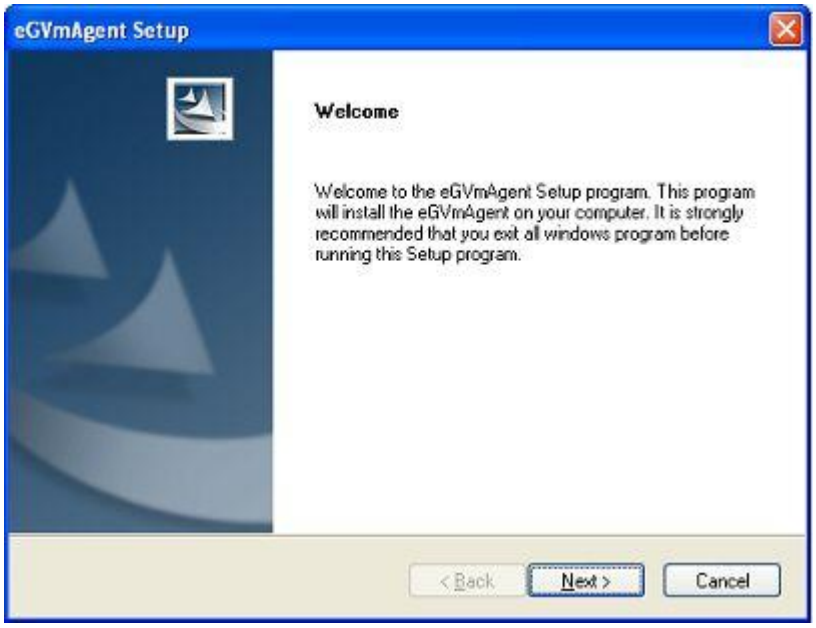

Figure 12: Welcome screen of the eG VM Agent installation wizard

3. When Figure 13 appears, click on **Yes** to accept the displayed license agreement.

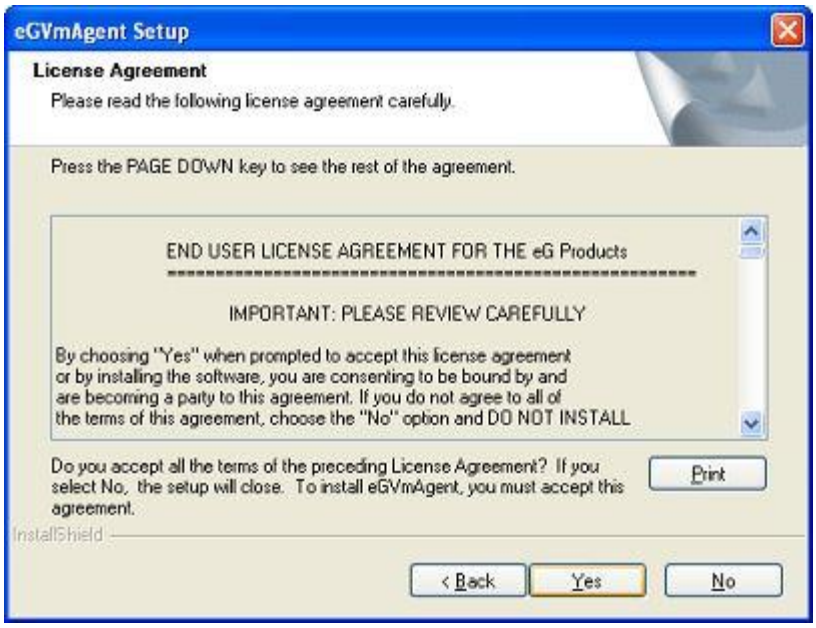

Figure 13: Accepting the license agreement

4. Use the **Browse** button in Figure 14 to indicate the location in which the agent should be installed, and click the **Next** button to proceed.

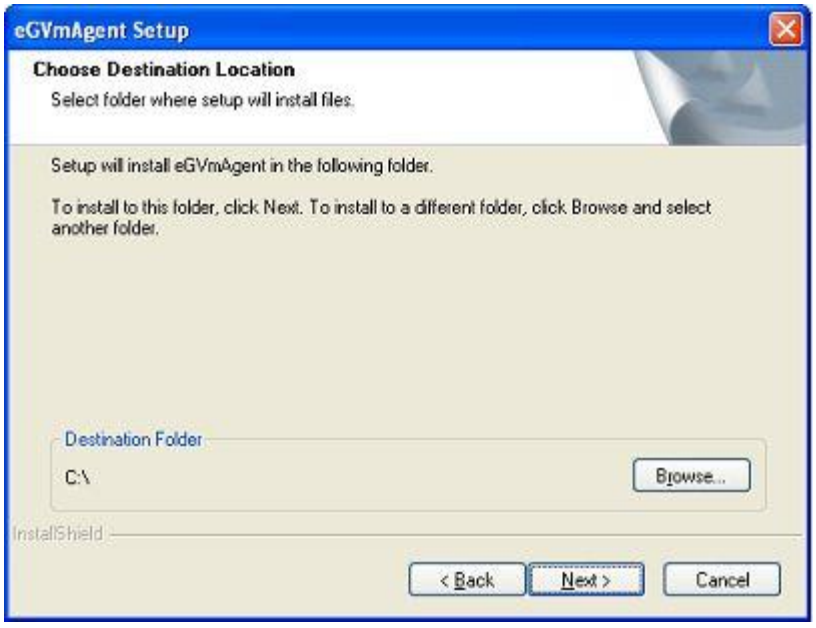

Figure 14: Specifying the install directory of the eG VM Agent

5. Next, specify the port at which the VM agent listens for requests from the eG agent. The default port is 60001. After port specification, click on the **Next** button in Figure 15 to proceed.

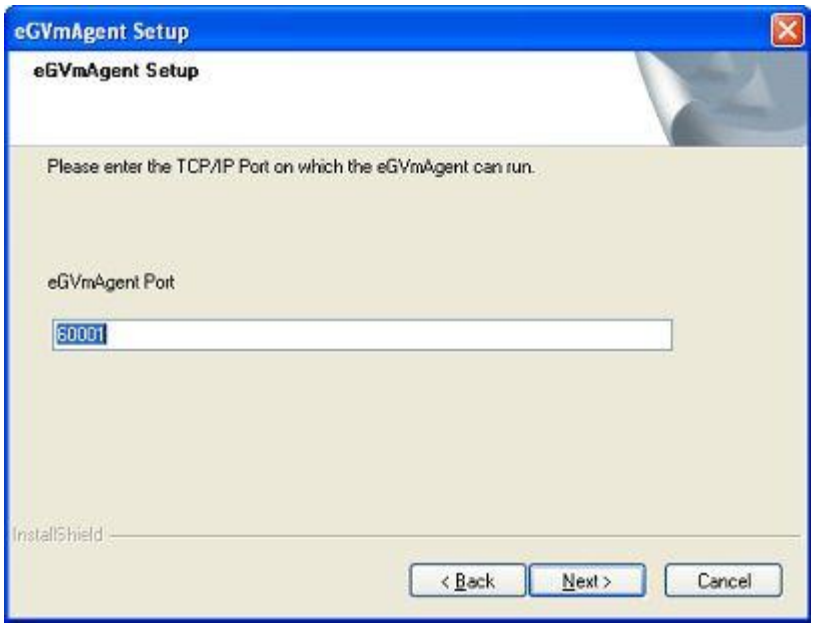

Figure 15: Specifying the VM agent port

6. A summary of your specifications then follows (see Figure 16). Click **Next** to proceed.

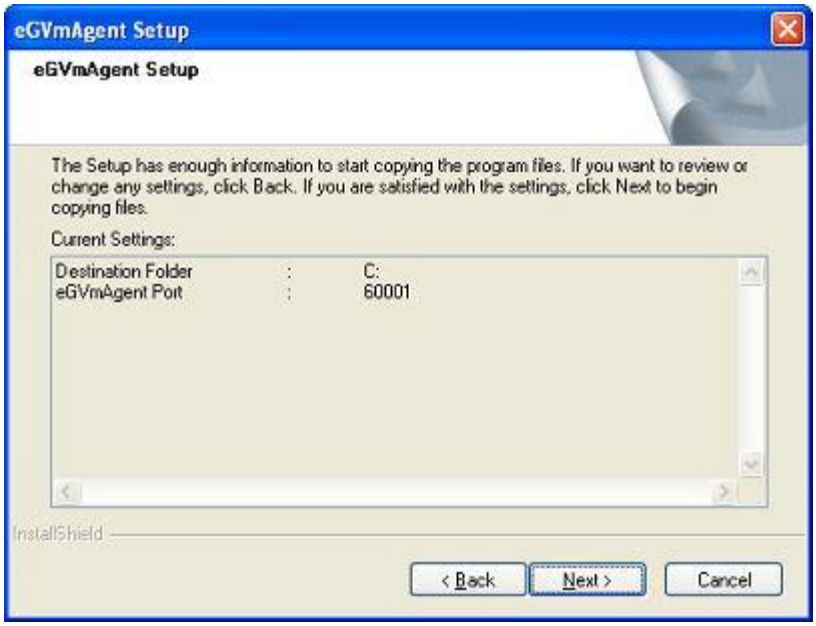

Figure 16: A summary of your specifications

7. Finally, click the **Finish** button in Figure 17 to complete the installation.

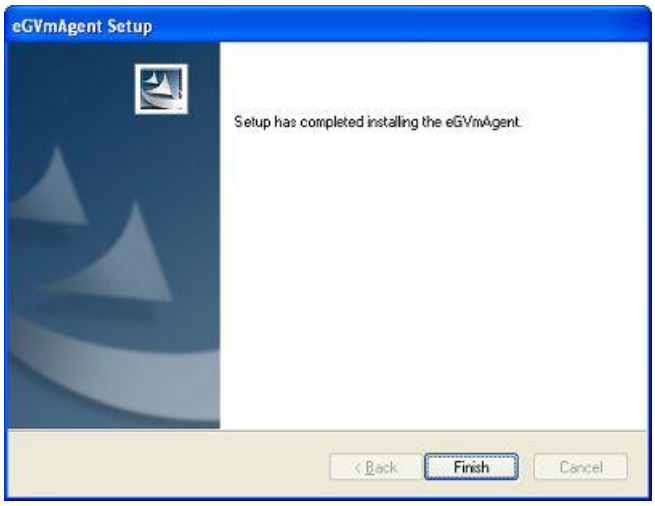

Figure 17: Finishing the installation

After installing the VM agent, you need to configure the eG agent to communicate with the eG VM agent for inside-view metrics. For this, you need to follow the steps given below:

- Login to the eG manager host.
- Edit the **eg_tests.ini** file in the **<EG_INSTALL_DIR>\manager\config** directory.
- The **WmiInsideViewPort** parameter in the **[AGENT_SETTINGS]** section of the file is set to **60001** by default. If the eG VM agent's port is changed at the time of installation, then you will have to ensure that this parameter reflects the new port. Therefore, change the default port specification accordingly.
- Save the file.

Once installed and configured, the eG VM agent starts automatically and begins listening for requests at the configured port. The eG agent, when configured to use the eG VM agent for obtaining the "inside view" (i.e., if the **INSIDE VIEW USING** flag is set to **eG VM Agent (Windows)** for the "inside view" tests), polls every eG VM agent at configured intervals for the "inside view" metrics. Upon receipt of request from the eG agent, the eG VM agent extracts the desired metrics from the Windows VM, which are then downloaded by the eG agent and reported to the eG manager.

The sections to come discuss the *inside view*, *outside view*, and host-level metrics reported by the single eG agent, in great detail.

1.3 The Operating System Layer

The **Operating System** layer reveals how effectively the virtual server host uses the physical memory and disk resources.

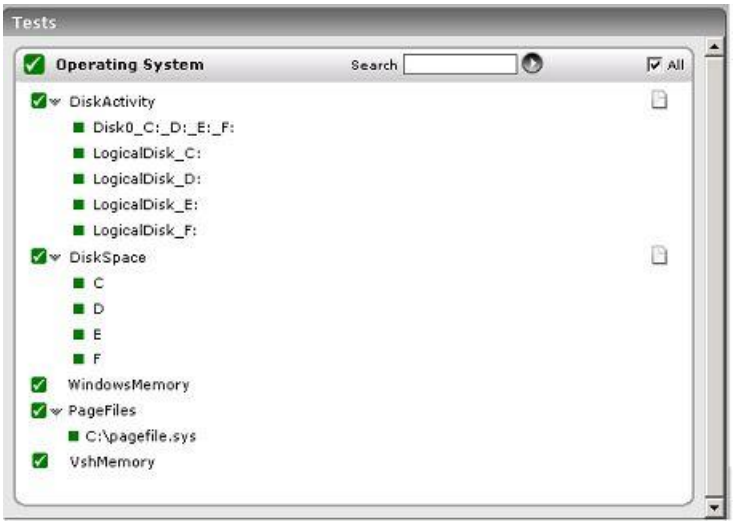

Figure 18: Tests mapped to the Operating System layer

The following section discusses the VirtualServerMemory test alone, as all other tests depicted by Figure 3 have been elaborately discussed in the *Monitoring Unix and Windows Servers* document.

