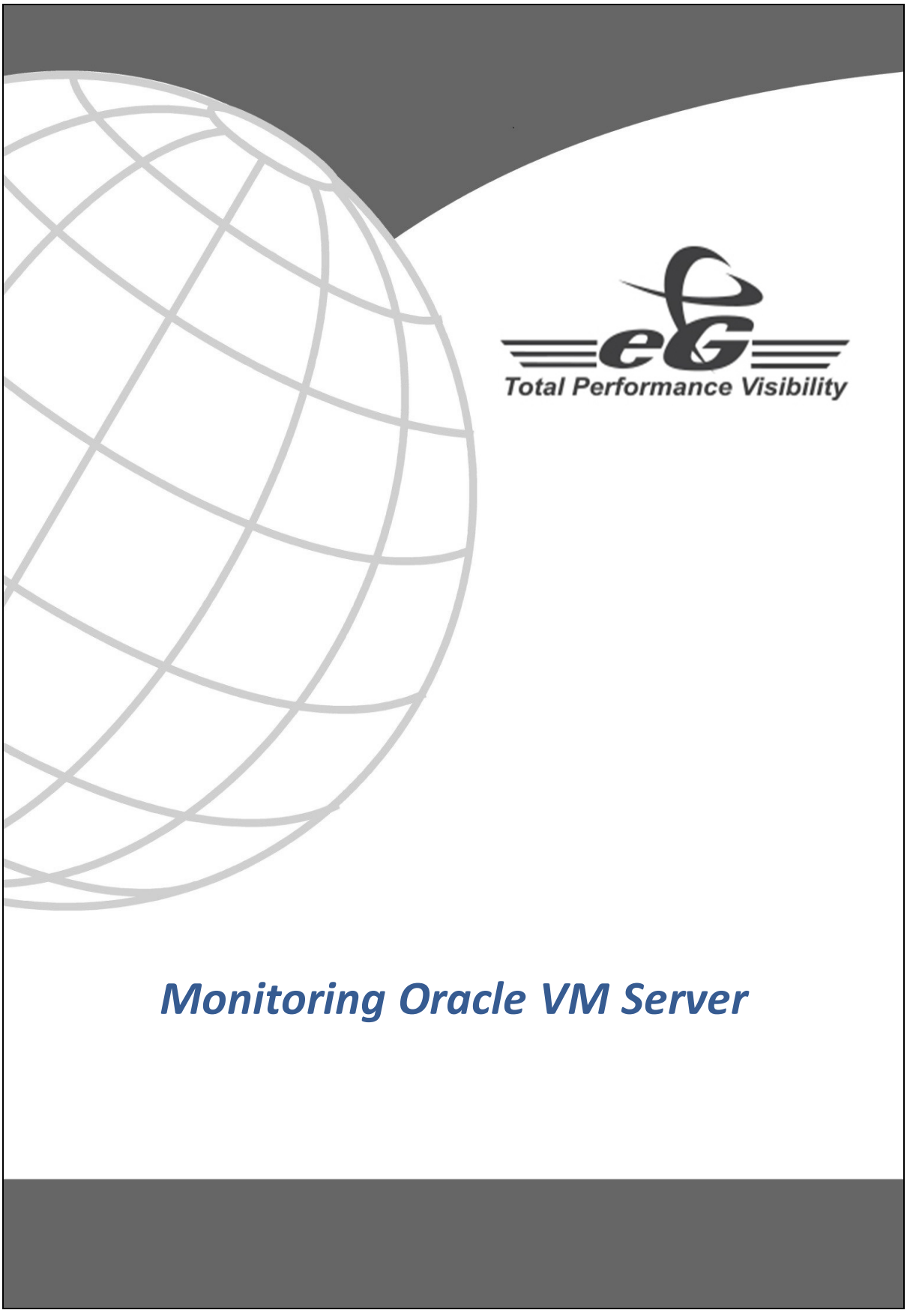


Monitoring Oracle VM Server

Restricted Rights Legend

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

Trademarks

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

©2016 eG Innovations Inc. All rights reserved.

Table of contents

Table of Figures

1

Introduction

Oracle VM is an enterprise-class server virtualization solution comprised of Oracle VM Server for x86, Oracle VM Server for SPARC and Oracle VM Manager. Oracle VM Manager controls the virtualization environment, creating and monitoring Oracle VM servers and the virtual machines. Oracle VM Server installs directly on server hardware and does not require a host operating system. An Oracle VM Server is comprised of a hypervisor and privileged domain (Dom0) that allows multiple domains or virtual machines (i.e. Linux, Solaris, Windows, etc.) to run on one physical machine. The Dom0 runs a process called Oracle VM Agent. The Oracle VM Agent receives and processes management requests, provides event notifications and configuration data to the Oracle VM Manager.

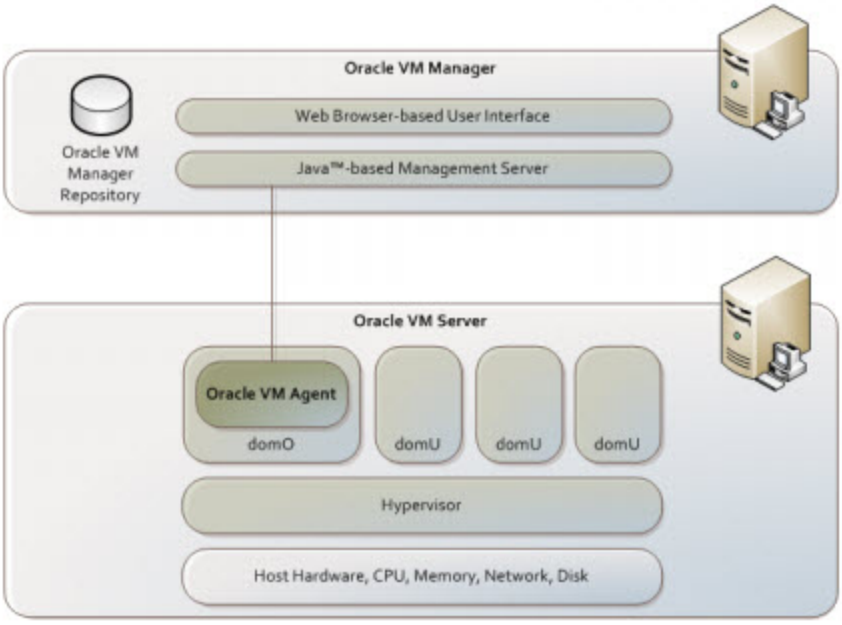


Figure 1.1: The Citrix XenMobile Architecture

As can be inferred from above figure, multiple virtual machines on the Oracle VM server share the physical resources of the server – i.e., the CPU, memory, network, and disk resources of the host. This resource dependency introduces many management troubles for administrators! For instance, a resource contention at the host-level will not only affect the performance of the host, but also the VMs on the host. In the same way, a resource-intensive application running on any of the VMs will significantly degrade the performance of the other VMs on the host and even the virtual host itself. This is why, when a virtual application slows down, administrators often take hours to figure out where the bottleneck is – is it owing to the a resource-starved host? Is it because of resource-intensive applications running on VMs? Or is because of poor resource allocation to the VMs? The specially designed Oracle VM Server model that eG Enterprise accurately answers these questions!

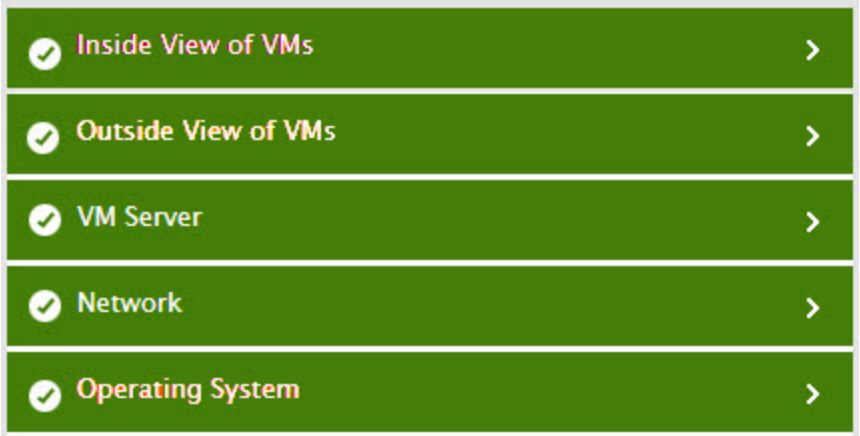


Figure 1.2: The layer model of the Oracle VM Server

This is an 'agentless' model that requires the eG agent to be deployed on any remote Windows/Linux/Solaris host in the environment. This eG agent should then be configured to employ a patented 'In-N-Out' monitoring approach for measuring and reporting the health of an Oracle VM server and its VMs. According to this approach, the eG agent remotely connects to the Oracle VM Manager and uses the **Oracle VM Manager web services API** to monitor the health of the Oracle VM server's host and to measure how each VM on the host uses the host's physical resources. This is the "outside view of VM performance", with the help of which the resource-hungry VMs on the host can be isolated. The eG agent then directly connects to each VM on the monitored host to pull out statistics revealing the internal health of each VM – i.e., revealing how each VM utilizes the resources allocated to it. This is the "inside view of VM performance", which reveals what is causing a VM to consume resources excessively.

Using the inside and outside views, administrators can find quick and accurate answers for the following performance queries:

- How many guest VMs are running on each Oracle VM server, what is the IP address of each of guests, what operating system is each guest running, and when was the guest powered on?
- Is the web services interface accessible? If so, how quickly can it be accessed?
- How much memory is allocated to each guest and does each guest VM have sufficient free memory?
- Is the control domain consuming resources optimally?
- Does the Oracle VM server have sufficient memory available to support the guest VMs that it is hosting?
- What is the CPU utilization of the Oracle VM server and which of the guest VMs is taking up excessive CPU?
- Which application(s) running on each of the guest VMs is taking CPU, memory, and disk resources?
- Is there sufficient disk space in each of the disk partitions of the guest operating system?
- Which of the guests is seeing the highest and lowest network traffic?
- Is there excessive queuing for disk access on any of the guest VMs?

To enable the eG agent to obtain the inside and outside views of performance, the pre-requisites detailed in Section **1.1** should be fulfilled.

1.1 Pre-requisites for Monitoring the Oracle VM Server and its VMs

1.1.1 General Pre-requisites

- Enable the remote agent to communicate with the eG manager port (default: 7077).
- If VMs running on multi-byte operating systems are to be monitored (eg., *Windows Japanese*), then the remote agent monitoring such VMs should also run on a multi-byte operating system.

1.2 Pre-requisites for Monitoring the Oracle VM Server and its VMs

1.2.1 General Pre-requisites

- Enable the remote agent to communicate with the eG manager port (default: 7077).
- If VMs running on multi-byte operating systems are to be monitored (eg., *Windows Japanese*), then the remote agent monitoring such VMs should also run on a multi-byte operating system.

1.2.2 Pre-requisites for Auto-Discovering the VMs on an Oracle VM Server

To enable the eG agent to auto-discover the IP address and operating system of the VMs on the Oracle VM server, make sure that the **Windows PV driver** is installed on each VM.

1.2.3 Pre-requisites for Collecting the 'Outside View' Metrics

To obtain the outside view of VM performance, the following pre-requisites should be fulfilled:

- Ensure that the remote agent has IP connectivity to the Oracle VM Manager.
- Ensure that the remote agent has web access to the **WEBPORT** (default port: 7002) configured for the Oracle VM Manager.
- All the tests that the remote agent executes should be configured with the IP address of Oracle VM Manager and the name and password of a user with Admin rights to the Oracle VM Manager.

1.2.4 Pre-requisites for Collecting the 'Inside View' Metrics from Windows VMs

To enable the eG agent to connect to a Windows VM and pull out 'inside view' metrics from it, you need to configure the eG agent with domain administrator privileges. In environments where administrators prefer not to expose the credentials of a domain administrator, a proprietary **eG VM Agent** software can be installed on each Windows VM to be monitored, which will enable the eG agent to obtain the 'inside view' without domain administrator permissions. The pre-requisites for obtaining the 'inside view' will therefore depend upon the how the Windows VMs are monitored – using the eG VM Agent? Or without using the eG VM Agent?

1.2.4.1 Pre-requisites for Obtaining the 'Inside View' of VMs, without using the eG VM Agent

- Ensure that the remote agent has IP connectivity to at least one of the network interfaces of the VMs.
- The **ADMIN$** share should be enabled for all Windows VMs being monitored and the administrative account must have permissions to this share drive. Refer to Section 1.2 of this document for a step-by-step procedure to achieve this.
- To enable the remote agent to communicate with the Windows VMs, an administrative account login and password (either a local account or a domain account) must be provided when configuring the eG monitoring capabilities.
- In case of VMs with the Windows XP/Windows 2003/Windows 2008/Windows Vista/Windows 7/Windows 2012 operating systems, the firewall on the guest should be explicitly configured to allow Windows File and Print Sharing services which are required for the remote agent to communicate with the guest operating system.
- For monitoring a Windows VM, TCP port 139 must be accessible from the remote agent to the VM.
- For obtaining the "inside view" of VMs running Windows Vista/Windows 7/Windows 2008/Windows 2012 operating systems, the **eGurkhaAgent** service of the eG remote agent should be configured to run using *domain administrator* privileges. Refer to the *eG User Manual* for the procedure. For obtaining the "inside view" of other Windows VMs however, the remote agent service requires no such privileges.
- Set the inside view using flag for all the "inside view" tests to **Remote connection to VM (Windows)**.