1.3.1 VirtualServerMemory Test

This test indicates the memory usage of the MS Virtual server, and enables administrators to judge whether/not adequate free memory is available on the virtual host.

Purpose	Indicates the memory usage of the MS Virtual server, and enables administrators to judge whether/not adequate free memory is available on the virtual host
Target of the test	A Virtual Server
Agent deploying the test	An internal agent

<table>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD - How often should the test be executed
2. HOST - The host for which the test is to be configured.
3. PORT - The port at which the HOST listens.
4. DOMAIN - Specify the DOMAIN within which the virtual guests reside. If the guests belong to a specific domain, an administrative account in that domain can be provided in the ADMIN USER field. On the other hand, if the guests belong to different domains, specify "none" in the DOMAIN field, and specify a local administrator account name in the ADMIN USER field below. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored.
5. ADMIN USER - This test connects to each virtual guest and extracts statistics of interest from every guest. In order to do so, the test must be configured with user privileges that allow a remote connection to the virtual guest from the virtual host. If the virtual guests are within a DOMAIN, then provide a domain administrator account name in the ADMIN USER text box. If the DOMAIN parameter is set to "none", then a local administrator account has to be specified in the ADMIN USER text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. In either case, the eG agent should be able to connect to each guest operating system.
6. ADMIN PASSWORD - The password of the ADMIN USER needs to be provided here.
7. CONFIRM PASSWORD – Confirm the ADMIN PASSWORD by retyping it here.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Virtual server monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Total memory:
Indicates the total amount of physical memory installed.</td><td>MB</td><td></td></tr>
<tr><td>Memory available:
Indicates the amount of physical memory that is currently available for use.</td><td>MB</td><td>A very low value of this measure is indicative of excessive usage of physical memory by the virtual host.</td></tr>
</table>

1.4 The Network Layer

Using the tests mapped to this layer, administrators can figure out whether the virtual server is available over the network or not, and also analyze the data traffic handled by the virtual server and each of the network interfaces supported by the server.

Figure 19: The tests associated with the Network layer

The tests depicted by Figure 19 have all been dealt with extensively in the *Monitoring Unix and Windows Servers* document.

1.5 The Tcp Layer

The TCP connectivity of the virtual server host and the ratio of TCP retransmissions are measured by the tests associated with this layer.

Figure 20: The tests mapped to the Tcp layer

The tests depicted by Figure 20 have all been dealt with extensively in the *Monitoring Unix and Windows Servers* document.

1.6 The VM Processes Layer

Using the tests associated with this layer, you can:

- Check whether the critical virtual server processes are running;
- Identify resource-intensive processes executing on the host;
- Determine whether error events/warning events have occurred on the host

Figure 21: The tests associated with the VM Processes Layer

The **Processes** test indicated by Figure 21 has already been dealt with in the *Monitoring Unix and Windows Servers* document. Let us therefore focus on the **VsEventLog** test instead.

1.6.1 VsEventLog Test

The VsEventLog test reports statistical information about the application error and warning events generated by the target virtual host.

Purpose	Reports statistical information about the application error and warning events generated by the target virtual host
Target of the test	A Microsoft virtual server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured 3. **PORT –** Refers to the port used by the EventLog Service. Here it is null. 4. **POLICY BASED FILTER** - Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: ➢ Manually specify the event sources, IDs, and descriptions in the **FILTER** text area, or, ➢ Select a specification from the predefined filter policies listed in the **FILTER** box For explicit, manual specification of the filter conditions, select the **NO** option against the **POLICY BASED FILTER** field. This is the default selection. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the **YES** option against the **POLICY BASED FILTER** field. 5. **FILTER** - If the **POLICY BASED FILTER** flag is set to **NO**, then a **FILTER** text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that the **FILTER** text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here: ➢ *OS_events* is the display name that will appear as a descriptor of the test in the monitor UI; ➢ *all* indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify *none*. ➢ Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, *Browse* and *Print* have been excluded from monitoring. Alternatively, you can use *all* to indicate that all the event sources have to be excluded from monitoring, or *none* to denote that none of the event sources need be excluded. ➢ In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The *all* in our example represents that all the event IDs need to be considered while monitoring. ➢ Similarly, the *none* (following *all* in our example) is indicative of the fact that none of the event IDs need to be excluded from monitoring. On the other hand, if you want to instruct the eG Enterprise system to ignore a few event IDs during monitoring, then provide the IDs as a comma-separated list. Likewise, specifying *all* makes sure that all the event IDs are excluded from monitoring.

- The *all* which follows implies that all events, regardless of description, need to be included for monitoring. To exclude all events, use *none*. On the other hand, if you provide a comma-separated list of event descriptions, then the events with the specified descriptions will alone be monitored. Event descriptions can be of any of the following forms - *desc**, or *desc*, or **desc**,or *desc**, or *desc1*desc2*, etc. *desc* here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
- In the same way, you can also provide a comma-separated list of event descriptions to be excluded from monitoring. Here again, the specification can be of any of the following forms: *desc**, or *desc*, or **desc**,or *desc**, or *desc1*desc2*, etc. *desc* here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. In our example however, none is specified, indicating that no event descriptions are to be excluded from monitoring. If you use *all* instead, it would mean that all event descriptions are to be excluded from monitoring.

By default, the **FILTER** parameter contains the value*: all:all:none:all:none:all:none*. Multiple filters are to be separated by semi-colons (;).

Note:

The event sources and event IDs specified here should be exactly the same as that which appears in the Event Viewer window.

On the other hand, if the **POLICY BASED FILTER** flag is set to **YES**, then a **FILTER** list box will appear, displaying the filter policies that pre-exist in the eG Enterprise system. A filter policy typically comprises of a specific set of event sources, event IDs, and event descriptions to be monitored. This specification is built into the policy in the following format:

{Policyname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}

To monitor a specific combination of event sources, event IDs, and event descriptions, you can choose the corresponding filter policy from the **FILTER** list box. Multiple filter policies can be so selected. Alternatively, you can modify any of the existing policies to suit your needs, or create a new filter policy. To facilitate this, a **Click here** link appears just above the test configuration section, once the **YES** option is chosen against **POLICY BASED FILTER**. Clicking on the **Click here** link leads you to a page where you can modify the existing policies or create a new one (refer to the *Monitoring Even tLogs* document). The changed policy or the new policy can then be associated with the test by selecting the policy name from the **FILTER** list box in this page.

<table>
<tr><td></td><td colspan="3">6. USEWMI - The eG agent can either use WMI to extract event log statistics or directly parse the event logs using event log APIs. If the USEWMI flag is YES, then WMI is used. If not, the event log APIs are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set the USEWMI parameter value to NO.
7. DD FREQUENCY - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying none against DDFREQ.
8. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
➢ The eG manager license should allow the detailed diagnosis capability
➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the FILTER configured</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Information messages:
This refers to the number of information events generated when the test was last executed.</td><td>Number</td><td>A change in the value of this measure may indicate infrequent but successful operations performed by one or more processes on the virtual server.

Please check the detailed diagnosis of this measure (if available), for more details.</td></tr>
<tr><td>Warnings:
This refers to the number of warnings that were generated when the test was last executed.</td><td>Number</td><td>A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems.

Please check the the detailed diagnosis of this measure (if available), for more details.</td></tr>
</table>

	Errors: This refers to the number of virtual server error events that were generated.	Number	A very low value (zero) indicates that the virtual host is in a healthy state and all processes are running smoothly without any potential problems. An increasing trend or high value indicates the existence of problems like loss of functionality or data in one or more processes on the virtual host. Please check the detailed diagnosis of this measure (if available), for more details. Please check the Virtual Server Logs for more details.

1.7 The Windows Service Layer

This layer checks whether the virtual server service is currently running or not.

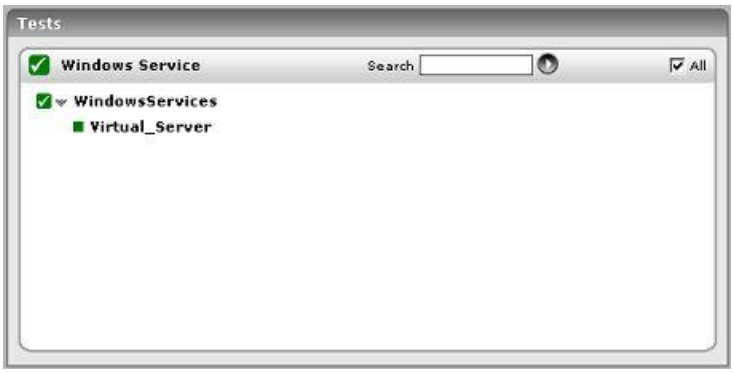

Figure 22: The tests associated with the Windows Service layer

The **WindowsServices** test mapped to this layer has already been discussed in the *Monitoring Unix and Windows Servers* document. Therefore, let us proceed to look at the next layer.

1.8 The Outside View of VMs Layer

The **Outside View of VMs** layer represents the host's view of the resource usage levels of each of the VM guests hosted on it. Using the information reported by this test, administrators can:

- Determine which of the VM guests is taking up more resources (CPU, memory, network, or disk) than the others. This information can help with load balancing or capacity planning.
- Determine times when sudden or steady spikes in the physical resource utilization are caused by the guest machines
- Track the overall status of the virtual machines – how many are registered, which ones are powered on, and at what times, etc.

Figure 23: The tests mapped to the Outside View of VMs Layer

1.8.1 Virtual Machine Details Test

This test monitors the amount of the physical server's resources that each guest on an MS Virtual server is taking up. Using the metrics reported by this test, administrators can determine which virtual guest is taking up most CPU, which guest is generating the most network traffic, which guest is taking up the maximum memory utilization, which guest has the maximum disk activity, etc. Note that the amount of resources taken up by a virtual guest will be limited by the resource allocations that have been made by administrators. For example, an administrator could cap the amount of memory that a specific guest may take.

Purpose	Monitors the amount of the physical server's resources that each guest on an MS Virtual server is taking up
Target of the test	A Virtual Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **INSIDE VIEW USING** - By default, this test communicates with every VM remotely and extracts "inside view" metrics. Therefore, by default, the **INSIDE VIEW USING** flag is set to **Remote connection to VM (Windows)**. Typically, to establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. In high-security environments, where the IT staff might have reservations about exposing the credentials of their domain administrators, this approach to extracting "inside view" metrics might not be preferred. In such environments therefore, eG Enterprise provides administrators the option to deploy a piece of software called the **eG VM Agent** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** Refer to Section 1.2.2 for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 5. **DOMAIN, ADMIN USER, ADMIN PASSWORD,** and **CONFIRM PASSWORD** – By default, this test connects to each virtual guest remotely and attempts to collect "inside view" metrics. In order to obtain a remote connection, the test must be configured with user privileges that allow remote communication with the virtual guests. The first step towards this is to specify the **DOMAIN** within which the virtual guests reside. The **ADMIN USER** and **ADMIN PASSWORD** will change according to the **DOMAIN** specification. Discussed below are the different values that the **DOMAIN** parameter can take, and how they impact the **ADMIN USER** and **ADMIN PASSWORD** specifications: ▪ **If the VMs belong to a single domain** : If the guests belong to a specific domain, then specify the name of that domain against the **DOMAIN** parameter. In this case, any administrative user in that domain will have remote access to all the virtual guests. Therefore, an administrator account in the given domain can be provided in the **ADMIN USER** field and the corresponding password in the **ADMIN PASSWORD** field. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. ▪ **If the guests belong to different domains -** In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section 1.8.1.1 of this document. ▪ **If the INSIDE VIEW USING flag is set to 'eG VM Agent (Windows)'** – In this case, the inside view can be obtained without domain administrator privileges. Therefore, set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 6.

Outputs of the test	One set of results for every guest to the Virtual server monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Network traffic sent: Indicates the rate at which the guest transmitted data over the network.	KB/Sec	Comparing the data transmitted across all the virtual guests provides an indicator of the guest that is generating most out-bound network traffic.
	Network traffic received: Indicates the rate at which the guest received data over the network.	KB/Sec	Comparing the data received across all the virtual guests provides an indicator of the guest that has the most in-bound network traffic.
	Data read from disk: Indicates the rate at which data that was read from the disk by all IDE and SCSI controllers.	KB/Sec	
	Data written to disk: Indicates the rate at which data was written to the disk by all IDE and SCSI controllers.	KB/Sec	
	CPU utilization: Indicates the percentage of physical CPU used by the guest, currently.	Percent	A high value for this measure indicates a virtual machine that is using a lot of the processor - possibly because one or more processes on this VM are taking a lot of CPU.