1.2.4.2 Pre-requisites for Obtaining the "Inside View" of Windows VMs, using the eG VM Agent

- Install the eG VM Agent on each Windows VM. For details on how to install the eG VM Agent, refer to Section 1.3 of this document.
- Enable the remote agent to communicate with the port at which the eG VM Agent listens (default port: 60001).
- Set the inside view using flag for all the "inside view" tests to **eG VM Agent (Windows)**.

1.2.5 Pre-requisites for Obtaining the 'Inside View' of Linux VMs

For monitoring a Linux VM, the SSH port (TCP port 22) must be enabled for communication between the remote agent and the VM being monitored.

Note:

If the Linux VMs in your environment listen on a different SSH port, then, you can override the default SSH port of 22 using the steps provided below:

- Login to the eG manager.
- Edit the **eg_tests.ini** file(in the **<EG_INSTALL_DIR>\manager\config** directory) on the eG manager host.
- In the **[AGENT_SETTINGS]** section of the file, set the **JavaSshPortForVm** parameter to an SSH port of your choice. By default, this parameter is set to 22.
- If your environment consists of multiple Linux VMs, each listening on a different SSH port, then, you can specify a comma-separated list of SSH ports against the **JavaSshPortForVm** parameter. For example: *7711,7271,8102*
- Finally, save the file.

1.3 Configuring Windows Virtual Machines to Support the eG Agent's Inside View without the eG VM Agent

For the "inside" view, by default, the eG agent uses SSH/WMI (depending upon the virtual OS to be monitored) to communicate remotely with the virtual machines on the Oracle VM server and collect metrics. To establish this remote connection with Windows VMs in particular, eG Enterprise requires that the eG agent be configured with domain administrator privileges. Besides, the **INSIDE VIEW USING** flag of all "inside view" tests should be set to **Remote connection to a VM**.

In addition, the **ADMIN$** share will have to be available on the Windows guests

1.3.1 Enabling ADMIN$ Share Access on Windows Virtual Guests

1.3.1.1 Enabling ADMIN$ Share Access on Windows 2000/2003 VMs

If the **ADMIN$** share is not available on any Windows-based 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 1.3 appears indicating the same.

Figure 1.3: The ADMIN$ share does not exist

On the other hand, if the **ADMIN$** share pre-exists, Figure 1.4 appears. In such a case, first, remove the **ADMIN$** share by selecting the **Do not share this folder** option from Figure 1.4 and clicking the **Apply** and **OK** buttons. After this, you will have to repeat step 1 of this procedure to open Figure 1.3. Then, proceed as indicated by step 3 onwards.

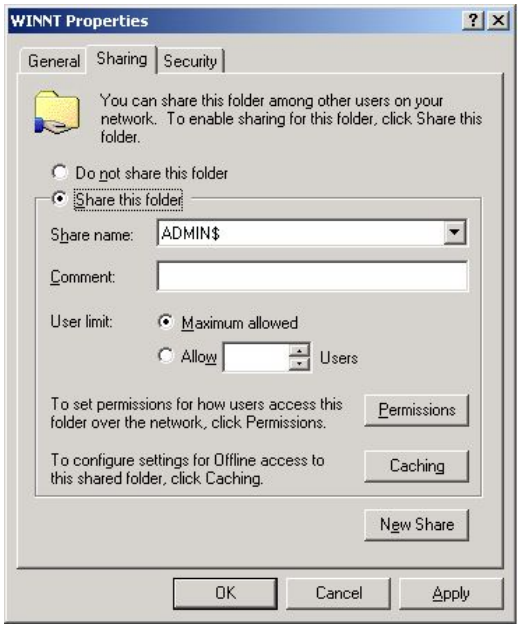


Figure 1.4: Admin$ share pre-exists

3. To create (or re-create) the **ADMIN$** share, select the **Share this folder** option from Figure 1.4, and provide **ADMIN$** share against the **Share name** text box (see Figure 1.5).

Figure 1.5: 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$** share is granted to an administrative user (local/domain); also, the **credentials of this user should be passed while configuring the eG monitoring capabilities** - i.e., while configuring the Oracle VM server tests. To grant the access permissions, click on the **Permissions** button in Figure 1.5.
5. By default, the **ADMIN$** share can be accessed by **Everyone** (see Figure 1.6). To grant access rights to a specific administrative (local/domain) user, select the **Add** button in Figure 1.6. When 1.3.1 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.

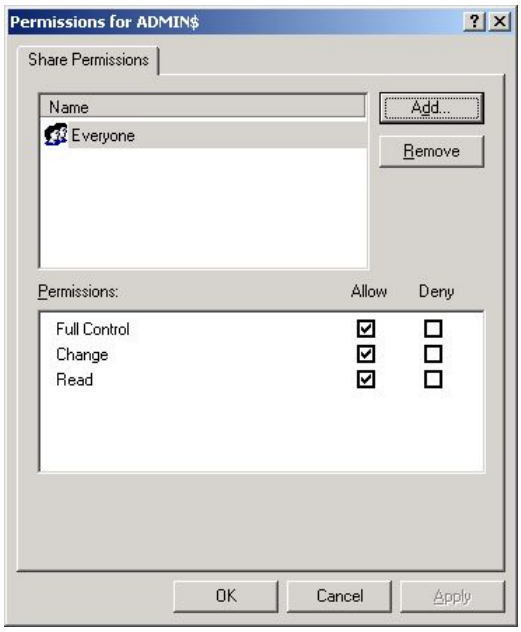


Figure 1.6: Clicking the Add button

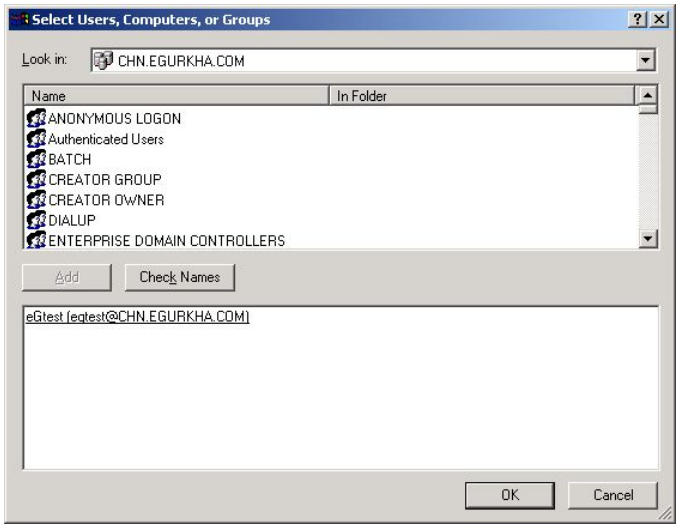


Figure 1.7: Selecting the administrative user to whom access rights are to be granted

6. Finally, click the **OK** button. You will then switch to Figure 1.8, where the newly added administrator account will appear.

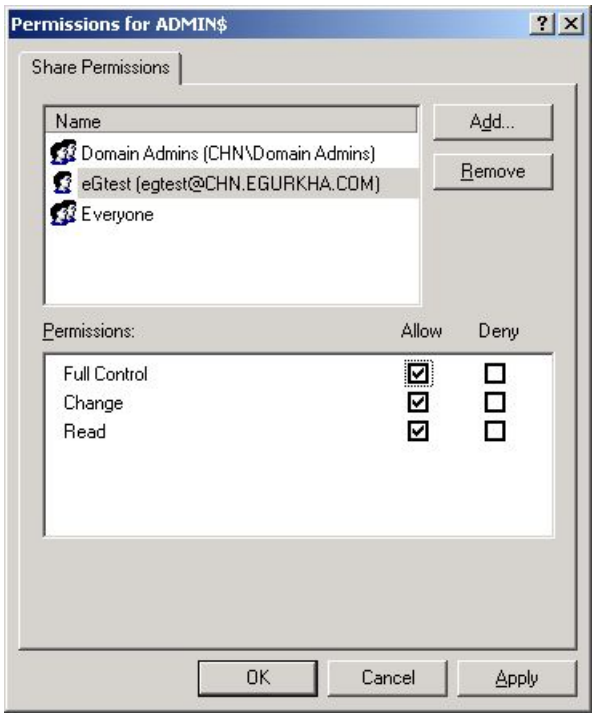


Figure 1.8: The administrator account granted access permissions

7. Select the newly added administrator account from Figure 1.8, 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 1.8 to register the changes.
9. Once you return to Figure 1.5, click on the **Security** tab to define the security settings for the **ADMIN$** share (see Figure 1.9).

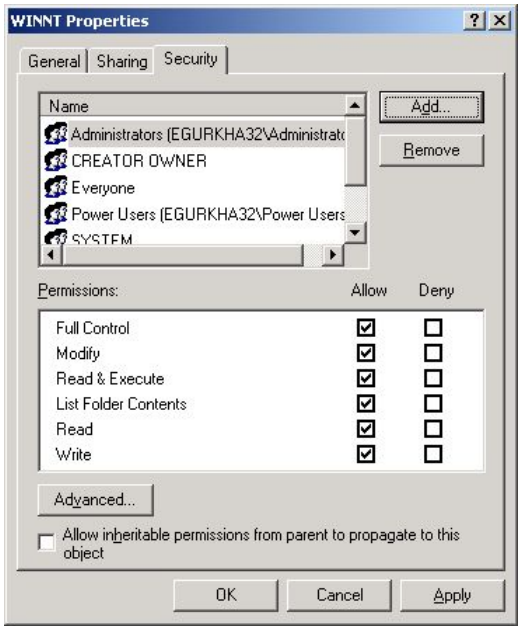


Figure 1.9: Defining the Security settings for the ADMIN$ share

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 1.9, pick a domain from the **Look in** list of 1.3.1, select the said administrator account from the domain users list below, and click the **Add** button (in 1.3.1) to add the chosen account. Then, click the **OK** button in 1.3.1.

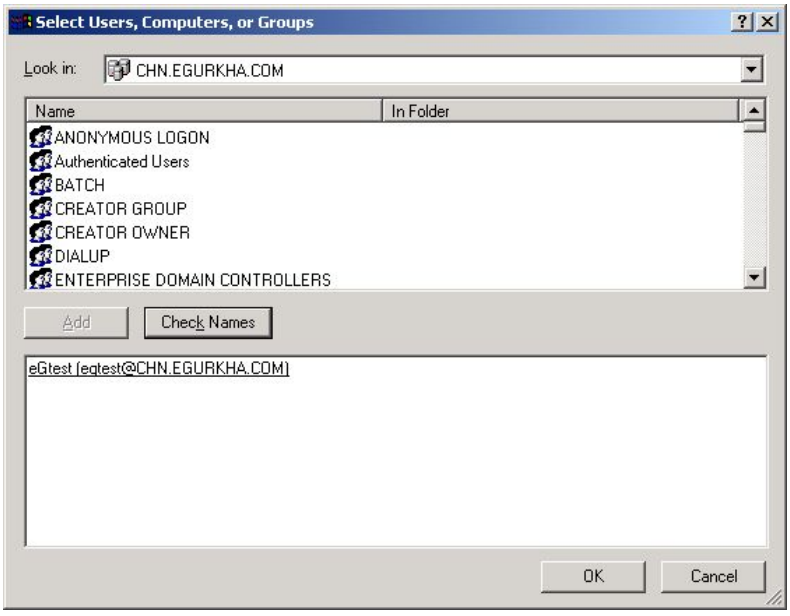


Figure 1.10: Adding the administrator account

11. This will bring you back to Figure 1.9, but this time, the newly added domain administrator account will be listed therein as indicated by 1.3.1.

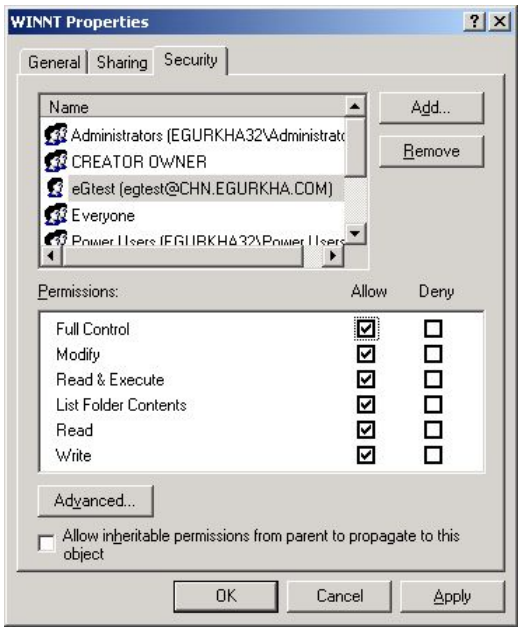


Figure 1.11: The Administrator account in the Security list

12. Finally, click the **Apply** and **OK** buttons in Figure 1.11.

1.3.1.2 Enabling ADMIN$ Share Access on Windows 2008 VMs

To enable the **ADMIN$** share on a Windows 2008 VM, do the following:

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 **Share** option from the shortcut menu.