1.8.1.1 Configuring Users for VM Monitoring

In order to enable the eG agent to connect to VMs in multiple domains and pull out metrics from them, the eG administrative interface provides a special page using which the different **DOMAIN** names, and their corresponding **ADMIN USER** names and **ADMIN PASSWORDS** can be specified. To access this page, just click on the **Click here** hyperlink in any of the VM test configuration pages.

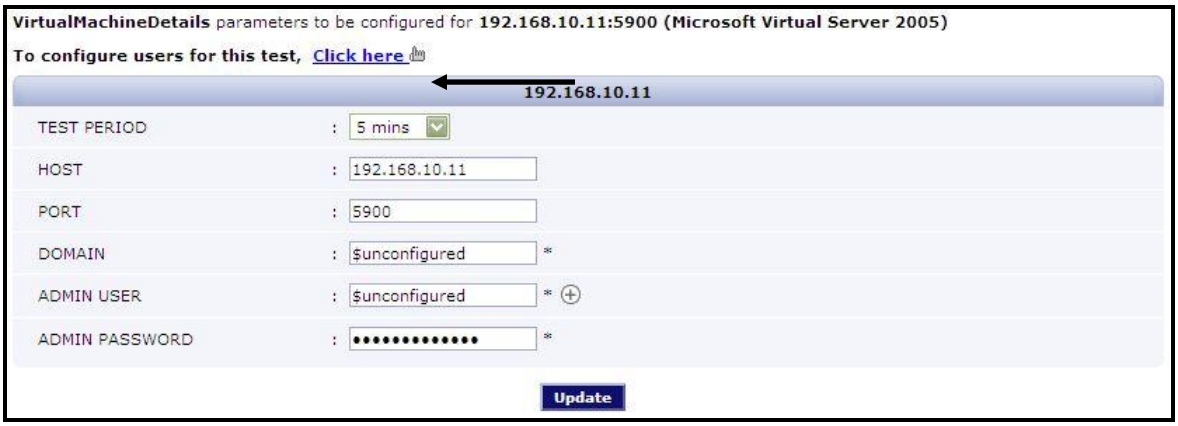

Figure 24: Configuring a VM test

Upon clicking, Figure 25 will appear, using which the VM user details can be configured.

Figure 25: The VM user configuration page

To add a user specification, do the following:

1. First, provide the name of the **Domain** to which the VMs belong (see Figure 25). If one/more VMs do not belong to any domain, then, specify *none* here.
2. The eG agent must be configured with user privileges that will allow the agent to communicate with the VMs in a particular domain and extract statistics. If a valid **Domain** name has been specified, then a domain administrator account can be provided in the **Admin User** text box.
3. The password of the specified **Admin User** should be mentioned in the **Admin Pwd** text box.
4. Confirm the password by retyping it in the **Confirm Pwd** text box.
5. To add more users, click on the ⊕ button in Figure 25. This will allow you to add one more user specification as depicted by Figure 26.

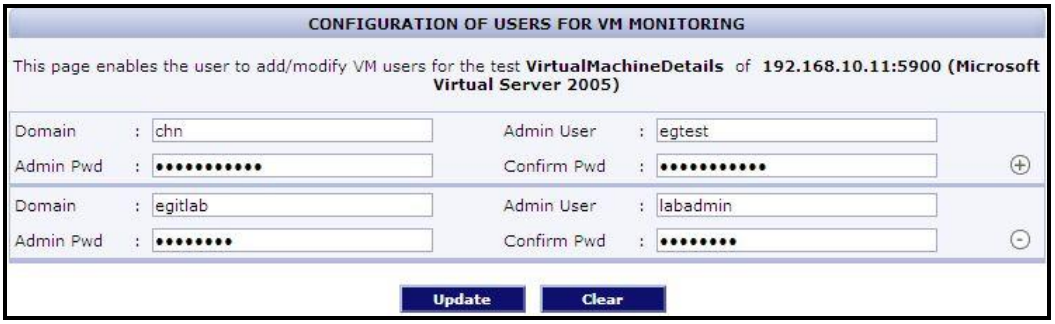

Figure 26: Adding another user

6. In some virtualized environments, the same **Domain** could be accessed using multiple **Admin User** names. For instance, to login to a **Domain** named *egitlab*, the eG agent can use the **Admin User** name *labadmin* or the **Admin User** name *jadmn*. You can configure the eG agent with the credentials of both these users as shown by Figure 27.

Figure 27: Associating a single domain with different admin users

When this is done, then, while attempting to connect to the domain, the eG agent will begin by using the first **Admin User** name of the specification. In the case of Figure 27, this will be *labadmin*. If, for some reason, the agent is unable to login using the first **Admin User** name, then it will try to login again, but this time using the second **Admin User** name of the specification – i.e., *jadmin* in our example (see Figure 27). If the first login attempt itself is successful, then the agent will ignore the second **Admin User** name.

7. To clear all the user specifications, simply click the **Clear** button in Figure 27.
8. To remove the details of a particular user alone, just click the ⊖ button in Figure 27.
9. To save the specification, just click on the **Update** button in Figure 27. This will lead you back to the test configuration page, where you will find the multiple domain names, user names, and passwords listed against the respective fields (see Figure 28).

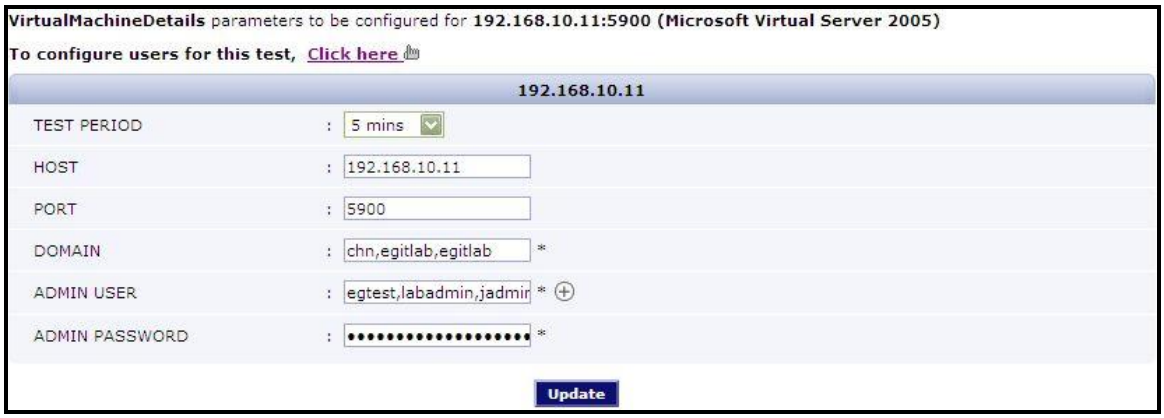

Figure 28: The test configuration page displaying multiple domain names, user names, and passwords

1.8.2 Virtual Machine Status Test

This test tracks the overall status of the VMs by reporting how many VMs have been configured on the virtual server, how many have been registered, how many were newly added/removed, etc.

Purpose	Overall status of the VMs by reporting how many VMs have been configured on the virtual server, how many have been registered, how many were newly added/removed, etc.		
Target of the test	A Virtual Server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **DETAILED DIAGNOSIS** - It is recommended that this flag be set to **ON** when executing this test on a virtual server. The **AutoVirtualMapping** feature will take effect only if the VirtualMachineStatus test is reporting detailed measures.		
Outputs of the test	One set of results for the Virtual server monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Registered guests: Indicates the total number of virtual machines that have been registered with the virtual server.	Number	
	Guests powered on: Indicates the number of guests that are currently powered on.	Number	To know which are the guests that are powered on, use the detailed diagnosis capability of this measure (if enabled).
	Added guests: Indicates the number of guests that were newly added to the virtual server during this measurement period.	Number	The detailed diagnosis of these measures, if enabled, lists the virtual machines that were migrated to or from (as the case may be) the virtual server.
	Removed guests: Indicates the number of guests that were newly removed from the virtual server during this measurement period.	Number	

The detailed diagnosis of the **Guests powered on** measure, if enabled, provides the IP addresses of the VMs configured on the virtual server, and the operating systems on which they are executing (see Figure 29).

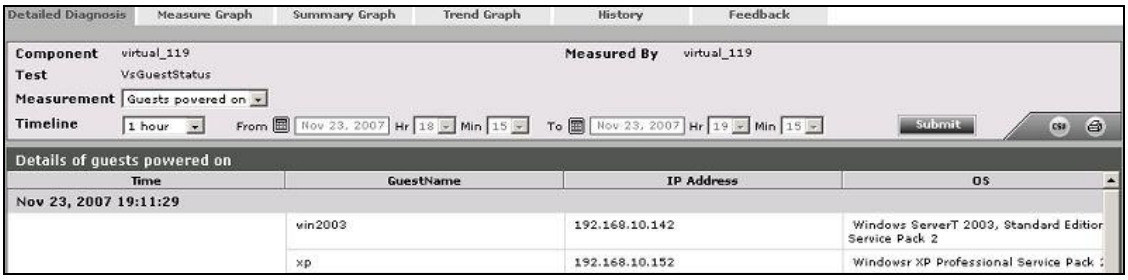

Figure 29: The detailed diagnosis of the Guests powered on measure

1.9 The Inside View of VMs Layer

The **Inside View of VMs** layer provides the individual guest operating system's view of the usage of the resources available to it.

By default, clicking on the **Inside View of VMs** layer invokes the **Server View** depicted by Figure 30. Using this view, you can quickly determine the health of each of the zones (including *global* zones) configured on the monitored Solaris host.

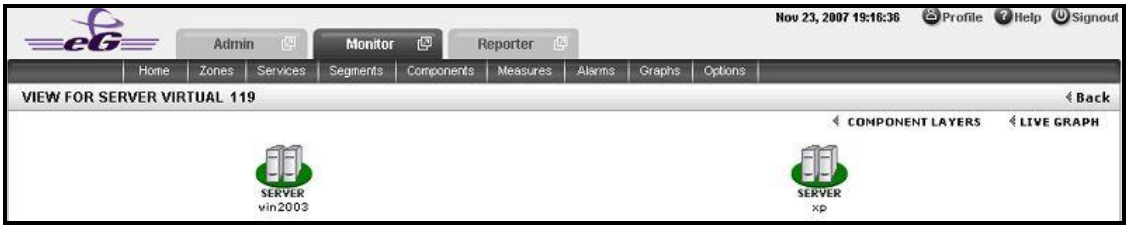

Figure 30: The Virtual Machine view

To zoom into the performance of a particular guest on the virtual server, click on a guest in Figure 30. This will lead you to a page that displays all the metrics that the eG agent collected from that guest. You are thus enabled to cross-correlate across the various metrics, and quickly detect the root-cause of current/probable disturbances to the internal health of a guest. To view the time-of-day variations in a measure, simply click on a measure in the page.

To view real-time graphs of pre-configured measures (pertaining to the virtual server and the guests operating on it), click on the **LIVE GRAPH** link in Figure 30. The graph display that appears subsequently has been organized in such a way that next to every host-pertinent measure graph, the closely related guest-specific measure graph appears. For instance, next to the graph of the CPU utilized' measure of the **VsGuest** test, you will find a graph of the ' CPU utilization' measure of the **Processor** test. This way, you can easily compare and correlate how well the physical CPU resources are being utilized by both the host's processes and those that are executing on the guests. On the basis of this analysis, you can proactively isolate potential performance issues, and also determine the root-cause of the issue - is it the host? or is it the guest?

If you prefer to view the tests associated with the **Inside View of VMs** layer instead of guest-specific measures or live graphs, then, simply click on the **COMPONENT LAYERS** link in Figure 30. This will lead you back to the layer model page, wherein you can view the complete list of tests associated with the **Inside View of VMs** layer (see Figure 31).