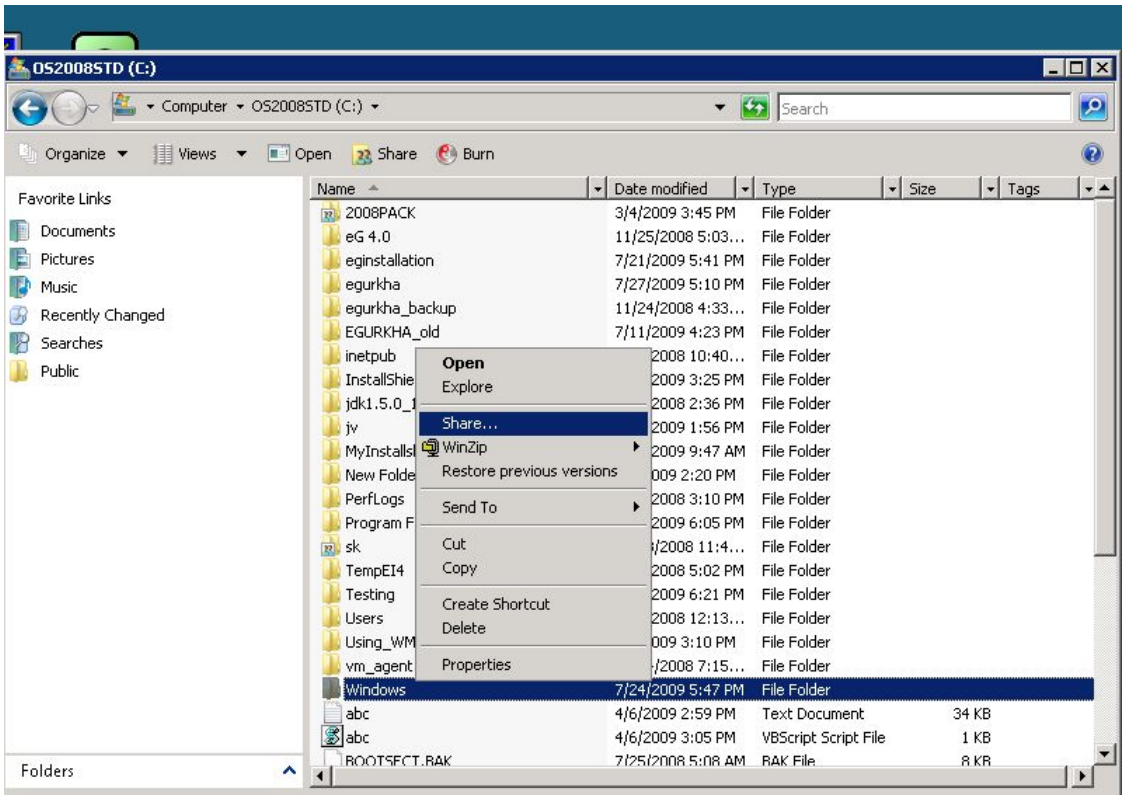


Figure 1.12: Selecting the Share option from the shortcut menu

2. 1.3.1 will then appear. Click on **Advanced Sharing** in 1.3.1.

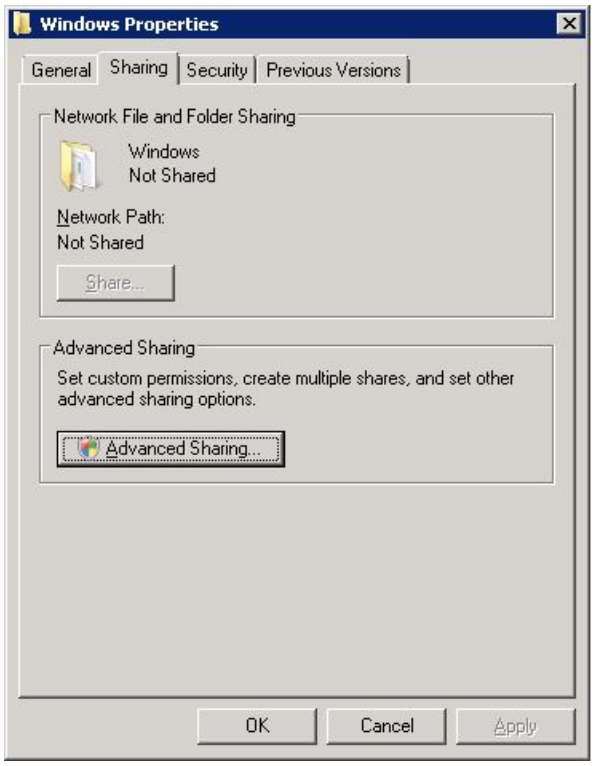


Figure 1.13: Clicking on Advanced Sharing

3. Select the **Share this folder** check box in Figure 1.14 that appears, enter **ADMIN$** against **Share name**, and click on the **Permissions** button in Figure 1.14, to allow only a local/domain administrator to access the folder.

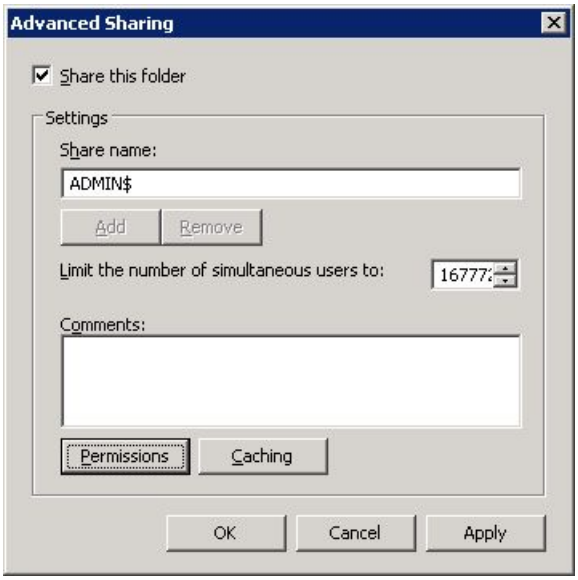


Figure 1.14: Enabling the ADMIN$ share

4. When Figure 1.15 appears, click on the **Add** button therein.

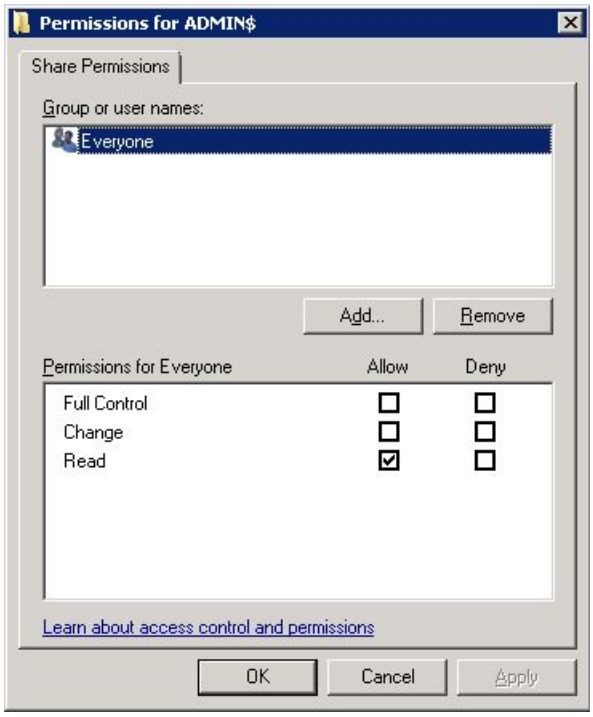


Figure 1.15: Clicking on the Add button

5. To allow a domain administrator to access the folder, first, ensure that a valid domain is specified in the **From this location** box of Figure 1.16. If you want to grant access to a local administrator instead, ensure that the name of the local host is displayed in the **From this location** box. To change this specification, use the **Locations** button in Figure 1.16. Then, enter the name of the local/domain administrator in the **Enter the object names to select** text area, and click the **OK** button.

Figure 1.16: Allowing a domain administrator to access the folder

6. The newly added user will be listed in the **Group or user names** section, as depicted by Figure 1.17. Select this user, and then, check all the three check boxes under **Allow** in the **Permissions for <user>** section in Figure 1.17. Then, click the **Apply** and **OK** buttons therein.

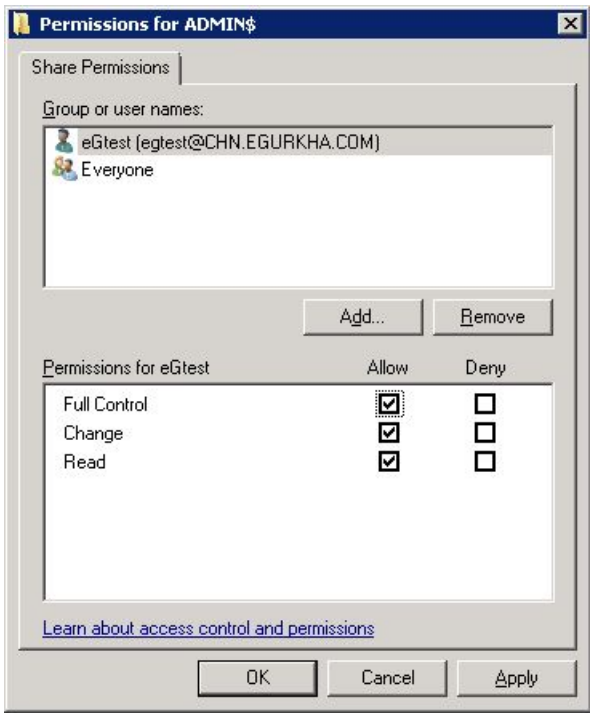


Figure 1.17: Allowing full access to the local/domain administrator

7. When 1.3.1 appears, click on the **Apply** and **OK** buttons therein to register the changes.

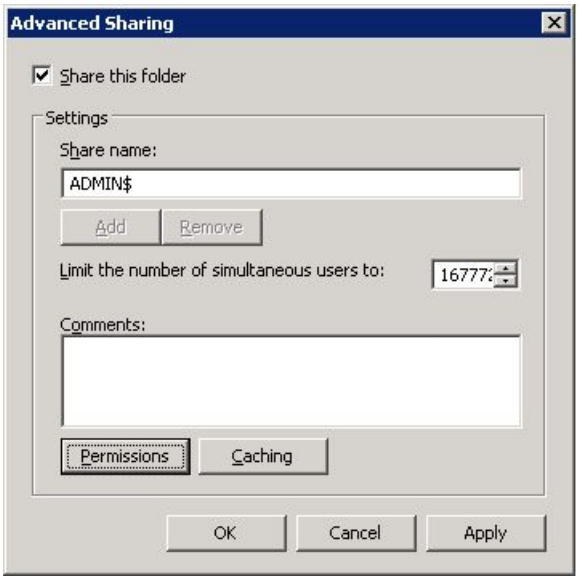


Figure 1.18: Applying the changes

Alternatively, by adding a new entry in the Windows registry, you can quickly enable the **ADMIN$** share. The steps for the same are discussed hereunder:

1. In Run prompt type **regedit** to open registry editor.
2. Browse through the following sub key:

   HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM
3. Create a new entry with the below information
   - Key Name : LocalAccountTokenFilterPolicy
   - Key Type : DWORD (32-bit)
   - Key Value : 1
4. Exit registry editor.

Note:

As with any change to the registry, ensure that the above-mentioned change is also performed with utmost care, so as to avoid problems in the functioning of the operating system.

1.4 Configuring the Remote Agent to Obtain the Inside View of Windows VMs, using the eG VM Agent

To provide the inside view of a Unix VM, the eG agent uses secure shell (SSH). To obtain the inside view of a Windows VM, the eG agent offers two options. The first option uses Windows File & Print Sharing services to push monitoring components to the VMs. These monitoring components are then executed on the VM to collect metrics from the VMs. To push monitoring components to the VM and to periodically invoke these components, the eG agent requires **domain administrator privileges** to all the VMs being monitored.

In many production environments, strict security restrictions are enforced, and it may not be possible to configure a monitoring solution with domain administration privileges for each of the VMs. To handle such environments, the eG VM monitor uses a lightweight monitoring component called the **eG VM Agent**, which is installed inside each of the VMs to obtain metrics regarding the health of the VMs. The **eG VM Agent** can be best described as a software that can be installed on the Windows virtual machines of a virtual infrastructure to allow a single eG agent to obtain an inside view of these VMs, **without domain administrator privileges**.

Users have multiple options to choose from when it comes to installing the eG VM Agent. These options have been discussed below:

- Manually install the eG VM Agent on every Windows VM using the executable that eG Enterprise includes;
- Bundle the eG VM Agent as part of a template VM, and use this template to create multiple VMs; this way, the eG VM Agent is automatically available in all the VMs that are created using the template;
- Use a software distribution solution such as Microsoft System Center to distribute the eG VM Agent software to existing VMs from a central location;

Use the install procedure that is ideal for your environment, and quickly get the eG VM Agent up and running. The detailed manual installation procedure has been discussed hereunder:

1. To install the eG VM Agent on a 32-bit VM, double-click on the **eGVMAgent.exe**, and to install the same on a 64-bit VM, double-click the **eGVMAgent_64.exe**.