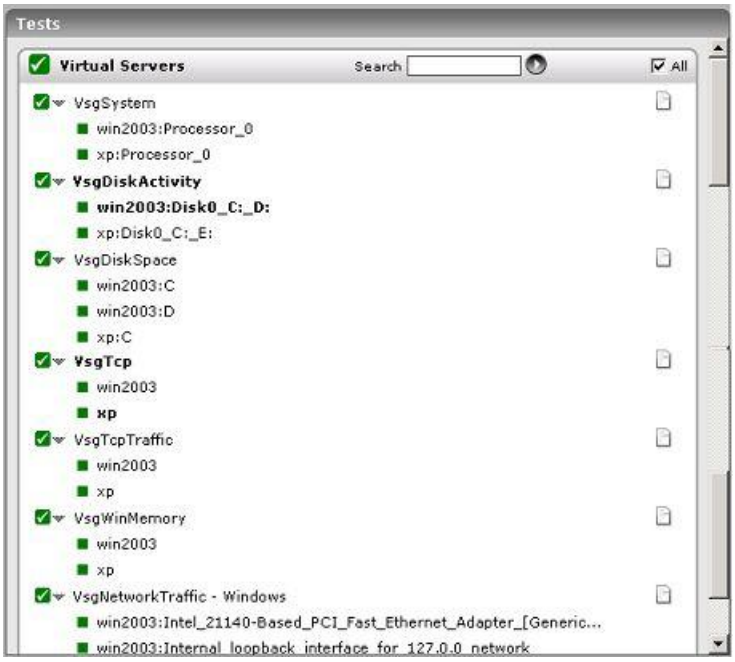

Figure 31: The tests mapped to the Virtual Servers layer

1.9.1 VsgDiskSpace Test

This test measures the space usage of every disk partition on each virtual machine of a Microsoft virtual server.

Purpose	Measures the space usage of every disk partition on each virtual machine of a Microsoft virtual server
Target of the test	A Microsoft Virtual Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **INSIDE VIEW USING** - By default, this test communicates with every VM remotely and extracts "inside view" metrics. Therefore, by default, the **INSIDE VIEW USING** flag is set to **Remote connection to VM (Windows)**. Typically, to establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. In high-security environments, where the IT staff might have reservations about exposing the credentials of their domain administrators, this approach to extracting "inside view" metrics might not be preferred. In such environments therefore, eG Enterprise provides administrators the option to deploy a piece of software called the **eG VM Agent** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** Refer to Section 1.2.2 for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 5. **DOMAIN, ADMIN USER, ADMIN PASSWORD,** and **CONFIRM PASSWORD** – By default, this test connects to each virtual guest remotely and attempts to collect "inside view" metrics. In order to obtain a remote connection, the test must be configured with user privileges that allow remote communication with the virtual guests. The first step towards this is to specify the **DOMAIN** within which the virtual guests reside. The **ADMIN USER** and **ADMIN PASSWORD** will change according to the **DOMAIN** specification. Discussed below are the different values that the **DOMAIN** parameter can take, and how they impact the **ADMIN USER** and **ADMIN PASSWORD** specifications: ▪ **If the VMs belong to a single domain** : If the guests belong to a specific domain, then specify the name of that domain against the **DOMAIN** parameter. In this case, any administrative user in that domain will have remote access to all the virtual guests. Therefore, an administrator account in the given domain can be provided in the **ADMIN USER** field and the corresponding password in the **ADMIN PASSWORD** field. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. ▪ **If the guests belong to different domains -** In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section 1.8.1.1 of this document. ▪ **If the INSIDE VIEW USING flag is set to 'eG VM Agent (Windows)'** – In this case, the inside view can be obtained without domain administrator privileges. Therefore, set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 6.

Outputs of the test	One set of results for each disk partition on every zone monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total capacity: Indicates the total capacity of a disk partition.	MB	
	Used disk space: Indicates the amount of space used in a disk partition.	MB	
	Free disk space: Indicates the current free space available for each disk partition of a guest.	MB	
	Disk utilization: Indicates the percentage of space usage on each disk partition of a guest.	Percent	A value close to 100% can indicate a potential problem situation where applications executing on the guest may not be able to write data to the disk partition(s) with very high usage.

1.9.2 VsgDiskActivity Test

This test reports statistics pertaining to the input/output utilization of each physical disk on a guest.

Purpose	Reports statistics pertaining to the input/output utilization of each physical disk on a guest
Target of the test	A Microsoft Virtual Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **INSIDE VIEW USING** - By default, this test communicates with every VM remotely and extracts "inside view" metrics. Therefore, by default, the **INSIDE VIEW USING** flag is set to **Remote connection to VM (Windows)**. Typically, to establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. In high-security environments, where the IT staff might have reservations about exposing the credentials of their domain administrators, this approach to extracting "inside view" metrics might not be preferred. In such environments therefore, eG Enterprise provides administrators the option to deploy a piece of software called the **eG VM Agent** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** Refer to Section 1.2.2 for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 5. **DOMAIN, ADMIN USER, ADMIN PASSWORD,** and **CONFIRM PASSWORD** – By default, this test connects to each virtual guest remotely and attempts to collect "inside view" metrics. In order to obtain a remote connection, the test must be configured with user privileges that allow remote communication with the virtual guests. The first step towards this is to specify the **DOMAIN** within which the virtual guests reside. The **ADMIN USER** and **ADMIN PASSWORD** will change according to the **DOMAIN** specification. Discussed below are the different values that the **DOMAIN** parameter can take, and how they impact the **ADMIN USER** and **ADMIN PASSWORD** specifications: ▪ **If the VMs belong to a single domain** : If the guests belong to a specific domain, then specify the name of that domain against the **DOMAIN** parameter. In this case, any administrative user in that domain will have remote access to all the virtual guests. Therefore, an administrator account in the given domain can be provided in the **ADMIN USER** field and the corresponding password in the **ADMIN PASSWORD** field. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. ▪ **If the guests belong to different domains -** In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section 1.8.1.1 of this document. ▪ **If the INSIDE VIEW USING flag is set to 'eG VM Agent (Windows)'** – In this case, the inside view can be obtained without domain administrator privileges. Therefore, set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

<table>
<tr><td></td><td colspan="3">6. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
➢ The eG manager license should allow the detailed diagnosis capability
➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each disk partition on every virtual server monitored</td></tr>
<tr><td rowspan="5">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Disk busy:
Indicates the percentage of elapsed time during which the disk is busy processing requests (i.e., reads or writes).</td><td>Percent</td><td>Comparing the percentage of time that the different disks are busy, an administrator can determine whether load is properly balanced across the different disks.</td></tr>
<tr><td>Disk busy due to reads:
Indicates the percentage of elapsed time that the selected disk drive is busy servicing read requests.</td><td>Percent</td><td></td></tr>
<tr><td>Disk busy due to writes:
Indicates the percentage of elapsed time that the selected disk drive is busy servicing write requests.</td><td>Percent</td><td></td></tr>
<tr><td>Disk read time:
Indicates the average time in seconds of a read of data from the disk.</td><td>Secs</td><td></td></tr>
</table>

	Disk write time: Indicates the average time in seconds of a write of data from the disk.	Secs	
	Average queue length: Indicates the average number of both read and write requests that were queued for the selected disk during the sample interval.	Number	
	Current queue length: Indicates the number of requests outstanding on the disk at the time the performance data is collected.	Number	This measure includes requests in service at the time of the snapshot. This is an instantaneous length, not an average over the time interval. Multi-spindle disk devices can have multiple requests active at one time, but other concurrent requests are awaiting service. This counter might reflect a transitory high or low queue length, but if there is a sustained load on the disk drive, it is likely that this will be consistently high. Requests experience delays proportional to the length of this queue minus the number of spindles on the disks. This difference should average less than two for good performance.
	Read operations from disk: Indicates the number of reads happening on a logical disk per second.	Reads/Sec	A dramatic increase in this value may be indicative of an I/O bottleneck on the guest.
	Data reads from disk: Indicates the rate at which bytes are transferred from the disk during read operations.	KB/Sec	A very high value indicates an I/O bottleneck on the guest.
	Write operations to disk: Indicates the number of writes happening on a local disk per second.	Writes/Sec	A dramatic increase in this value may be indicative of an I/O bottleneck on the guest.

	Data writes to disk: Indicates the rate at which bytes are transferred from the disk during write operations.	KB/Sec	A very high value indicates an I/O bottleneck on the guest.

The detailed diagnosis of the *Disk busy* measure, if enabled, provides the list of processes currently executing on the disk, the I/O operations performed by the processes, and the statistics pertaining to these I/O operations (see Figure 32).

Shows the IO operations done by the processes

Time	ID Process	ProcessName	IO Rate(Bytes/sec)	IO Read Rate (Bytes/sec)	IO Read Ops Rate (Ops/Sec)	IO Write Rate (Bytes/sec)	IO Write Ops Rat (Ops/sec)
Nov 23, 2007 19:10:38							
	380	lsass	1718.96	853.82	11.98	865.14	11.98
	784	svchost	299.47	171.70	2.33	127.77	2
	368	services	230.26	0	0	230.26	1.66
Nov 23, 2007 19:00:50							
	380	lsass	1721.31	854.99	12	866.32	12
	784	svchost	299.88	171.93	2.33	127.95	2
	368	services	230.57	0	0	230.57	1.67
Nov 23, 2007 18:50:54							
	4	System	19789.36	0	0	19789.36	5.33
	380	lsass	1721.31	854.99	12	866.32	12
	784	svchost	299.88	171.93	2.33	127.95	2
	368	services	230.57	0	0	230.57	1.67
Nov 23, 2007 18:40:53							
	4	System	19781.90	0	0	19781.90	5.33
	380	lsass	1720.66	854.67	11.99	865.99	11.99
	784	svchost	299.77	171.87	2.33	127.90	2
	368	services	230.49	0	0	230.49	1.67

Figure 32: The detailed diagnosis of the VmgDiskActivity test

1.9.3 System – Guest Test

This test collects various metrics pertaining to the CPU and memory usage of every processor supported by a guest. The details of this test are as follows:

Purpose	Ccollects various metrics pertaining to the CPU and memory usage of every processor supported by a guest
Target of the test	A Microsoft Virtual Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **INSIDE VIEW USING** - By default, this test communicates with every VM remotely and extracts "inside view" metrics. Therefore, by default, the **INSIDE VIEW USING** flag is set to **Remote connection to VM (Windows)**. Typically, to establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. In high-security environments, where the IT staff might have reservations about exposing the credentials of their domain administrators, this approach to extracting "inside view" metrics might not be preferred. In such environments therefore, eG Enterprise provides administrators the option to deploy a piece of software called the **eG VM Agent** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** Refer to Section 1.2.2 for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 5. **DOMAIN, ADMIN USER, ADMIN PASSWORD,** and **CONFIRM PASSWORD** – By default, this test connects to each virtual guest remotely and attempts to collect "inside view" metrics. In order to obtain a remote connection, the test must be configured with user privileges that allow remote communication with the virtual guests. The first step towards this is to specify the **DOMAIN** within which the virtual guests reside. The **ADMIN USER** and **ADMIN PASSWORD** will change according to the **DOMAIN** specification. Discussed below are the different values that the **DOMAIN** parameter can take, and how they impact the **ADMIN USER** and **ADMIN PASSWORD** specifications: ▪ **If the VMs belong to a single domain** : If the guests belong to a specific domain, then specify the name of that domain against the **DOMAIN** parameter. In this case, any administrative user in that domain will have remote access to all the virtual guests. Therefore, an administrator account in the given domain can be provided in the **ADMIN USER** field and the corresponding password in the **ADMIN PASSWORD** field. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. ▪ **If the guests belong to different domains -** In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section 1.8.1.1 of this document. ▪ **If the INSIDE VIEW USING flag is set to 'eG VM Agent (Windows)'** – In this case, the inside view can be obtained without domain administrator privileges. Therefore, set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 6.

<table>
<tr><td></td><td colspan="3">7. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
➢ The eG manager license should allow the detailed diagnosis capability
➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each processor supported by every guest on the monitored virtual server</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>CPU usage:
This measurement indicates the percentage of CPU utilized by the processor.</td><td>Percent</td><td>A high value could signify a CPU bottleneck. The CPU utilization may be high because a few processes are consuming a lot of CPU, or because there are too many processes contending for a limited resource. The detailed diagnosis of this test reveals the top-10 CPU-intensive processes on the guest.</td></tr>
<tr><td>System CPU usage:
Indicates the percentage of CPU time spent for system-level processing.</td><td>Percent</td><td>An unusually high value indicates a problem and may be due to too many system-level tasks executing simultaneously.</td></tr>
<tr><td>Run queue:
Indicates the instantaneous length of the queue in which threads are waiting for the processor cycle. This length does not include the threads that are currently being executed.</td><td>Number</td><td>A value consistently greater than 2 indicates that many processes could be simultaneously contending for the processor.</td></tr>
<tr><td>Processes blocked:
Indicates the number of processes blocked for I/O, paging, etc.</td><td>Number</td><td>A high value could indicate an I/O problem on the guest (e.g., a slow disk).</td></tr>
</table>

	Swap memory: Denotes the committed amount of virtual memory. This corresponds to the space reserved for virtual memory on disk paging file(s).	MB	An unusually high value for the swap usage can indicate a memory bottleneck. Check the memory utilization of individual processes to figure out the process(es) that has (have) maximum memory consumption and look to tune their memory usages and allocations accordingly.
	Free memory: Indicates the free memory available.	MB	A very low value of free memory is also an indication of high memory utilization on a guest. The detailed diagnosis of this measure lists the top 10 processes responsible for maximum memory consumption on the guest.
	Scan rate: Indicates the memory scan rate.	Pages/Sec	A high value is indicative of memory thrashing. Excessive thrashing can be detrimental to guest performance.