2. Figure 1.19 then appears. Click on the **Next** button in Figure 1.19 to continue.

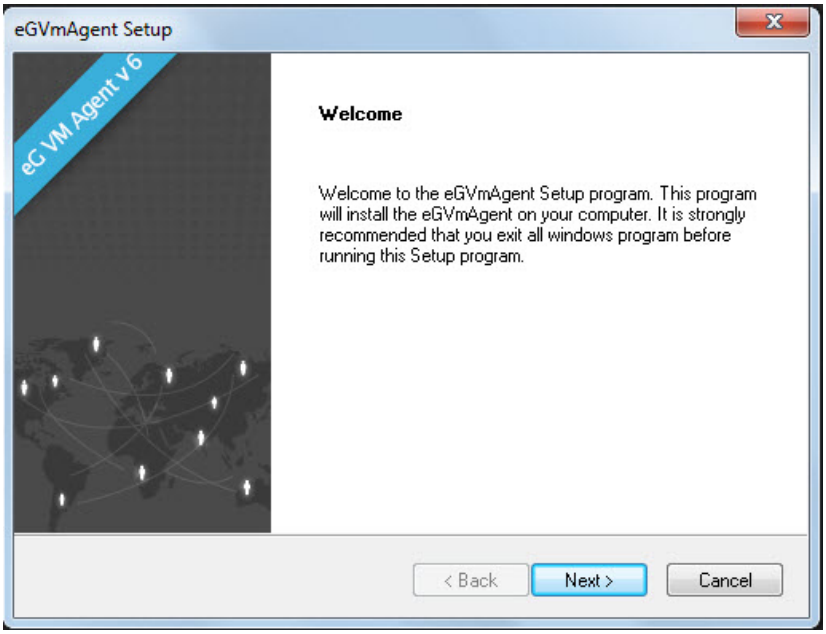


Figure 1.19: Welcome screen of the eG VM Agent installation wizard

3. When Figure 1.20 appears, click on **Yes** to accept the displayed license agreement.

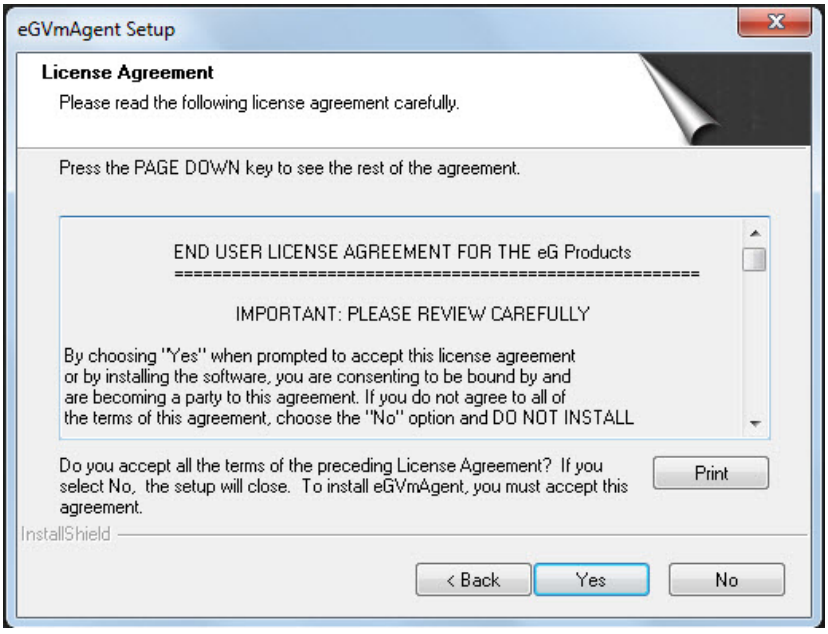


Figure 1.20: Accepting the license agreement

4. Use the **Browse** button in 1.4 to indicate the location in which the agent should be installed, and click the **Next** button to proceed.

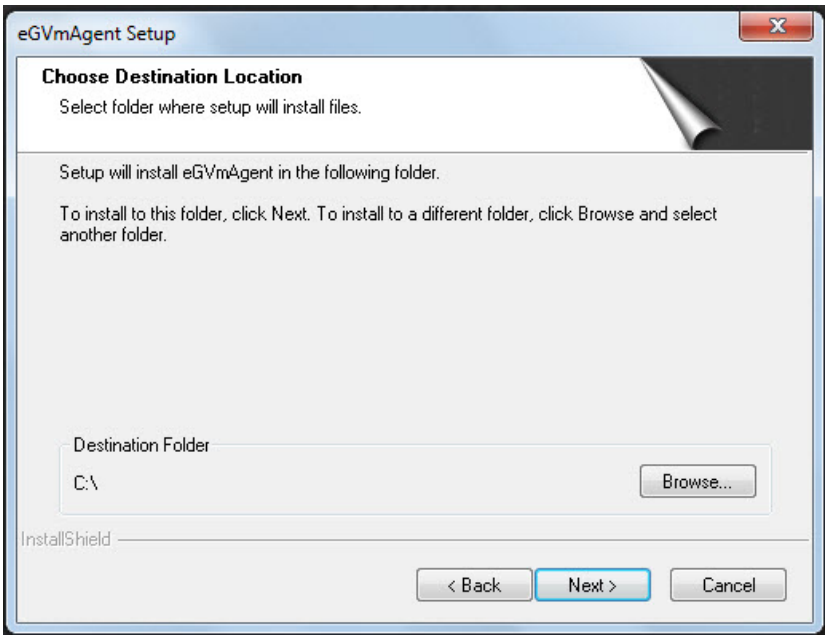


Figure 1.21: Specifying the install directory of the eG VM Agent

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 1.4 to proceed.

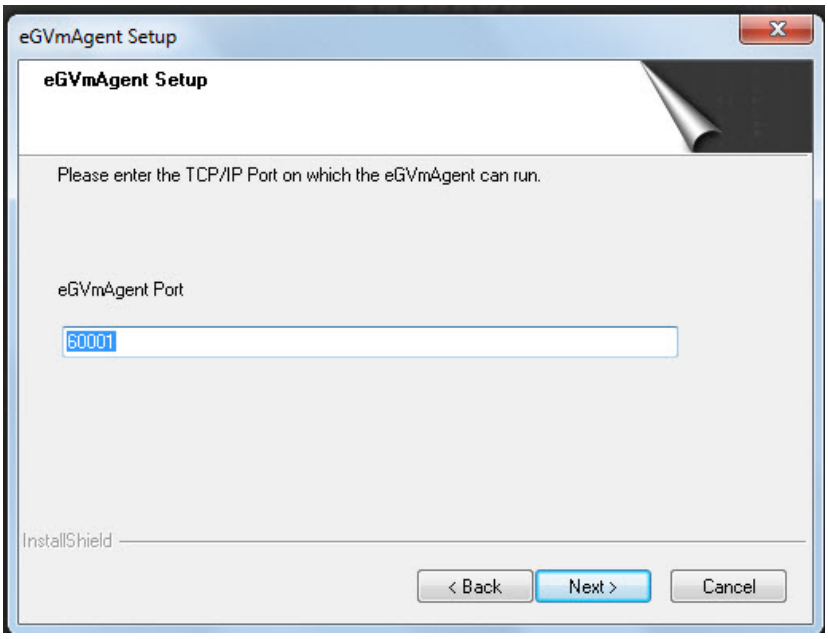


Figure 1.22: Specifying the VM agent port

6. A summary of your specifications then follows (see Figure 1.23). Click **Next** to proceed.

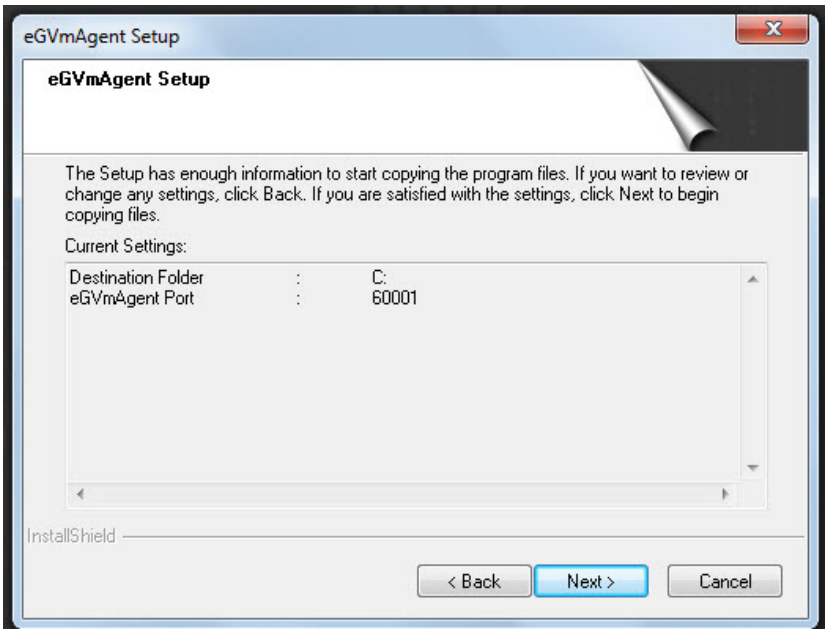


Figure 1.23: A summary of your specifications

7. Finally, click the **Finish** button in 1.4 to complete the installation.

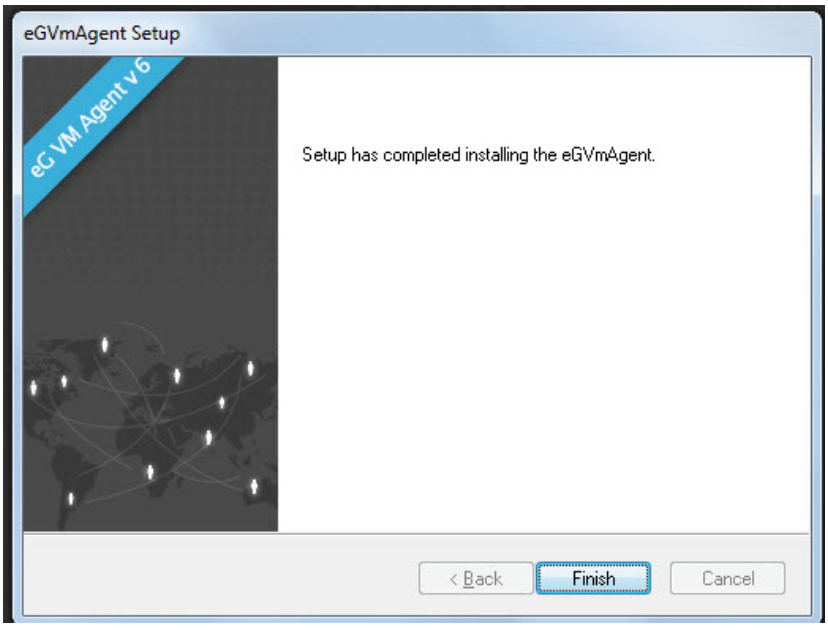


Figure 1.24: Finishing the installation

1.4.1 Communication between the eG Agent and the eG VM Agent

At the time of the installation of the eG VM agent, a folder named **eGVMAgent** is created in the install destination specified. The setup program also creates a Windows Service named **eGVMAgent** on the

Windows VM. This service must be running for the eG agent to obtain the inside view of the virtual machine.

Upon successful installation, the eG VM agent starts automatically and begins listening for requests at default TCP port 60001. However, if, during the installation process, you have configured a different port for the eG VM agent, then, after completing the installation, follow the steps below to make sure that the eG agent communicates with the eG VM agent via the port that you have configured:

- 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.

At configured intervals, the eG remote agent issues commands to each of the eG VM Agents (using the TCP port configured during the VM agent installation). The eG VM Agent executes the commands, collects the "inside view" metrics from the Windows VM, and sends the output back to the eG agent. The eG agent then analyzes the metrics and informs the eG manager about the status of the Windows VMs.

1.4.2 Licensing of the eG VM Agent

The eG VM Agent is not license-controlled. Therefore, you can install and use any number of VM agents in your infrastructure.

1.4.3 Benefits of the eG VM Agent

The eG VM Agent offers several key benefits:

- *Ideal for high-security environments:* The eG VM Agent is capable of collecting "inside view" metrics from Windows VMs, without domain administrator privileges. It is hence ideal for high-security environments, where administrators might not be willing to expose the credentials of the domain administrators.
- *Easy to install, configure*: The eG VM Monitor offers users the flexibility to choose from multiple methodologies for installing the eG VM Agent on the target VMs. Even a manual installation procedure, would not take more than a few minutes. Moreover, since the eG VM agent communicates only with the eG agent and not the eG manager, no additional configuration needs to be performed on the VM agent to facilitate the communication. In addition, the VM agent starts automatically upon installation, thereby saving the time and trouble involved in manually starting each of the VM agents.
- *License independent*: Since the eG VM agent is not license-controlled, you can add any number of VM agents, as and when required, to your environment.

2

Monitoring Oracle VM Servers

Figure 2.1 depicts the Oracle VM Server model that eG Enterprise offers.

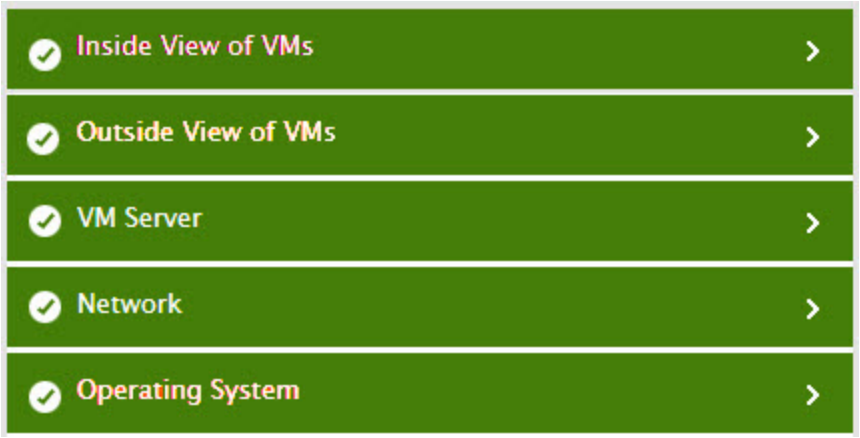


Figure 2.1: The layer model of the Oracle VM Server

The sections that follow discuss each layer of above figure.

2.1 The Operating System Layer

Using the tests mapped to this layer, you can ascertain the CPU, memory, and disk space capacity of the Oracle VM server and determine how the server, the control domain, and other VMs use the available physical resources. Resource-hungry guests and resource-intensive processing performed on the control domain will come to light in the process.

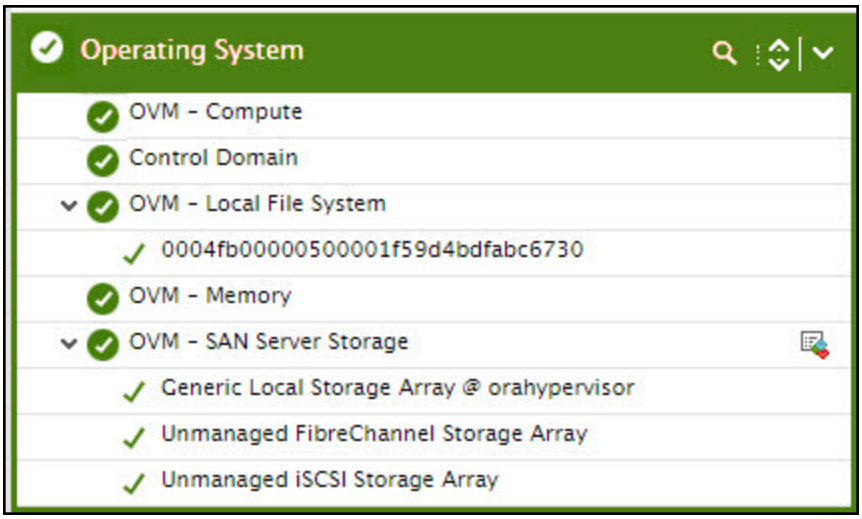


Figure 2.2: The tests mapped to the Operating System layer

2.1.1 OVM – Compute Test

In the absence of adequate compute resources, the performance of the Oracle VM Server and its VMs will deteriorate. Administrators should therefore track how the server and its VMs use the available CPU resources, so that any potential contention for CPU resources can be proactively detected and resolved. This is where the **OVM – Compute** test helps. This test reports the physical CPU usage of the Oracle VM Server and points to that VM that is hogging the resources.

Target of the test: Oracle VM Server

Agent deploying the test: A remote agent

Outputs of the test: One set of results for the Oracle VM Server being monitored

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** – The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is

<table>
<tr><td></td><td colspan="3">set to Yes by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default.

6. WEBPORT - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the WEBPORT parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.

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 enable/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 rowspan="5">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Number of processors:

Indicates the number of processors supported by the server.</td><td>Number</td><td></td></tr>
<tr><td>Cores per socket:

Indicates the number of cores available per socket of the server.</td><td>Number</td><td></td></tr>
<tr><td>Processor speed:

Indicates the speed at which the processors of the server have been configured to run.</td><td>Ghz</td><td></td></tr>
<tr><td>CPU utilization:

Indicates the percentage of CPU resources used by the server and its VMs.</td><td>Percent</td><td>A very high value for this measure indicates excessive CPU utilization by the processors. The CPU utilization may be high because a few processes could be consuming a lot of CPU, or because there are too many processes contending for a</td></tr>
</table>

			limited resource. The detailed diagnosis of this measure, if enabled, lists the VMs and the physical CPU usage of each so that, the virtual machine that consumes the maximum CPU can be isolated.

The detailed diagnosis of the *CPU utilization* measure lists the VMs and the physical CPU usage of each so that, the virtual machine that consumes the maximum CPU can be isolated.

Lists the top ten VMs by physical cpu utilized

VM NAME	PHYSICAL CPU UTILIZED(%)
Sep 22, 2014 05:07:40	
CRM-ORACLE 11G	45.8306
24x7-MSSQL-PR	10.2429
MSFILE-PR	5.2851
PUB APPS-DR	5.2357
APPS-DR	5.2761
PROD-APPS-PR	5.265

Figure 2.3: The detailed diagnosis of the CPU utilization measure of the OVM-Compute test

2.1.2 Control Domain Test

When Oracle VM Server for SPARC software is installed, a domain called the control domain is created. From this control domain, you can create virtual machines called logical domains that each run an independent OS. The control domain manages the logical domains and in the process consumes the physical CPU and memory resources of the Oracle VM server. In the event of a resource contention, administrators must figure out what is draining resources from the server – is it the control domain? Or is it one/more of the logical domains on the server? Using this test, administrators can accurately tell whether/not the control domain is contributing to the resource crunch experienced by the Oracle VM server.

Target of the test: Oracle VM Server

Agent deploying the test: A remote agent

Outputs of the test: One set of results for the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web

	services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Processors assigned: Indicates the number of processors assigned to the control domain.	Number	
	CPU utilization: Indicates the percentage of physical CPU resources utilized by the control domain.	Percent	If the value of this measure consistently grows closer to 100%, it is indicative of excessive CPU usage by the control domain.
	Memory used: Indicates the amount of memory used by the control domain.	MB	Ideally, the value of this measure should be low.

2.1.3 OVM – Memory Test

Excessive memory usage by the Oracle VM server and its VMs can significantly degrade the quality of a user's experiencewith the server. Under such circumstances, administrator need to identify what is causing the memory bottleneck – is it the host? Or is the VMs on the host? Using the **OVM – Memory** test administrators can quickly understand how the VMs are using the memeory resources and can thus determine whether/not they are likely to cause a memory contention on the host.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics.In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port. 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 enable/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.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**

	Total physical memory: Indicates the total amount of physical memory on the host.	MB	
	Memory usable by VMs: Indicates the amount of memory allocated to VMs for use.	MB	
	Used physical memory: Indicates the amount of physical memory used.	MB	A low value is desired for this measure.
	Usage of physical memory: Indicates the percentage of total physical memory resources used.	Percent	A value close to 100% is indicative of excessive usage of physical memory on the host. This can significantly degrade the performance of the host operating system.
	Memory consumed by VMs: Indicates the amount of physical memory consumed by the VMs.	MB	Ideally, the value of this measure should be low. Using the detailed diagnosis of this measure, you can determine the amount of memory used by each VM.
	Percent of physical memory free: Indicates the percentage of physical memory resources of the host that is currently unused.	Percent	A very low value for this measure indicates a shortage of memory resources. If more machine memory is not made available soon, then this could significantly degrade the performance of the host operating system and the VMs.

The detailed diagnosis of the Memory consumed by VMs measure clearly indicates the VMs that are using the host's memory resources and the amount and percentage of memory utilized by each VM. From the detailed diagnostics, administrators can quickly identify which VM is draining the memory resources of the host.

Lists the top ten VMs by memory consumed

VM NAME	CONSUMED MEMORY(MB)	PHYSICAL MEMORY UTILIZED(%)
Sep 22, 2014 05:08:30		
24x7-MSSQL-PR	4097.6303	10.004
CRM-ORACLE 11G	4093.251	9.9933
MSFILE-PR	2049.8943	5.0046
APPS-DR	2049.2553	5.0031
PROD-APPS-PR	2041.8907	4.9851
PUB APPS-DR	2041.4456	4.984

Figure 2.4: The detailed diagnosis of the Memory consumed by VMs measure

2.1.4 OVM Local File System Test

Network Attached Storage - typically NFS - is a commonly used file-based storage system that is very suitable for the installation of Oracle VM storage repositories. Storage repositories contain various categories of resources such as templates, virtual disk images, DVD iso files and virtual machine configuration files, which are all stored as files in the directory structure on the remotely located, attached file system. Since these resources tend to consume space in the file system, administrators will have to closely track how each NFS storage is utilized and proactively detect any potential space shortage. This can be performed using the **OVM Local File System** test. With the help of this test, the space usage on each file system can be checked and the exact file system that may run out of space very soon.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each file system attached to the Oracle VM Server being monitored

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** - The port at which the host listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** - This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL**- By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In some such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**

	File system capacity: Indicates the total capacity of this file system.	MB	
	Free space: Indicates the amount of space in this file system that is still to be used.	MB	A high value is desired for this measure. A consistent drop in this value is indicative of a steady space erosion, which is a cause for concern. Compare the value of this measure across file systems to know which file system is running short of free space.
	Used space: Indicates the amount of space used on this file system.	MB	A low value is desired for this measure. Compare the value of this measure across file systems to know which file system has very little
	Local file system utilization: Indicates the percentage of space in this file system that is currently in use.	Percent	A value close to 100% is indicative of excessive usage of file system space. This can significantly degrade the performance of the host operating system.
	Is shared file system?: Indicates whether/not this file system is shared.		NFS storage is exposed to Oracle VM Servers in the form of shares on the NFS server which are mounted onto the Oracle VM Server's file system. Since mounting an NFS share can be done on any server in the network segment to which NFS is exposed, it is possible not only to share NFS storage between servers of the same pool but also across different server pools. If an NFS file system is shared between servers of the same/different pools, then the value of this measure is Yes. If the NFS file system is not shared, then the value of this measre is No. The values that this measure can report and their corresponding numeric values are discussed in the table below: **Measure Value** / **Numeric Value** Yes / 1 No / 0 **Note:** By default, this measure reports one of the values

			listed under **Measure Values** to indicate whether/not a file system is shared. In the graph of this measure however, the same is represented using the numeric equivalents only.

2.1.5 OVM – SAN Server Storage Test

Besides local storage and NFS storage, Oracle VM also allows administrators to use the following types of SAN storage:

- iSCSI Storage Attacsshed Network
- Fibre Channel Storage Attached Network.

With Internet SCSI, or iSCSI, you can cone ct storage entities to client machines, making the disks behave as if they are locally attached disks. Fibre channel SAN uses dedicated hardware such as special controllers on the SAN hardware, host bus adapters or HBAs on the client machines, and special fibre channel cables and switches to interconnect the components

Regardless of the SAN storage used, the space usage on the storage medium has to be observed, so that abnormal usage trends can be captured early, and potential space shortages can be averted. This is possible using the **OVM – SAN Server Storage** test. For each SAN server storage used by the Oracle VM server, this test reports the current status of the storage and the space usage on the storage. In the process, offline storage arrays and those that are running out of free space can be accurately isolated.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each SAN storage attached to the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the

	CONFIRM PASSWORD text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In some environments, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Capacity: Indicates the total capacity of this SAN storage.	MB	
	Free space: Indicates the amount of space in this SAN storage that is still unused.	MB	A high value is desired for this measure. A consistent drop in this value is indicative of a steady space erosion, which is a cause for concern. Compare the value of this measure across SAN storage arrays to know which array is running short of free space.
	Used space: Indicates the amount of space used on this SAN storage.	MB	A low value is desired for this measure. Compare the value of this measure across arrays to know which arrays has very little free space.
	SAN server utilization: Indicates the percentage of space in this storage array that is currently in use.	Percent	A value close to 100% is indicative of excessive usage of space. This can significantly degrade the performance of the host operating system and VMs using this array.
	Allocated space: Indicates the amount of space that is available for use by the SAN server.	MB	
	Status: Indicates whether/not this SAN storage is online currently.		The values that this measure can report and their corresponding numeric values are discussed in the table below:

			<table><tr><td>Measure Value</td><td>Numeric Value</td></tr><tr><td>Online</td><td>1</td></tr><tr><td>Offline</td><td>0</td></tr></table> **Note:** By default, this measure reports one of the values listed under **Measure Values** to indicate the current status of a storage array. In the graph of this measure however, the same is represented using the numeric equivalents only.

2.1.6 System - Console Test

The **Control Domain** test discussed above reports the CPU and memory usage of the control domain. While this can indicate a contention for resources on the control domain, it cannot lead admiistrators to the exact process (es) executing on the domain that could be causing the contention. To enable administrtors to accurately diagnose the root-cause of CPU or memory contentions experienced by the control domain, and to facilitate effective analysis of its impact on other parameters such as run queue length and swap memory usage, eG Enterprise offers the specialized **System - Console** test.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page. To access this page, follow the Tests -> Enable/Disable menu sequence in the **Agents** tile of the **Admin** tile menu. In the **ENABLE/DISABLE TESTS** page, pick *Oracle VM Server* as the **Component type**, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Oracle VM Server being monitored

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** – The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the

credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default.
6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.
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 enable/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.