The detailed diagnosis of the *Free memory* measure of the VsgSystem Test reveals the top 10 memory -consuming processes on a guest (see Figure 33).

Lists the top 10 memory consuming processes

Time	PID	Memory used(MB)	ARGS
Nov 23, 2007 19:15:06			
	836	27.77	svchost
	1460	13.23	explorer
	752	6.12	vsggetcpu
	448	5.75	services
	1064	4.68	wuaudt
	628	4.18	svchost
	948	4.16	svchost
	404	4.12	winlogon
	1128	3.95	spoolsv
	772	3.67	svchost

Figure 33: The detailed diagnosis of the VsgSystem Test

1.9.4 Tcp - Guest Test

This test tracks various statistics pertaining to TCP connections to and from each guest of an MS Virtual server host. The details of the test are provided below:

Purpose	Tracks various statistics pertaining to TCP connections to and from each guest of an MS Virtual server host
Target of the test	A Microsoft Virtual Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **INSIDE VIEW USING** - By default, this test communicates with every VM remotely and extracts "inside view" metrics. Therefore, by default, the **INSIDE VIEW USING** flag is set to **Remote connection to VM (Windows)**. Typically, to establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. In high-security environments, where the IT staff might have reservations about exposing the credentials of their domain administrators, this approach to extracting "inside view" metrics might not be preferred. In such environments therefore, eG Enterprise provides administrators the option to deploy a piece of software called the **eG VM Agent** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** Refer to Section 1.2.2 for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 5. **DOMAIN, ADMIN USER, ADMIN PASSWORD,** and **CONFIRM PASSWORD** – By default, this test connects to each virtual guest remotely and attempts to collect "inside view" metrics. In order to obtain a remote connection, the test must be configured with user privileges that allow remote communication with the virtual guests. The first step towards this is to specify the **DOMAIN** within which the virtual guests reside. The **ADMIN USER** and **ADMIN PASSWORD** will change according to the **DOMAIN** specification. Discussed below are the different values that the **DOMAIN** parameter can take, and how they impact the **ADMIN USER** and **ADMIN PASSWORD** specifications: ▪ **If the VMs belong to a single domain** : If the guests belong to a specific domain, then specify the name of that domain against the **DOMAIN** parameter. In this case, any administrative user in that domain will have remote access to all the virtual guests. Therefore, an administrator account in the given domain can be provided in the **ADMIN USER** field and the corresponding password in the **ADMIN PASSWORD** field. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. ▪ **If the guests belong to different domains -** In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section 1.8.1.1 of this document. ▪ **If the INSIDE VIEW USING flag is set to 'eG VM Agent (Windows)'** – In this case, the inside view can be obtained without domain administrator privileges. Therefore, set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 6.

Outputs of the test	One set of results for every guest on the monitored virtual server		
Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Incoming connections: Indicates the connections per second received by the guest.	Conns/Sec	A high value can indicate an increase in input load.
	Outgoing connections: Indicates the connections per second initiated by the guest.	Conns/Sec	A high value can indicate that one or more of the applications executing on the guest have started using a number of TCP connections to some other guest or host.
	Current connections Indicates the currently established connections.	Number	A sudden increase in the number of connections established on a guest can indicate either an increase in load to one or more of the applications executing on the guest, or that one or more of the applications are experiencing a problem (e.g., a slow down). On Microsoft Windows, the current connections metrics is the total number of TCP connections that are currently in the ESTABLISHED or CLOSE_WAIT states.
	Connection drops: Indicates the rate of established TCP connections dropped from the TCP listen queue.	Conns/Sec	This value should be 0 for most of the time. Any non-zero value implies that one or more applications on the guest are under overload.
	Connection failures: Indicates the rate of half open TCP connections dropped from the listen queue.	Conns/Sec	This value should be 0 for most of the time. A prolonged non-zero value can indicate either that the server is under SYN attack or that there is a problem with the network link to the server that is resulting in connections being dropped without completion.

1.9.5 TcpTraffic - Guest Test

Since most popular applications rely on the TCP protocol for their proper functioning, traffic monitoring at the TCP protocol layer can provide good indicators of the performance seen by the applications that use TCP. The most critical metric at the TCP protocol layer is the percentage of retransmissions. Since TCP uses an exponential back-off algorithm for its retransmissions, any retransmission of packets over the network (due to network congestion, noise, data link errors, etc.) can have a significant impact on

the throughput seen by applications that use TCP. This test monitors the TCP protocol traffic to and from a guest, and particularly monitors retransmissions.

Purpose	Tracks various statistics pertaining to TCP connections to and from each guest of an MS Virtual server host
Target of the test	A Microsoft Virtual Server
Agent deploying the test	An internal agent
Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **INSIDE VIEW USING** - By default, this test communicates with every VM remotely and extracts "inside view" metrics. Therefore, by default, the **INSIDE VIEW USING** flag is set to **Remote connection to VM (Windows)**. Typically, to establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. In high-security environments, where the IT staff might have reservations about exposing the credentials of their domain administrators, this approach to extracting "inside view" metrics might not be preferred. In such environments therefore, eG Enterprise provides administrators the option to deploy a piece of software called the **eG VM Agent** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** Refer to Section 1.2.2 for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 5. **DOMAIN, ADMIN USER, ADMIN PASSWORD,** and **CONFIRM PASSWORD** – By default, this test connects to each virtual guest remotely and attempts to collect "inside view" metrics. In order to obtain a remote connection, the test must be configured with user privileges that allow remote communication with the virtual guests. The first step towards this is to specify the **DOMAIN** within which the virtual guests reside. The **ADMIN USER** and **ADMIN PASSWORD** will change according to the **DOMAIN** specification. Discussed below are the different values that the **DOMAIN** parameter can take, and how they impact the **ADMIN USER** and **ADMIN PASSWORD** specifications: ▪ **If the VMs belong to a single domain** : If the guests belong to a specific domain, then specify the name of that domain against the **DOMAIN** parameter. In this case, any administrative user in that domain will have remote access to all the virtual guests. Therefore, an administrator account in the given domain can be provided in the **ADMIN USER** field and the corresponding password in the **ADMIN PASSWORD** field. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

<table>
<tr><td></td><td colspan="3">

If the guests belong to different domains - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple DOMAIN names, multiple ADMIN USER names and ADMIN PASSWORDS would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section 1.8.1.1 of this document.
If the INSIDE VIEW USING flag is set to 'eG VM Agent (Windows)' – In this case, the inside view can be obtained without domain administrator privileges. Therefore, set the DOMAIN, ADMIN USER, and ADMIN PASSWORD parameters to none.

</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every guest on the monitored virtual server</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Segments received:
Indicates the rate at which segments are received by the guest.</td><td>Segments/Sec</td><td></td></tr>
<tr><td>Segments sent:
Indicates the rate at which segments are sent to clients or other guests.</td><td>Segments/Sec</td><td></td></tr>
<tr><td>Retransmits:
Indicates the rate at which segments are being retransmitted by the guest.</td><td>Segments/Sec</td><td></td></tr>
</table>

	Retransmit ratio: Indicates the ratio of the rate of data retransmissions to the rate of data being sent by the guest.	Percent	Ideally, the retransmission ratio should be low (< 5%). Most often retransmissions at the TCP layer have significant impact on application performance. Very often a large number of retransmissions are caused by a congested network link, bottlenecks at a router causing buffer/queue overflows, or by lousy network links due to poor physical layer characteristics (e.g., low signal to noise ratio). By tracking the percentage of retransmissions at a guest, an administrator can quickly be alerted to problem situations in the network link(s) to the guest that may be impacting the service performance.

1.9.6 WindowsMemory - Guest Test

To understand the metrics reported by this test, it is essential to understand how memory is handled by the Operating System. On any system, memory is partitioned into a part that is available for user processes, and another that is available to the OS kernel. The kernel memory area is divided into several parts, with the two major parts (called "pools") being a nonpaged pool and a paged pool. The nonpaged pool is a section of memory that cannot, under any circumstances, be paged to disk. The paged pool is a section of memory that can be paged to disk. (Just being stored in the paged pool doesn't necessarily mean that something has been paged to disk. It just means that it has either been paged to disk or it could be paged to disk.) Sandwiched directly in between the nonpaged and paged pools (although technically part of the nonpaged pool) is a section of memory called the "System Page Table Entries," or "System PTEs." The VsgWinMemory test tracks critical metrics corresponding to the System PTEs and the pool areas of kernel memory.

Purpose	Tracks various statistics pertaining to TCP connections to and from each guest of an MS Virtual server host
Target of the test	A Microsoft Virtual Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **INSIDE VIEW USING** - By default, this test communicates with every VM remotely and extracts "inside view" metrics. Therefore, by default, the **INSIDE VIEW USING** flag is set to **Remote connection to VM (Windows)**. Typically, to establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. In high-security environments, where the IT staff might have reservations about exposing the credentials of their domain administrators, this approach to extracting "inside view" metrics might not be preferred. In such environments therefore, eG Enterprise provides administrators the option to deploy a piece of software called the **eG VM Agent** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** Refer to Section 1.2.2 for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 5. **DOMAIN, ADMIN USER, ADMIN PASSWORD,** and **CONFIRM PASSWORD** – By default, this test connects to each virtual guest remotely and attempts to collect "inside view" metrics. In order to obtain a remote connection, the test must be configured with user privileges that allow remote communication with the virtual guests. The first step towards this is to specify the **DOMAIN** within which the virtual guests reside. The **ADMIN USER** and **ADMIN PASSWORD** will change according to the **DOMAIN** specification. Discussed below are the different values that the **DOMAIN** parameter can take, and how they impact the **ADMIN USER** and **ADMIN PASSWORD** specifications:

<table>
<tr><td></td><td colspan="3">

If the VMs belong to a single domain : If the guests belong to a specific domain, then specify the name of that domain against the DOMAIN parameter. In this case, any administrative user in that domain will have remote access to all the virtual guests. Therefore, an administrator account in the given domain can be provided in the ADMIN USER field and the corresponding password in the ADMIN PASSWORD field. Confirm the password by retyping it in the CONFIRM PASSWORD text box.
If the guests belong to different domains - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple DOMAIN names, multiple ADMIN USER names and ADMIN PASSWORDS would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section 1.8.1.1 of this document.
If the INSIDE VIEW USING flag is set to 'eG VM Agent (Windows)' – In this case, the inside view can be obtained without domain administrator privileges. Therefore, set the DOMAIN, ADMIN USER, and ADMIN PASSWORD parameters to none.

</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every guest on the monitored virtual server</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Free entries in system page table:
Indicates the number of page table entries not currently in use by the guest.</td><td>Number</td><td>The maximum number of System PTEs that a server can have is set when the server boots. In heavily-used servers, you can run out of system PTEs. You can use the registry to increase the number of system PTEs, but that encroaches into the paged pool area, and you could run out of paged pool memory. Running out of either one is bad, and the goal should be to tune your server so that you run out of both at the exact same time. Typically, the value of this metric should be above 3000.</td></tr>
<tr><td>Pages read from disk:
Indicates the average number of times per second the disk was read to resolve hard fault paging.</td><td>Reads/Sec</td><td></td></tr>
</table>

	Pages written to disk: Indicates the average number of times per second the pages are written to disk to free up the physical memory.	Writes/Sec	
	Memory page ins: Indicates the number of times per second that a process needed to access a piece of memory that was not in its working set, meaning that the guest had to retrieve it from the page file.	Pages/Sec	
	Memory page outs: Indicates the number of times per second the guest decided to trim a process's working set by writing some memory to disk in order to free up physical memory for another process.	Pages/Sec	This value is a critical measure of the memory utilization on a guest. If this value never increases, then there is sufficient memory in the guest. Instantaneous spikes of this value are acceptable, but if the value itself starts to rise over time or with load, it implies that there is a memory shortage on the guest.
	Non-paged pool kernel memory size: Indicates the total size of the kernel memory non-paged pool.	MB	The kernel memory nonpage pool is an area of guest memory (that is, memory used by the guest operating system) for kernel objects that cannot be written to disk, but must remain in memory as long as the objects are allocated. Typically, there should be no more than 100 MB of non-paged pool memory being used.