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Virtual CPU utilization of console: This measurement indicates the percentage of utilization of the CPU time of the control domain.	Percent	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 control domain.
	System usage of CPU by console: Indicates the percentage of CPU time spent for system-level processing.	Percent	An unusually high value indicates a problem and may be due to too many system-level tasks executing simultaneously.
	Run queue length of console:	Number	A value consistently greater than 2 indicates that many processes could be

	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.		simultaneously contending for the processor.
	Blocked processes on console: Indicates the number of processes blocked for I/O, paging, etc.	Number	A high value could indicate an I/O problem on the console (e.g., a slow disk).
	Swap memory of console: 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 of console OS: Indicates the free memory available.	MB	A very low value of free memory is also an indication of high memory utilization. The detailed diagnosis of this measure lists the top 10 processes responsible for maximum memory consumption on the control domain.

2.1.7 Disk Space - Console Test

This test auto-discovers the disk partitions supported by the control domain, and reports the space usage of each partition; this way, space-hungry partitions can be isolated.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page. To access this page, follow the Tests -> Enable/Disable menu sequence in the **Agents** tile of the **Admin** tile menu. In the **ENABLE/DISABLE TESTS** page, pick *Oracle VM Server* as the **Component type**, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each disk partition of the control domain

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** – The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER** user and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In some environments, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total capacity: Indicates the total capacity of a disk partition; for the Total descriptor however, this measure indicates the total capacity across all disk partitions.	MB	
	Used space: Indicates the amount of space used in a disk partition; for the Total descriptor however, this measure indicates the sum of space used across all disk partitions of the control domain.	MB	Ideally, this value should be low.
	Free space:	MB	Ideally, this value should be high.

	Indicates the current free space available for each disk partition; for the Total descriptor however, this measure indicates the sum of free space available across all disk partitions.		
	Percent usage: Indicates the percentage of space usage on each disk partition; for the Total descriptor however, this measure indicates the percentage of space utilized across all disk partitions.	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.

2.1.8 Disk Activity - Console Test

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

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page. To access this page, follow the Tests -> Enable/Disable menu sequence in the **Agents** tile of the **Admin** tile menu. In the **ENABLE/DISABLE TESTS** page, pick *Oracle VM Server* as the **Component type**, *Performance* as the **Test type**, choose this test from the **DISABLED TESTS** list, and click on the **<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test: Oracle VM Server

Agent deploying the test: A remote agent

Outputs of the test: One set of results for each disk partition of the control domain

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE**

	VM MANAGER USER and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Percent disk busy: Indicates the percentage of elapsed time during which the disk is busy processing requests (i.e., reads or writes).	Percent	Comparing the percentage of time that the different disks are busy, an administrator can determine whether load is properly balanced across the different disks.
	Disk read time: Indicates the average time (in seconds) taken by the disk to read data.	Secs	Ideally, the value of this measure should be low.
	Disk write time: Indicates the average time (in seconds) taken by the disk to write data.	Secs	Ideally, the value of this measure should be low.
	Reads 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 control domain.
	Data reads from disk: Indicates the rate at	Kbytes/Sec	A very high value indicates an I/O bottleneck.

	which bytes are transferred from this disk during read operations.		
	Writes to disk: Indicates the number of writes happening on this disk per second.	Writes/Sec	A dramatic increase in this value may be indicative of an I/O bottleneck.
	Data writes to disk: Indicates the rate at which bytes are transferred from the disk during write operations.	Kbytes/Sec	A very high value indicates an I/O bottleneck.
	Data writes to disk: Indicates the rate at which bytes are transferred from the disk during write operations.	Kbytes/Sec	A very high value indicates an I/O bottleneck.

2.2 The Network Layer

This layer monitors the network connection to the Oracle VM server and reports whether/not it is available currently. The quality of the connection is also verified and reported.

Figure 2.5: The test mapped to the Network layer

Since the test mapped to this layer is already discussed in the Monitoring Unix and Windows Servers document, let us proceed to look at the next layer.

2.3 The VM Server Layer

This layer reports the current status of the Oracle VM server and availability of the Oracle VM Manager's web interface.

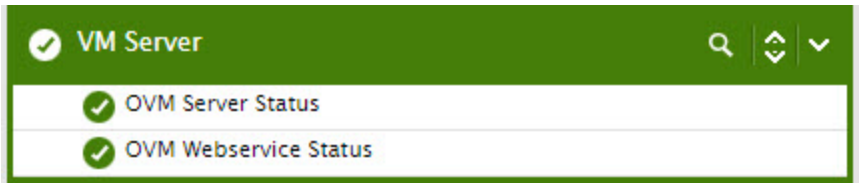


Figure 2.6: The tests mapped to the VM Server layer

2.3.1 OVM Server Status Test

If a user complains that he/she is unable access a VM on an Oracle VM server, more often than not the reason for the inaccessibility is that the server has stopped running. To spot such abnormalities before a user complains, administrators can use the **OVM Server Status** test. This test tracks the status of the Oracle VM server and reports whether it is running or not. In addition, it indicates whether/not the server is in maintenance mode.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the oracle vm manager text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that

<table>
<tr><td></td><td colspan="3">port.</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>Server status:
Indicates the current status of the Oracle VM server.</td><td></td><td>The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Stopped</td><td>0</td></tr><tr><td>Running</td><td>1</td></tr><tr><td>Starting</td><td>2</td></tr><tr><td>Not running</td><td>3</td></tr></table>Note:
By default, this measure reports one of the values listed under Measure Values to indicate the current status of an Oracle VM server. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
<tr><td></td><td>Is in maintenance mode?:
Indicates whether/not the server is in maintenance mode.</td><td></td><td>An Oracle VM Server can be placed into maintenance mode to perform hardware or software maintenance. When an Oracle VM Server is placed in maintenance mode, any virtual machines running on the Oracle VM Server are automatically migrated to other Oracle VM Servers in the server pool, if they are available; otherwise they are stopped.
The values that this measure can report and their corresponding numeric values are discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>Note:</td></tr>
</table>

			By default, this measure reports one of the values listed under **Measure Values** to indicate whether/not the server is in maintenance mode. In the graph of this measure however, the same is represented using the numeric equivalents only.

2.3.2 OVM Webservice Status Test

Without access to the Oracle VM manager's web services interface, administrators cannot add VM servers, create VMs, create storage repositories, server pools, import resources, or any other management activity. It is therefore imperative that administrators are notified of the unavailability of or delays in access to the web services interface of the Oracle VM Manager. The **OVM Webservice Status** test does just that! This test emulates an HTTP/S access to the Oracle VM Manager's web services interface and reports whether/not the interface is accessible, and if so, how quickly the connection was made. This way, administrators can promptly detect the unavailability of the web services interface and a probable slowdown in access to the interface.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case,

	against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Availability: Indicates whether/not the web interface is available.	Percent	If the interface is accessible, the value of this measure will be 100. If not, the value will be 0.
	Response time: Indicates the time it took to connect to the web interface.	Secs	If the value of this measure consistently increases, it indicates a bottleneck in connectivity to the Oracle VM manager's web interface.

2.4 Outside View of VMs

This layer provides the host operating system's view of the resource usage levels of each of the virtual guests hosted on it. Using the information reported by this test, administrators can:

- Determine which of the guests is taking up more resources (CPU, memory, network, or disk) than the others. This information can help with load balancing or capacity planning. For example, if one of the guests is receiving a very high rate of requests compared to the others, this guest may be a candidate for migration to another Oracle VM server, so as to minimize the impact it has on the other guests on the current Oracle VM server.
- 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.
- Understand how resources are shared amongst all available resource pools, and identify resource pools that have been over-utilized.

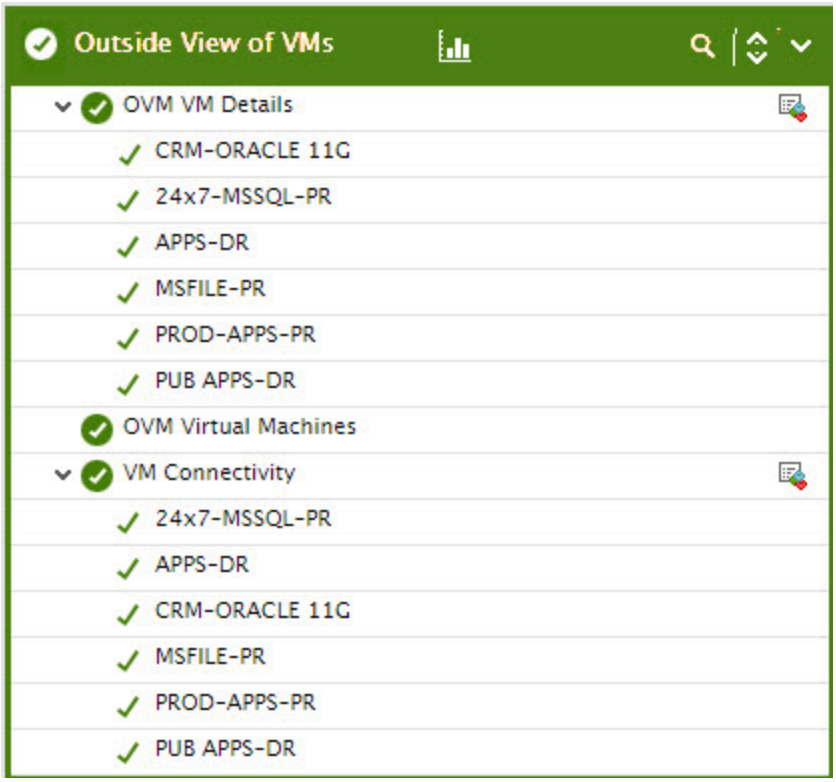


Figure 2.7: The tests mapped to the Outside View of VMs layer

2.4.1 OVM VM Details Test

This test monitors the amount of the physical server's resources that each virtual machine on an Oracle VM server is taking up. Using the metrics reported by this test, administrators can determine which virtual machine is taking up most CPU, which guest is taking up the maximum resources.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each VM on the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the

credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default.
6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.
7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

   Note:

   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.

10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect “inside view” metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)** : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

      If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with

the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations*. Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key-based Authentication* refer to the Monitoring VMware Infrastructures document.

- **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 PASSWORD**s 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.

- **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*.

12. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG 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 enable/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 abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	VM state: Indicates the current operational state of this VM.		The values that this measure can report and their corresponding numeric values are discussed in the table below: **Measure Value** / **Numeric Value** Stopped / 0

			<table><tr><td>Running</td><td>1</td></tr><tr><td>Starting</td><td>2</td></tr><tr><td>Stopping</td><td>3</td></tr><tr><td>Suspended</td><td>4</td></tr><tr><td>Template</td><td>5</td></tr></table> **Note:** By default, this measure reports one of the values listed under **Measure Values** to indicate the current status of VM. In the graph of this measure however, the same is represented using the numeric equivalents only.
	vCpu count: Indicates the number of virtual CPUs allocated to this VM.	Number	
	Max vCpu limit: Indicates the number of processors that this VM is allowed to make use of.	Number	
	Virtual processor utilization: Indicates the percentage of the vCPUs allowed for use that is currently in use.	Percent	A high value for this measure indicates that the VM is consuming too many vCPUs. Compare this value across VMs to know which VM is consuming the maximum vCPUs.
	Physical processor utilization: Indicates the percentage of the physical CPUs currently used by this VM.	Percent	A high value for this measure indicates that the VM is consuming too many vCPUs physical CPUs. A probable cause for high CPU utilization is the presence of one or more CPU-intensive processes on the VM. Use the detailed diagnosis of this measure to identify the CPU-intensive processes running on a VM.
	vCpu priority: Indicates CPU priority value set for for this VM when scheduling.	Number	
	vCpu cap: Indicates the maximum	Number	Oracle VM's default CPU scheduler is the credit scheduler. The credit scheduler uses a credit/debit

	number of CPUs used by this VM, as per the credit scheduler.		system to fairly share CPU resources between virtual machines. Credits are assigned to each running virtual machine, along with the allocated fraction of CPU resources. The credit scheduler continually increments/decrements credits from running virtual machines, which is how the credit scheduler balances CPU resources.
	Current memory: Indicates the amount of memory currently used by this VM.	MB	
	Allocated memory: Indicates the amount of memory allocated to this VM.	MB	
	Memory limit: Indicates the maximum amount of memory that this VM can consume.	MB	
	Physical memory utilization: Indicates the percentage of physical memory used by this VM.	Percent	Compare the value of this measure across VMs to know which VM is consuming the maximum memory. A high value for this measure indicates that the VM is consuming memory resources excessively. One of the common causes for this is the execution of one/more memory- intensive operations on the VM. Use the detailed diagnosis of this measure to identify the memory-intensive processes running on a VM.
	Disk capacity: Indicates the total disk capacity of this VM.	MB	
	Huge pages: Indicates whether/not Huge Pages are enabled for this VM.		Paging is a process whereby the CPU, for a system, allocates contiguous blocks of memory for use by a running process. These pages are tracked by the operating system, so that processes access the correct blocks of assigned memory. Typically, these blocks are sized at 4 KB. This means that when a process uses 1 GB of memory, 262144 page (1 GB/4 KB) entries are

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>created and are referenced continually by the process.