	Memory paged pool size: Indicates the total size of the Paged Pool.	MB	If the Paged Pool starts to run out of space (when it's 80% full by default), the guest will automatically take some memory away from the System File Cache and give it to the Paged Pool. This makes the System File Cache smaller. However, the system file cache is critical, and so it will never reach zero. Hence, a significant increase in the paged pool size is a problem. This metric is a useful indicator of memory leaks in a guest. A memory leak occurs when the guest allocates more memory to a process than the process gives back to the pool. Any time of process can cause a memory leak. If the amount of paged pool data keeps increasing even though the workload on the guest remains constant, it is an indicator of a memory leak.

1.9.7 VsgNetworkTraffic – Windows Test

This is an internal test that monitors the incoming and outgoing traffic through each guest of an MS Virtual server host.

Purpose	Monitors the incoming and outgoing traffic through each guest of an MS VIrtual server host
Target of the test	A Microsoft Virtual Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TESTPERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured. 3. **PORT** - The port at which the **HOST** listens. 4. **INSIDE VIEW USING** - By default, this test communicates with every VM remotely and extracts "inside view" metrics. Therefore, by default, the **INSIDE VIEW USING** flag is set to **Remote connection to VM (Windows)**. Typically, to establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. In high-security environments, where the IT staff might have reservations about exposing the credentials of their domain administrators, this approach to extracting "inside view" metrics might not be preferred. In such environments therefore, eG Enterprise provides administrators the option to deploy a piece of software called the **eG VM Agent** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** Refer to Section 1.2.2 for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*. 5. **DOMAIN, ADMIN USER, ADMIN PASSWORD,** and **CONFIRM PASSWORD** – By default, this test connects to each virtual guest remotely and attempts to collect "inside view" metrics. In order to obtain a remote connection, the test must be configured with user privileges that allow remote communication with the virtual guests. The first step towards this is to specify the **DOMAIN** within which the virtual guests reside. The **ADMIN USER** and **ADMIN PASSWORD** will change according to the **DOMAIN** specification. Discussed below are the different values that the **DOMAIN** parameter can take, and how they impact the **ADMIN USER** and **ADMIN PASSWORD** specifications: ▪ **If the VMs belong to a single domain** : If the guests belong to a specific domain, then specify the name of that domain against the **DOMAIN** parameter. In this case, any administrative user in that domain will have remote access to all the virtual guests. Therefore, an administrator account in the given domain can be provided in the **ADMIN USER** field and the corresponding password in the **ADMIN PASSWORD** field. Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. ▪ **If the guests belong to different domains -** In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section 1.8.1.1 of this document.

<table>
<tr><td></td><td colspan="3">▪ If the INSIDE VIEW USING flag is set to 'eG VM Agent (Windows)' – In this case, the inside view can be obtained without domain administrator privileges. Therefore, set the DOMAIN, ADMIN USER, and ADMIN PASSWORD parameters to none.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for every guest on the monitored virtual server</td></tr>
<tr><td rowspan="6">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Incoming traffic:
Indicates the rate at which data (including framing characters) is received on a network interface.</td><td>Mbps</td><td>An abnormally high rate of incoming traffic may require additional analysis.</td></tr>
<tr><td>Outgoing traffic:
Represents the rate at which data (including framing characters) is sent on a network interface.</td><td>Mbps</td><td>An abnormally high rate of outgoing traffic may require additional analysis.</td></tr>
<tr><td>Max bandwidth:
An estimate of the capacity of a network interface.</td><td>Mbps</td><td></td></tr>
<tr><td>Bandwidth used:
Indicates the percentage of bandwidth used by a network interface.</td><td>Percent</td><td>By comparing the bandwidth usage with the maximum bandwidth of an interface, an administrator can determine times when the network interface is overloaded or is being a performance bottleneck.</td></tr>
<tr><td>Output queue:
Indicates the length of the output packet queue (in packets).</td><td>Number</td><td>If this is longer than 2, delays are being experienced and the bottleneck should be found and eliminated if possible.</td></tr>
<tr><td></td><td>Outbound packet errors:
Indicates the number of outbound packets that could not be transmitted because of errors..</td><td>Number</td><td>Ideally, number of outbound errors should be 0.</td></tr>
</table>

	Inbound packet errors: Indicates the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.	Number	Ideally, number of inbound errors should be 0.

1.10 Correlation between Applications in a Virtualized Environment

Using the eG Enterprise administration console, administrators can add applications running on the VMs for monitoring. To monitor these applications, agents can be installed in the guests, or an agentless monitoring approach can be used. To effectively monitor the applications running in a virtual environment, it is important to be able to determine which virtual server an application is running. This mapping of applications to virtual servers is important for root-cause diagnosis – for example, a problem with the virtual server (e.g., excessive disk slowdowns) can impact the performance of all the applications running on the server's virtual machines. eG Enterprise is able to automatically determine the mapping of applications to virtual servers.

Whether eG Enterprise automatically determines the mapping of applications to virtual servers or not is determined by the value of the **AutoVirtualMapping** variable in the **[MISC]** section of the **eg_external.ini** configuration file in the **<EG_INSTALL_DIR>\manager\config** directory of the eG manager. If the value of this variable is **true**, the eG manager auto-discovers the applications to virtual servers mapping.

Note:

- For **AutoVirtualMapping** to work, the detailed diagnosis frequencies set globally (i.e., using the Configure -> Diagnosis menu sequence) should not be set to *0:0*.
- As long as the **AutoIpNameCheck** parameter in the **eg_services.ini** file (in the **<EG_INSTALL_DIR>\manager\config** directory) is **Yes** (which is the default), eG Enterprise can automatically identify the server applications executing on a virtual server host, using the host/nick names that are mapped to the IP addresses discovered on the host. If the **AutoIPNameCheck** flag is set to **No** instead, then make sure that, while managing a server application executing in a virtualized environment, the hostname of the virtual machine is specified as the nick name of the corresponding server application. If more than one server application is executing on the same virtual machine, then any one of those server applications should have the virtual machine name as its nick name.

To disable auto-discovery, set this value to **false.** In such a case, once a *Virtual Server* is added, then, when adding any new server application using the eG administrative interface, you will be prompted to manually set an association between the server application being added and the *Virtual Server*.

The mapping of applications to virtual servers is used by eG Enterprise for correlation – e.g., since the application runs on the virtual server, it is most likely that a problem with the virtual server will impact the performance of the application running on one of the guests. To view this application-virtual server association, simply click on the **VIRTUAL COMPONENTS** link in the layer model page of the virtual server.

Note:

The **VIRTUAL COMPONENTS** link will also be available in the layer model page of those server applications that are executing on virtual guests.

Doing so reveals Figure 34 depicting the *Virtual Server* and the server applications executing on it. By clicking on any of the components in Figure 34, the user can drill down into specific layers of this component for specific details on the performance of the component.

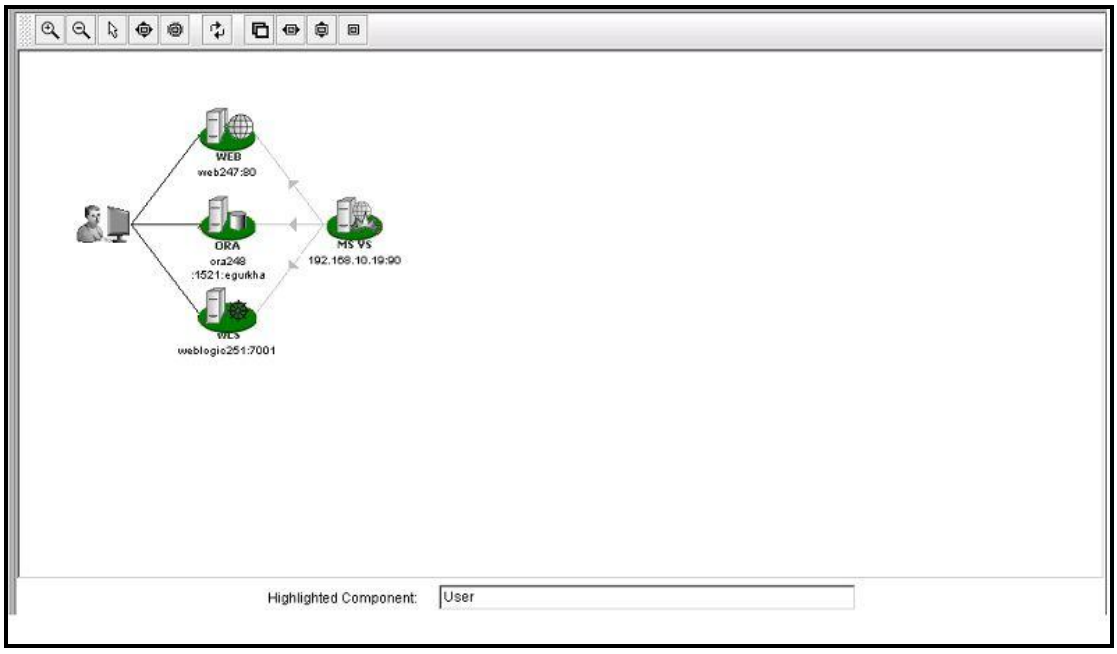

Figure 34: Depicts the applications that have been deployed on the guest OS of a virtual server

The arrows in Figure 34 depict the dependencies between the virtual server host and the applications running on it. Since the applications are hosted on one of the guests running on the host, they depend on the virtual server host – i.e., any unusual resource usage on the virtual server host impacts the applications running on any of the virtual guests. The dependency information between the virtual server host and the applications hosted on it is used by eG Enterprise for end-to-end correlation.

1.11 Troubleshooting

If the VirtualMachineStatus test, VirtualMachineDetails test, and all the "inside view" tests for a Microsoft Virtual server fail to run, then it could be owing to the inability of the eG agent to auto-discover the IP addresses of the VMs on the Virtual Server and their state. This can be due to any of the following reasons:

- Typically, the eG agent runs scripts on the virtual server and VMs to discover the IP addresses of the VMs. If the Virtual Servers and the VMs have been configured to disallow the execution of scripts, then the eG agent's scripts will not execute, thereby resulting in the failure of VM discovery.

  To check whether scripts can execute on the virtual server and VMs, do the following:

  - Login to the target Microsoft Virtual Server host as the user whose credentials have been passed to the VsGuest test, VsGuestStatus test, and the "inside view" tests.
  - Go to the command prompt.
  - Move to the **<EG_AGENT_INSTALL_DIR>\lib** directory.
  - The eG agent runs a script named **guestinfo.vbs** in the **<EG_AGENT_INSTALL_DIR>\lib** directory, which reports the names of the VMs on the virtual server, the state of each VM, and the operating

system of the VMs. To execute this script, issue the following command at the command prompt:

cscript guestinfo.vbs

- If this script executes smoothly, then it will return the names of the VMs, their state, and their operating system (OS). A sample query result is given below:

```
Machine Name:vm2#State:5#OS:Windowsr XP Professional
Service Pack 2
```

- On the other hand, if the query returns an error as displayed below, then it indicates a problem in script execution.

```
The name of the guest OS could not be retrieved
```

- To verify whether the problem is because the virtual server does not allow script execution, first, open the **Microsoft Virtual Server Administration Website** using the menu sequence depicted by Figure 15.

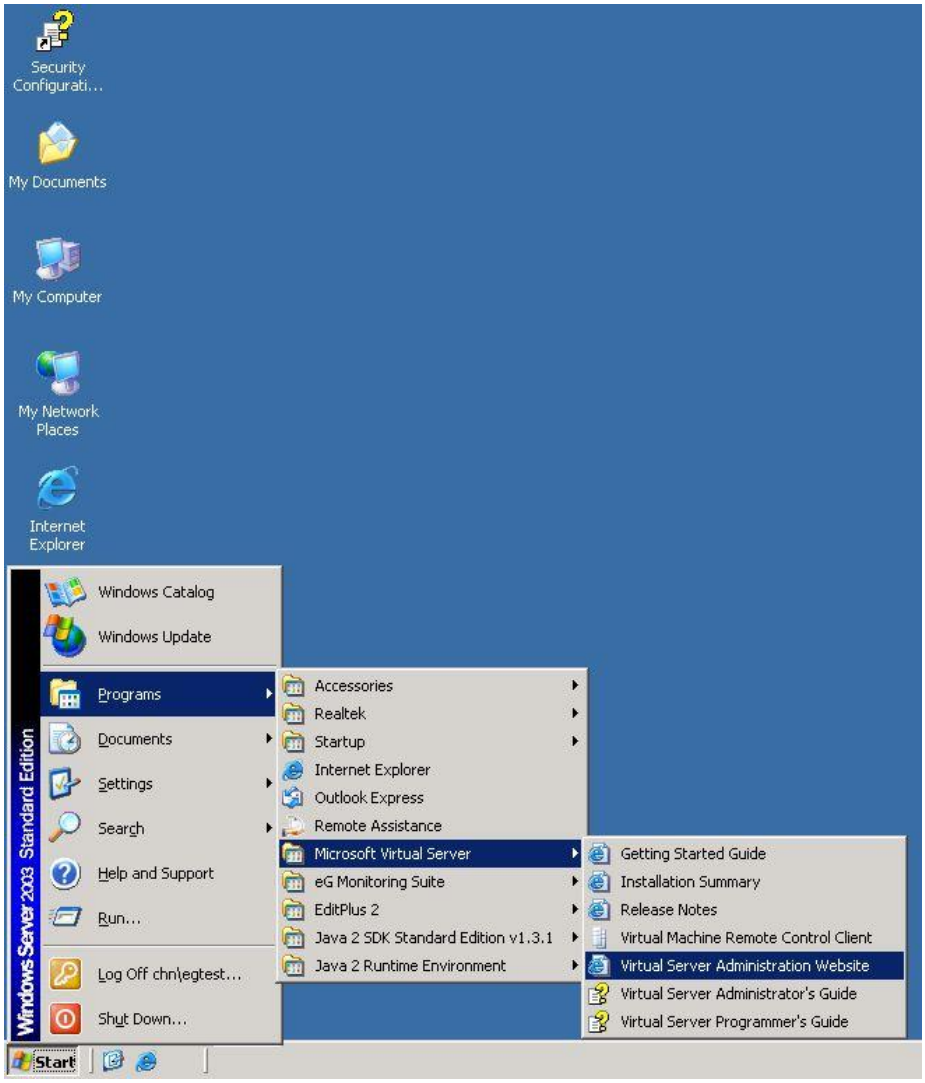

Figure 35: Opening the Virtual server Administration Website

- When figure 16 appears, click on the **Master Status** option in the left panel to view the VMs configured on the Virtual server and their current state in the right panel.