Most current CPU architectures support bigger pages to reduce the number of page lookups required by the CPU or Operating System. On Linux systems, these are called Huge Pages, while on Windows systems they are called Large Pages. These terminologies are equivalent.

Oracle VM Manager provides an option to enable huge page support for a paravirtualized virtual machine when you create or edit a virtual machine. Huge pages are not supported on virtual machines running on SPARC architecture. Attempting to enable Huge Page support for a virtual machine running on a SPARC server, causes an exception to be returned.

The values that this measure can report and their corresponding numeric values are discussed in the table below:

<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Enabled</td><td>1</td></tr>
<tr><td>Disabled</td><td>0</td></tr>
</table>

Note:

By default, this measure reports one of the values listed under Measure Values to indicate whether/not Huge Pages are enabled for a VM. In the graph of this measure however, the same is represented using the numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>High availability:

Indicates whether/not high availability is enabled for this VM.</td>
<td></td>
<td>You can set up High Availability to help ensure the uninterrupted availability of a virtual machine. If HA is configured and a Oracle VM Server is restarted or shut down, the virtual machines running on it are either restarted on, or migrated to, another Oracle VM Server.

The values that this measure can report and their corresponding numeric values are discussed in the table below:</td>
</tr>
</table>

			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>0</td></tr></table> **Note:** By default, this measure reports one of the values listed under **Measure Values** to indicate whether/not HA is enabled for a VM. In the graph of this measure however, the same is represented using the numeric equivalents only.

2.4.2 OVM Virtual Machines Test

Live migration is a process to move a running virtual machine from one Oracle VM Server to another, while applications on the existing virtual machine continue to run. Because of live migration, administrators often struggle to determine which VM was migrated between which two Oracle VM servers. This is where the **OVM Virtual Machines** test helps. This test enables administrators to determine how many guests have registered with the Oracle VM server, and how many of these are currently running. In addition, the test also indicates whether any guests have migrated to or from the virtual server.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Oracle VM Server being monitored

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** – The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the

Oracle VM Manager via HTTPS by default.

6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.
7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.
   Note:
   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.
10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)** : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

      If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations* . Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on

Implementing Key- based Authentication refer to the *Monitoring VMware Infrastructures* document.

- **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 PASSWORD**s 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.

- **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*.

12. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG 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 enable/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.

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Registered VMs: Indicates the number of VMs that are registered with the Oracle VM server.	Number	
	VMs powered on: Indicates the number of VMs that are currently powered on.	Number	Use the detailed diagnosis of this measure to know which VMs are powered on.
	Added VMs: Indicates the number of VMs that were migrated to the Oracle VM server during the last measurement period.	Number	Use the detailed diagnosis of this measure to know which VMs were newly migrated to the Oracle VM server being monitored.
	Removed VMs:	Number	Use the detailed diagnosis of this measure

	Indicates the number of VMs that were migrated from the Oracle VM server during the last measurement period.		to know which VMs were newly migrated from the Oracle VM server being monitored.

2.5 Inside View of VMs

The **Outside View of VMs** layer provides an “outside” view of the different VM guests - the metrics reported at this layer are based on what the Oracle VM server is seeing about the performance of the individual guest VMs. However, an outside view of the VM guest operating system and its applications may not be sufficient. For instance, suppose one of the disk partitions of the guest operating system has reached capacity. This information cannot be gleaned from host operating system. Likewise, bottlenecks such as a longer process run queue or a higher disk queue length are more visible using an internal monitor. Internal monitoring (from within the guest operating system) also provides details about the resource utilization of different application (s) or processes.

The tests mappedS to the **Inside View of VMs** layer provide an "inside" view of the workings of each of the guests - these tests send probes into each of the guest operating systems to analyze how well each guest utilizes the resources that are allocated to it, and how well it handles user sessions, TCP traffic, and network loading.

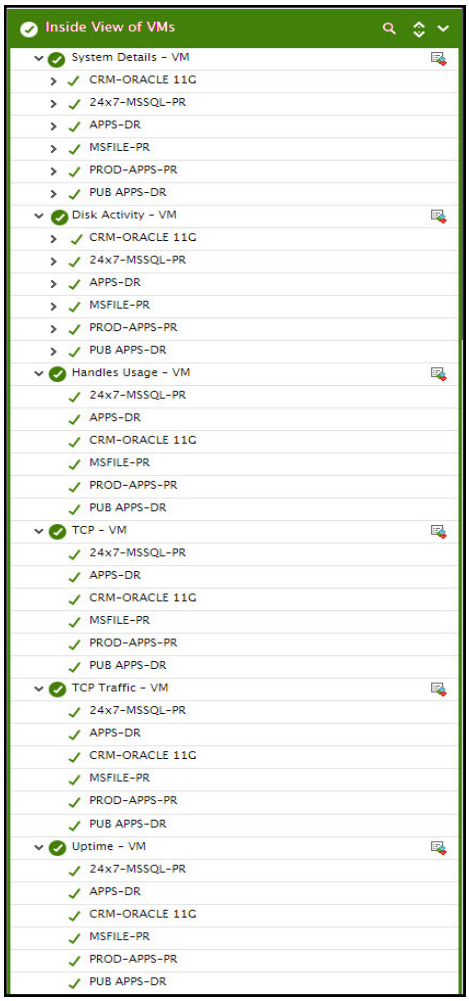


Figure 2.8: The tests mapped to the Inside View of VMs layer

2.5.1 Disk Activity - VM Test

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

Target of the test: Oracle VM Server

Agent deploying the test: A remote agent

Outputs of the test: One set of results for each disk partition on each powered-on VM of the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle

VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default.
6. **WEBPORT** - By default, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.
7. **EXCLUDE VMS**- Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW**- Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

Note:

While performing VM discovery, the eG agent will not discover the operating system of

	the VMs configured in the **IGNORE VMS INSIDE VIEW**text box. 9. **IGNORE WINNT**- By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT**flag is set to **Yes**by default. 10. **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 (Windows)** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights**. 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*. 11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)** : In this case, specify "none" in the **DOMAIN** field, and specify a local administrator account name in the **ADMIN USER** 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. Then, proceed to provide the password of the **ADMIN USER** against **ADMIN PASSWORD**, and confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

	If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the **ADMIN USER** text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named authorized_keys . The **ADMIN PASSWORD** in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations*. Specify this as the **ADMIN PASSWORD** if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key-based Authentication* refer to the *Monitoring VMware Infrastructures* document. • **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 PASSWORD**s 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. • **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*. 12. **DETAILED DIAGNOSIS**- To make diagnosis more efficient and accurate, the eG 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 enable/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.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Percent virtual disk busy: Indicates the percentage of elapsed time during which the disk is busy processing requests (i.e., reads or writes).	Percent	Comparing the percentage of time that the different disks are busy, an administrator can determine whether load is properly balanced across the different disks.

	Percent reads from virtual disk: Indicates the p ercentage of elapsed time that the selected disk drive is busy servicing read requests.	Percent	
	Percent writes to virtual disk: Indicates the percentage of elapsed time that the selected disk drive is busy servicing write requests.	Percent	
	Virtual disk read time: Indicates the average time in seconds of a read of data from the disk.	Secs	
	Virtual disk write time: Indicates the average time in seconds of a write of data from the disk.	Secs	
	Avg. queue for virtual disk: Indicates the average number of both read and write requests that were queued for the selected disk during the sample interval.	Number	
	Current queue for virtual disk: 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.

	Reads from virtual 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 virtual 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.
	Writes to virtual 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 virtual 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.
	Disk service time: Indicates the average time that this disk took to service each transfer request (i.e., the average I/O operation time)	Secs	A sudden rise in the value of this measure can be attributed to a large amount of information being input or output. A consistent increase however, could indicate an I/O processing bottleneck.
	Disk queue time: Indicates the average time that transfer requests waited idly on queue for this disk.	Secs	Ideally, the value of this measure should be low.
	Disk I/O time: Indicates the average time taken for read and write operations of this disk.	Secs	The value of this measure is the sum of the values of the Disk service time and Disk queue time measures. A consistent increase in the value of this measure could indicate a latency in I/O processing.
	Percent virtual disk busy: Indicates the percentage of elapsed time during which the disk is busy processing requests (i.e., reads or writes).	Percent	Comparing the percentage of time that the different disks are busy, an administrator can determine whether load is properly balanced across the different disks.
	Percent virtual disk busy: Indicates the percentage of elapsed time during which the disk	Percent	Comparing the percentage of time that the different disks are busy, an administrator can determine whether load is properly balanced

	is busy processing requests (i.e., reads or writes).		across the different disks.

2.5.2 Disk Space - VM Test

This test monitors the space usage of every disk partition on a guest.

Target of the test: Oracle VM Server

Agent deploying the test: A remote agent

Outputs of the test: One set of results for each disk partition on each powered-on VM of the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with *Admin* rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port. 7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box.

Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your **EXCLUDE VMS** specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.

8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.
   Note:
   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT operating systems**. Accordingly, the **IGNORE WINNT** flag is set to **Yes**by default.
10. **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 (Windows) on every **WINDOWS VM; THIS VM AGENT ALLOWS THE EG AGENT TO COLLECT "INSIDE VIEW" METRICS FROM THE WINDOWS VMS** without domain administrator rights. 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*.
11. **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 do not belong to any domain (as in the case of Linux/Solaris guests) :** In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

  If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations* . Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key- based Authentication* refer to the *Monitoring VMware Infrastructures* document.
- **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 PASSWORD**s 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.
- **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*.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total capacity: Indicates the total capacity of a disk partition; for the **Total** descriptor, this measure reports the sum of the total capacity of all disk partitions.	MB	
	Used space: Indicates the amount of space used in a disk partition; for the **Total** descriptor, this measure reports the sum of space used across all disk partitions.	MB	
	Free space: Indicates the current free space available for each disk partition of a system; for the **Total** descriptor, this measure reports the sum of the unused space in all disk partitions.	MB	
	Percent usage: Indicates the percentage of space usage on each disk	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

	partition of a system; for the **Total** descriptor, this measure reports the percentage of disk space used across all disk partitions.		usage.

2.5.3 System Details – VM Test

This test collects various metrics pertaining to the CPU and memory usage of every processor supported by a guest.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each processor supported by each powered-on VM of the Oracle VM Server being monitored

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** – The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that

port.

7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

   Note:

   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.
10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests) :** In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

      If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations* . Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key- based Authentication* refer to the Monitoring VMware Infrastructures document.

    - **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 PASSWORD**s 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. • **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*. 14. **ENABLE MEMORY DIAGNOSIS** - By default, the *ENABLE MEMORY DIAGNOSIS* flag is set to **NO**, indicating that detailed diagnosis will not be available for the Free memory in VM measure reported by this test by default. If you want to view the detailed diagnosis of the Free memory in VM measure - i.e., to view the top 10 processes on the VM that are utilizing memory excessively - you can change this flag to **YES**. 15. **USE TOP FOR DD** - **This parameter is applicable only to Linux VMs**. By default, this parameter is set to **No**. This indicates that, by default, this test will report the detailed diagnosis of the Virtual CPU utilization measure for each processor on a Linux VM by executing the usr/bin/ps command. On some Linux flavors however, this command may not function properly. In such cases, set the **USE TOP FOR DD** parameter to **Yes**. This will enable the eG agent to extract the detailed diagnosis of the Virtual CPU utilization measure by executing the /usr/bin/top command instead. 16. **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 *DD FREQUENCY.* 17. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG 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 enable/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.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Virtual CPU utilization: This measurement indicates	Percent	A high value could signify a CPU bottleneck. The CPU utilization may be high because a

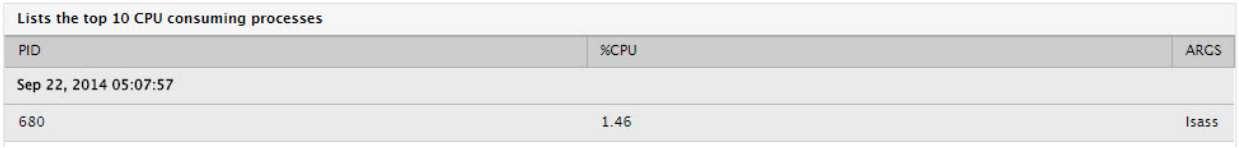
	the percentage of CPU utilized by the processor.		few processes are consuming a lot of CPU, or because there are too many processes contending for a limited resource. The detailed diagnosis of this test reveals the top-10 CPU-intensive processes on the guest.
	System usage of virtual CPU: Indicates the percentage of CPU time spent for system-level processing.	Percent	An unusually high value indicates a problem and may be due to too many system-level tasks executing simultaneously.
	Run queue in VM: 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.	Number	A value consistently greater than 2 indicates that many processes could be simultaneously contending for the processor.
	Blocked processes in VM: Indicates the number of processes blocked for I/O, paging, etc.	Number	A high value could indicate an I/O problem on the guest (e.g., a slow disk).
	Swap memory in VM: 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 in VM: 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, if enabled, lists the top 10 processes responsible for maximum memory consumption on the guest.
	Scan rate in VM: Indicates the memory scan rate.	Pages/Sec	A high value is indicative of memory thrashing. Excessive thrashing can be detrimental to guest performance.