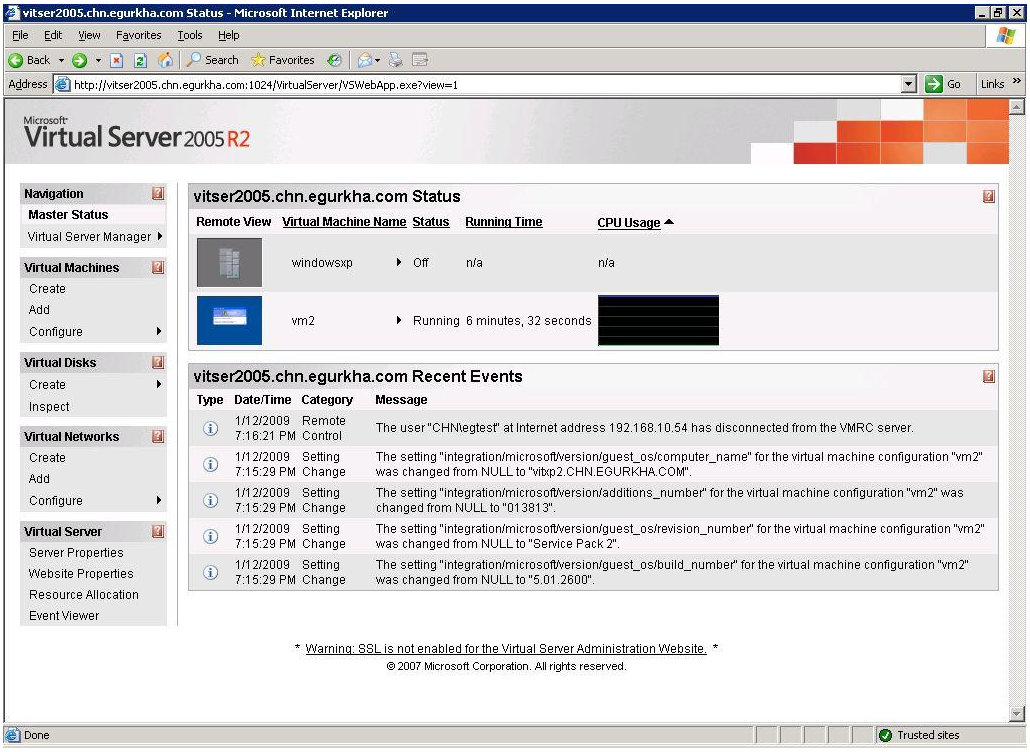

Figure 36: Viewing the names and state of VMs

- Make sure that all listed VMs are in an **Off** state. If not, right-click on every VM, and pick the **Turn Off** option from the shortcut menu.
- Then, click on the **Server Properties** option from the **Virtual Server** section in the left panel. Figure 17 then appears.

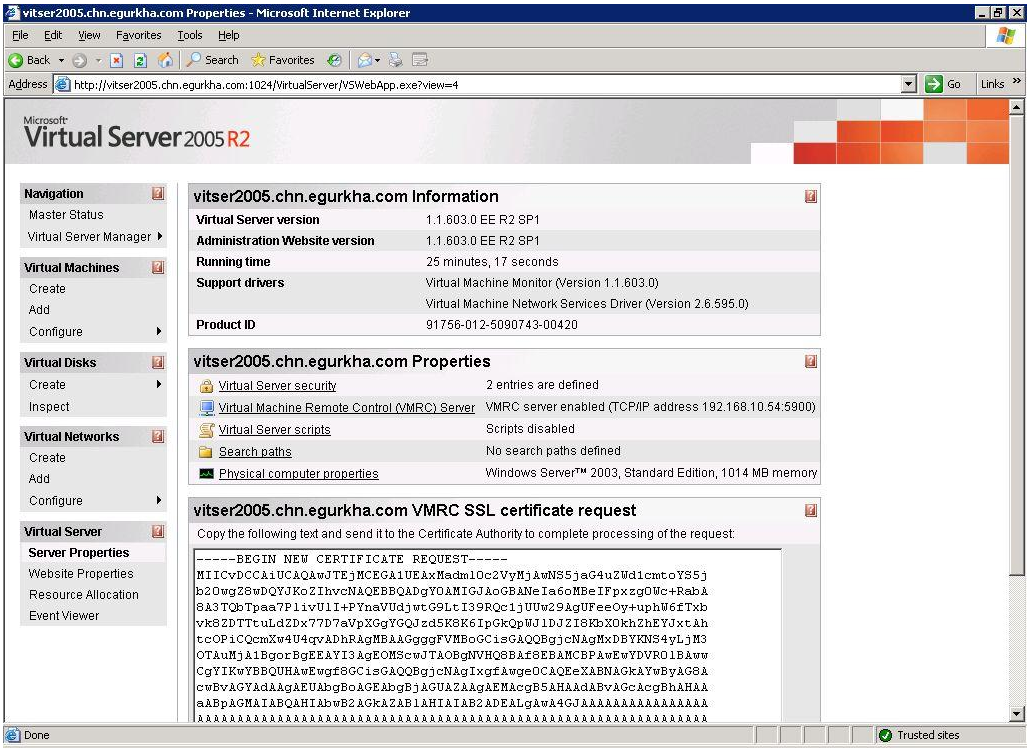

Figure 37: The Server Properties

- In the **Properties** section in the right panel of Figure 17, look for the **Virtual Server scripts** parameter. If it is set to **Scripts disabled**, then it indicates that no scripts can be executed on the virtual server. To enable script execution, click on the **Virtual Server scripts** link in the right panel of Figure 17.
- In the **Virtual Server Settings** section of Figure 18 that appears, click on the **Enable scripts attached to this server** and **Enable scripts attached to the virtual machines running on this server** check boxes to enable script execution on the virtual server and the VMs.
- Finally, click the **OK** button in Figure 18.

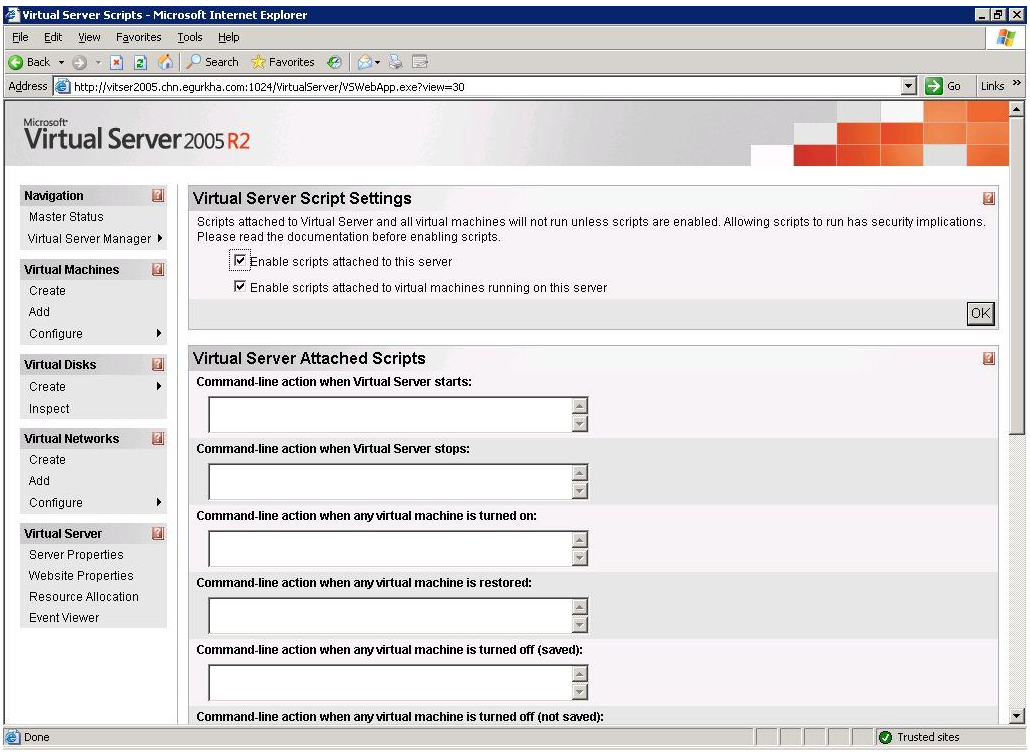

Figure 38: Enabling script execution

- The status of the **Virtual Server scripts** parameter then changes to **Scripts enabled** (see Figure 19).

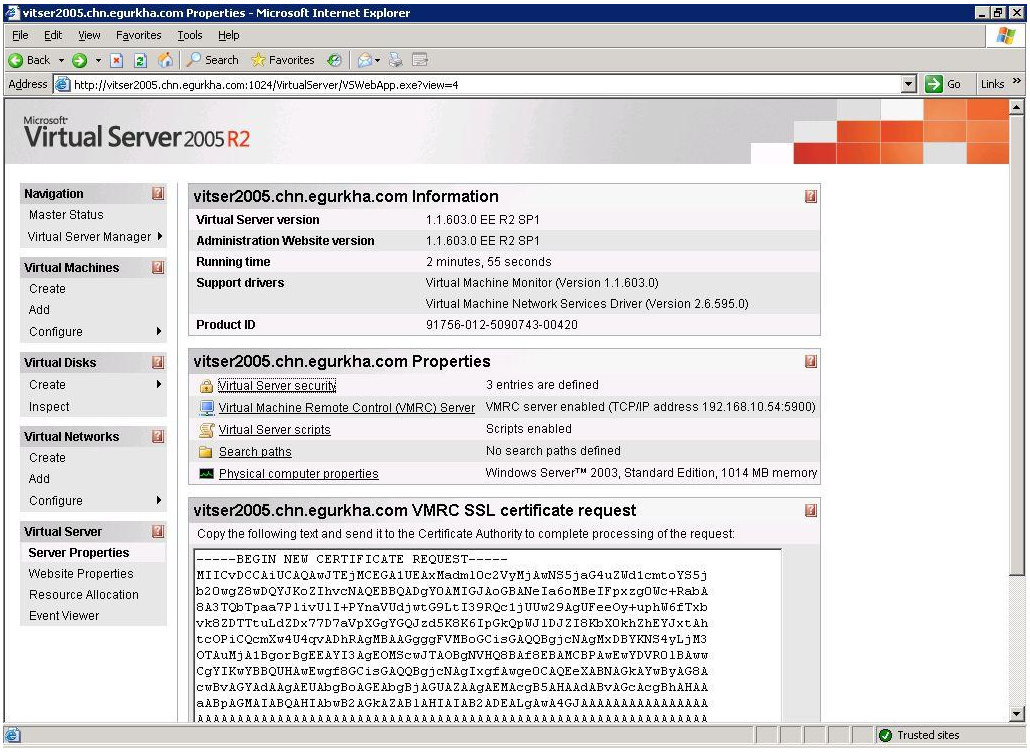

Figure 39: Change in the status of the Virtual Server scripts flag

- Once this is done, return to the command prompt, and once again try to execute the **guestinfo.vbs** script from the **<EG_INSTALL_DIR>\lib** directory.
- If the error persists, then proceed to check if this is a permission issue.

➢ The **guestinfo.vbs** script is used by the VsGuest test, VsGuestStatus test, and all "inside view" tests for VM discovery. Typically, these tests should be configured with the credentials of a user who has access to all the VMs on the virtual server. To check whether the configured user indeed has the required privileges, follow the steps given below:

- Login to the **Microsoft Virtual Server Administration Web Site**, and click on the **Server Properties** link in the right panel of the web site.
- Figure 19 appears. In the **Properties** section in the right panel of Figure 19, click on the **Virtual Server security** link. Figure 20 then appears.

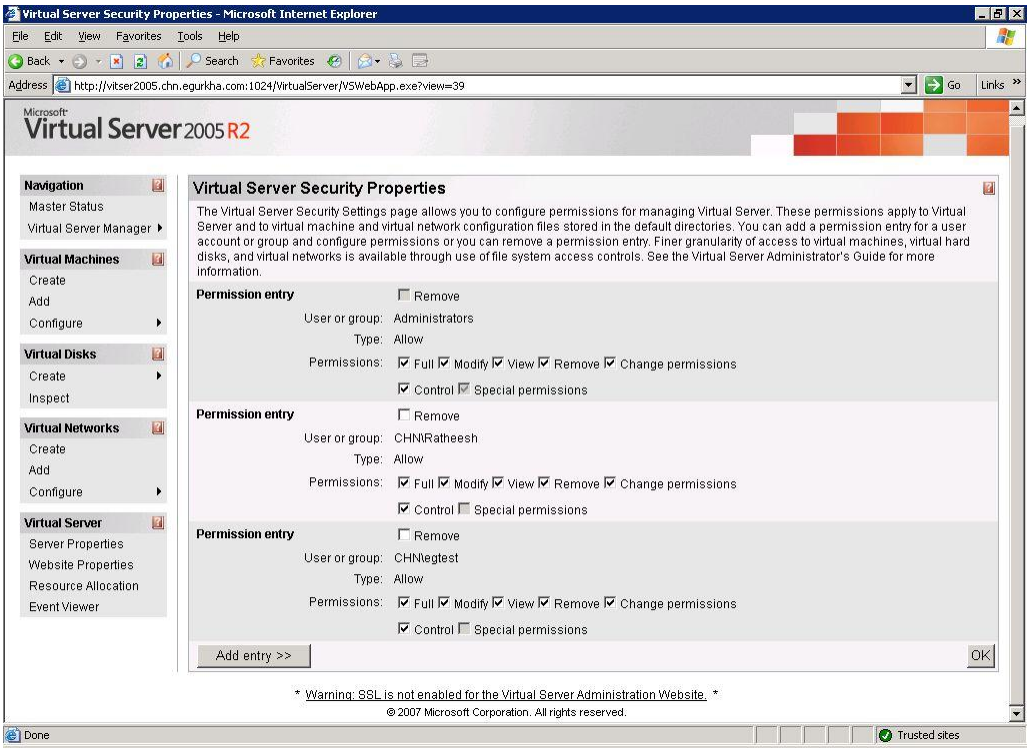

Figure 40: Checking for user privileges

- In the **Virtual Server Security Properties** section of Figure 20, you will find a **Permission entry** for every user who is allowed access to the virtual server, and the type of access he/she is entitled to. Scan the permission entries to determine whether the user who has been configured to run the VsGuest test, VsGuestStatus test, and all the "inside view" tests (i.e., the Vsg tests), is allowed **Full** access. If the user name you are looking for is not available in the page depicted by Figure 20, then it indicates that all the above-mentioned tests have been run by a user with "insufficient access permissions". To address this issue, you have to do either of the following

- Modify the test configuration, so that all the above-mentioned tests are configured with the credentials of any other user in Figure 20 with **Full** access;
- Grant **Full** access to the user, using whose credentials the tests are already being executed – i.e., add a **Permission entry** for the user. To achieve this, simply click on the **Add Entry** button in Figure 20, provide the name of the user against **User or Group**, set **Type** to **Access**, and then pick the **Full** check box against **Permissions** (see Figure 21). Finally, click the **OK** button in Figure 21.

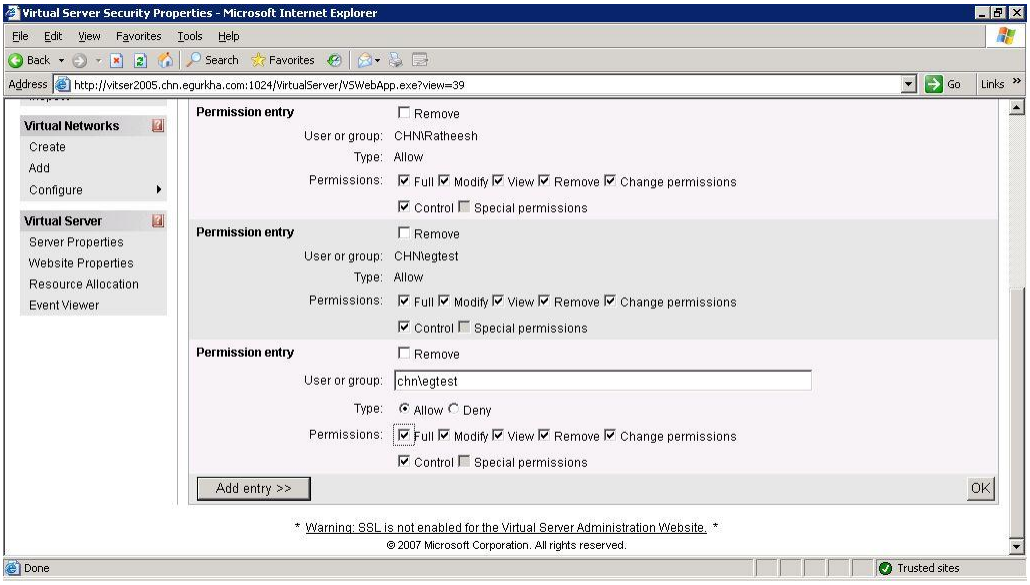

Figure 41: Adding a Permission entry

- Once the above steps are followed, the **guestinfo.vbs** script should execute without a glitch.

➢ While the eG agent that monitors the virtual server uses the **guestinfo.vbs** script to determine the state and OS of the VMs, it uses another script named **Ipaddress.vbs** to extract the IP address of the VMs. Typically, the **Ipaddress.vbs** script, upon execution, returns the names of the configuration files that correspond to the powered-on VMs on the virtual server. Upon receipt of these details, the eG agent automatically opens each of the configuration files that this script returns, reads the host names of the VMs from the files, and runs an **nslookup** on each name to determine the IP address of the VMs. However, if your DNS server is improperly configured, then **nslookup** will not be able to resolve the host name to IP address mappings. Therefore, to check whether the VM discovery failed due to an DNS error, follow the steps given below:

- Go to the command prompt, and once again switch to the **<EG_AGENT_INSTALL_DIR>\lib** directory.
- Next, execute the command: **cscript Ipaddress.vbs**.
- The command will return a list of files named in the format **<VMName>.vmc**. For instance, if the name of a powered-on VM is *vm2*, then the name of its corresponding configuration file will be: *vm2.vmc*.

- Open any of the configuration files, and search for the tag *<computer_name>* in them (see Figure 22).

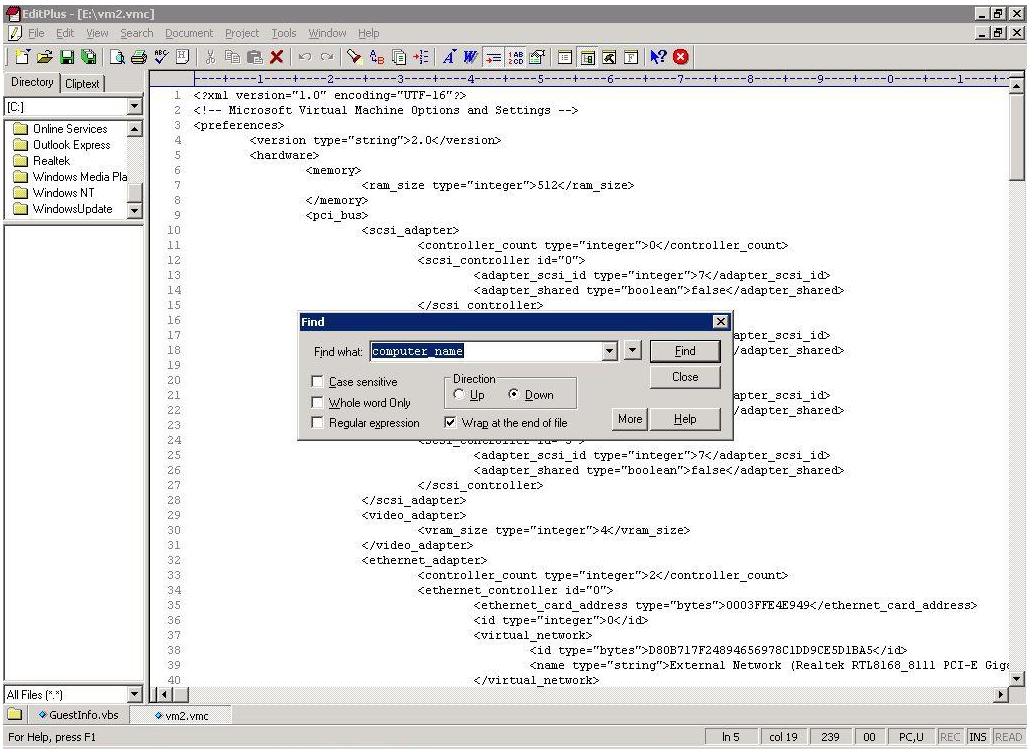

Figure 42: Searching for computer_name

6. Once the *computer_name* tag is found, copy the host name that is enclosed within the tags: *<computer_name> </computer_name>* (see Figure 23).

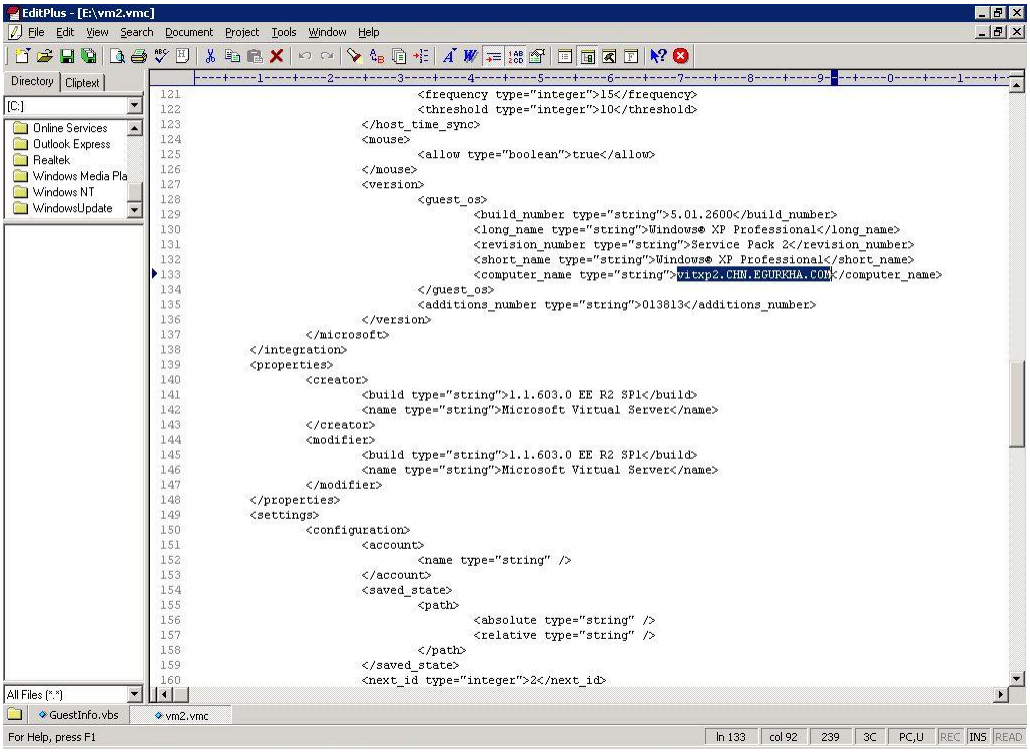

Figure 43: Determining the host name of the VM

7. Close the file, and return to the command prompt.
8. Issue the command: **nslookup <VMHostName>**. For instance, for the host name in Figure 23, the command will be: **nslookup vitxp2.CHN.EGURKHA.COM**
9. If this command returns an IP address, it indicates that the DNS server is functioning properly. If the command returns an error, it could indicate an issue with the DNS configuration.

Chapter 2

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to **the Microsoft Virtual Server**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.