Note:

For multi-processor systems, where the CPU statistics are reported for each processor on the system, the statistics that are system-specific (e.g., run queue length, free memory, etc.) are only reported for the

"Summary" descriptor of this test.

The detailed diagnosis capability of the *Virtual CPU utilization* measure, if enabled, provides a listing of the top 10 CPU-consuming processes (see Figure 2.9). In the event of a Cpu bottleneck, this information will enable users to identify the processes consuming a high percentage of CPU time. The users may then decide to stop such processes, so as to release the CPU resource for more important processing purposes.



Lists the top 10 CPU consuming processes

PID	%CPU	ARGS
Sep 22, 2014 05:07:57		
680	1.46	lsass

Figure 2.9: The top 10 CPU consuming processes

Note:

While instantaneous spikes in CPU utilization are captured by the eG agents and displayed in the Measures page, the detailed diagnosis will not capture/display such instantaneous spikes. Instead, detailed diagnosis will display only a consistent increase in CPU utilization observed over a period of time.

2.5.4 Uptime – VM Test

In most virtualized environments, it is essential to monitor the uptime of VMs hosting critical server applications in the infrastructure. By tracking the uptime of each of the VMs, administrators can determine what percentage of time a VM has been up. Comparing this value with service level targets, administrators can determine the most trouble-prone areas of the virtualized infrastructure.

In some environments, administrators may schedule periodic reboots of their VM. By knowing that a specific VM has been up for an unusually long time, an administrator may come to know that the scheduled reboot task is not working on a VM.

The **Uptime - VM** test included in the eG agent monitors the uptime of each VM on an Oracle VM server.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on VM on the Oracle VM Server being monitored

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** – The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using

the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default.
6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.
7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

   Note:

   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag

is set to **Yes** by default.

10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)* : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

      If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the

user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations*. Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key-based Authentication* refer to the Monitoring VMware Infrastructures document.

- **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 PASSWORD**s 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.

- **If the INSIDE VIEW USINGflag 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*.

12. **REPORTMANAGERTIME** - By default, this flag is set to **Yes**, indicating that, by default, the detailed diagnosis of this test, if enabled, will report the shutdown and reboot times of the VMs in the manager's time zone. If this flag is set to **No**, then the shutdown and reboot times are shown in the time zone of the system where the agent is running (i.e., the system being managed for agent-based monitoring, and the system on which the remote agent is running - for agentless monitoring).
13. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG 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 enable/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.

Measurements made by the test	Measurement	Measurement Unit	Interpretation

	Has the VM been rebooted?: Indicates whether this guest has been rebooted during the last measurement period or not.	Boolean	If this measure shows 1, it means that the guest was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this guest was rebooted.
	Uptime of the VM during the last measure period: Indicates the time period that the guest has been up since the last time this test ran.	Secs	If the guest has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the VM was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the VM was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period - the smaller the measurement period, greater the accuracy.
	Total uptime of the VM: Indicates the total time that the guest has been up since its last reboot.	Mins	Administrators may wish to be alerted if a VM has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

Note:

If a value less than a minute is configured as the **TEST PERIOD** of the **Uptime - VM** test, then, the *Uptime* during the last measure period measure will report the value 0 for Unix VMs (only) until the minute boundary is crossed. For instance, if you configure the **Uptime - Guest** test to run every 10 seconds, then, for the first 5 test execution cyles (i.e., 10 x 5 = 50 seconds), the *Uptime* during the last measure period measure will report the value 0 for Unix VMs; however, the sixth time the test executes (i.e, when test execution touches the 1 minute boundary), this measure will report the value 60 seconds for the same VMs. Thereafter, every sixth measurement period will report 60 seconds as the uptime of the Unix VMs. This is because, Unix-based operating systems report uptime only in minutes and not in seconds.

2.5.5 Windows Memory – VM Test

To understand the metrics reported by this test, it is essential to understand how memory is handled by the operating system. On any Windows 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 non-paged 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 **WindowsMemory – VM** test tracks critical metrics corresponding to the System PTEs and the pool areas of kernel memory of a Windows virtual machine.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on Windows VM on the Oracle VM Server being monitored

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** – The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port. 7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated

list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.

8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

   Note:

   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.

9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.

10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)** : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

  If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations* . Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key- based Authentication* refer to the Monitoring VMware Infrastructures document.

- **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 PASSWORD**s 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.

- **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*.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Free entries in system page table: Indicates the number of page table entries not currently in use by the guest.	Number	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.
	Page read rate in VM: Indicates the average number of times per second the disk was read to resolve hard fault paging.	Reads/Sec	
	Page write rate in VM: Indicates the average number of times per second the pages are written to disk to free up the physical memory.	Writes/Sec	
	Page input rate in VM: Indicates the number of times per second that a process needed to access apiece of memory that was not in its working set, meaning that the guest had to retrieve it from the page file.	Pages/Sec	
	Page output rate in VM: 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.

	Memory pool non-paged data in VM: Indicates the total size of the kernel memory nonpaged 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 pool paged data in VM : 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.

2.5.6 Windows Network Traffic – VM Test

This test monitors the incoming and outgoing traffic through each Windows guest of an Oracle VM server.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each network interface supported by every powered-on Windows VM on the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web

services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default.
6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.
7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

   Note:

   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW**text box.

9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.

10. **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 (Windows)** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** 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*.

11. **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 specification:

    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.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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD*, and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the

	password *eginnovations*. Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key-based Authentication* refer to the *Monitoring VMware Infrastructures* document. **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 PASSWORD**s 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. **If the INSIDE VIEW USINGflag 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. *If the guests do not belong to any domain (as in the case of Linux/Solaris guests)* : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* below.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Incoming traffic: Indicates the rate at which data (including framing characters) is received on a network interface.	Mbps	An abnormally high rate of incoming traffic may require additional analysis.
	Outgoing traffic: Represents the rate at which data (including framing characters) is sent on a network interface.	Mbps	An abnormally high rate of outgoing traffic may require additional analysis.
	Maximum bandwidth: An estimate of the capacity of a network interface.	Mbps	
	Bandwidth usage: Indicates the percentage of bandwidth used by a network interface.	Percent	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.
	Output queue length:	Number	If this is longer than 2, delays are being

	Indicates the length of the output packet queue (in packets)		experienced and the bottleneck should be found and eliminated if possible.
	Outbound packet errors: The number of outbound packets that could not be transmitted because of errors	Number	Ideally, number of outbound errors should be 0.
	Inbound packet errors: 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.

2.5.7 Network Traffic – VM Test

This test monitors the incoming and outgoing traffic through each Linux guest on an Oracle VM server.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each network interface supported by every powered-on VM of the Oracle VM Server being monitored

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** - The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** - This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **oracle vm manager** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER** password parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG

agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.

7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: *xp,*lin*,win*,vista. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

   Note:

   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.
10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)** : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

      If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations*. Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key-based Authentication* refer to the *Monitoring VMware Infrastructures* document.

	• **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 PASSWORD**s 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. • **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*.

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Incoming network traffic: Indicates the rate of incoming traffic.	Pkts/Sec	An increase in traffic to the guest can indicate an increase in accesses to the guest (from users or from other applications) or that the guest is under an attack of some form.
	Outgoing network traffic: Represents the rate of outgoing traffic.	Pkts/Sec	An increase in traffic from the guest can indicate an increase in accesses to the guest (from users or from other applications).

2.5.8 Tcp – VM Test

This test tracks various statistics pertaining to TCP connections to and from each guest of an Oracle VM server.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on VM of the Oracle VM Server being monitored

Configurable	1. **TEST PERIOD** - How often should the test be executed

parameters for the test	2. **HOST** - The host for which the test is to be configured. 3. **PORT** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the confirm password text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port. 7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: *xp,*lin*,win*,vista. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs. 8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be:

*xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

Note:

While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW**text box.

9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.

10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect “inside view” metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)* : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator

account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations*. Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key-based Authentication* refer to the Monitoring VMware Infrastructures document.

- **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 PASSWORD**s 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.

- **If the INSIDE VIEW USINGflag 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*.

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Incoming connections to VM: Indicates the connections per second received by the guest.	Conns/Sec	A high value can indicate an increase in input load.
	Outgoing connections to VM: 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 to VM:	Number	A sudden increase in the number of

	Indicates the currently established connections.		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 on VM: 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 on VM: 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.

2.5.9 Tcp Traffic – VM 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.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on VM of the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle

VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default.
6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.
7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

Note:

While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.

9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.

10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)** : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM*

	PASSWORD text box. If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a .ssh directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations*. Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key-based Authentication* refer to the Monitoring VMware Infrastructures document. • **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 PASSWORD**s 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. • **If the INSIDE VIEW USINGflag 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*.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Segments received by VM: Indicates the rate at which segments are received by the guest.	Segments/Sec	
	Segments sent by VM: Indicates the rate at which segments are sent to clients or other guests	Segments/Sec	
	Retransmits by VM: Indicates the rate at which segments are being retransmitted by the guest	Segments/Sec	
	Retransmit ratio from VM:	Percent	Ideally, the retransmission ratio should be low

	Indicates the ratio of the rate of data retransmissions to the rate of data being sent by the guest		(< 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.

2.5.10 Handles Usage – VM Test

This test monitors and tracks the handles opened by processes running in a target Windows virtual machine.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on Windows VM of the Oracle VM Server being monitored

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** – The port at which the host listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that

while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.

7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.

   Note:

   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW** text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.
10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect “inside view” metrics from the Windows VMs without domain administrator rights. 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.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests)** : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

      If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations* . Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key- based Authentication* refer to the Monitoring VMware

Infrastructures document.

- **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 PASSWORD**s 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.

- **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*.

12. **HANDLES GROWTH LIMIT** - This defines the upper limit of the handles opened by any process. By default, this parameter is set to 8000.

13. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG 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 enable/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.

Measurements made by the test

Measurement	Measurement Unit	Interpretation
Handles used by processes of the VM: Indicates the number of handles opened by various processes running in a target Windows virtual machine in the last measurement period.	Number	Use the detailed diagnosis of this measure to determine the top-10 processes in terms of number of handles opened. This information brings to light those processes with too many open handles. By closely tracking the handle usage of these processes over time, you can identify potential handle leaks.
Processes using handles above limit in the VM: Indicates the number of processes that have opened the handles on or above the value defined in the input	Number	Using the detailed diagnosis of this measure, you can accurately isolate the process (es) that has opened more handles than the permitted limit. A high value of this measure indicates that too

	parameter - **HANDLES GROWTH LIMIT**.		many processes are opening handles excessively. You might want to closely observe the handle usage of these processes over time to figure out whether the spike in usage is sporadic or consistent. A consistent increase in handle usage could indicate a handle leak.

2.5.11 Windows Services – VM Test

This test tracks the status (whether running or have stopped) of services executing on Windows virtual machines.

Target of the test: Oracle VM Server

Agent deploying the test: A remote agent

Outputs of the test: One set of results for each powered-on Windows VM of the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with *Admin* rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.

7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the **EXCLUDE VMS** text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the **EXCLUDE VMS** text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.
   Note:
   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW**text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.
10. **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 (Windows)** on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs **without domain administrator rights.** 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*.

11. **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 do not belong to any domain (as in the case of Linux/Solaris guests) :** In this case, specify "none" in the **DOMAIN** field, and specify a local administrator account name in the **ADMIN USER** 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. Then, proceed to provide the password of the **ADMIN USER** against **ADMIN PASSWORD**, and confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

      If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations*. Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key- based Authentication* refer to the Monitoring VMware Infrastructures document.

    - **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 PASSWORD**s 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.

<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.

12. IGNORESERVICES - Provide a comma-separated list of services that need to be ignored while monitoring.
13. 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 DD FREQUENCY.
14. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG 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 enable/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 rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>New automatic services started:
Indicates the number of Windows services with startup type as automatic, which were running in the last measurement period.</td><td>Number</td><td>The detailed diagnosis of this measure lists the services (with startup type as automatic) that are running.</td></tr>
<tr><td>New automatic services stopped:
Indicates the number of Windows services with startup type as automatic, which were not running in the last measurement period.</td><td>Number</td><td>To know which services stopped, use the detailed diagnosis of this measure (if enabled).</td></tr>
<tr><td>New manual services started:
Indicates the number of Windows services with startup type as manual, which were</td><td>Number</td><td>Use the detailed diagnosis of this measure to identify the manual services that are running.</td></tr>
</table>

	running in the last measurement period.		
	New manual services stopped: Indicates the number of Windows services with startup type as *manual*, which stopped running in the last measurement period.	Number	To identify the services that stopped, use the detailed diagnosis of this measure.

2.5.12 Memory Usage – VM Test

This test reports statistics related to the usage of physical memory of the VMs.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on VM of the Oracle VM Server being monitored

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** – The port at which the host listens. By default, this is *NULL*. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER USER** and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port.

7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.
   Note:
   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW**text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.
10. **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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs without domain administrator rights. 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.

11. **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 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 PASSWORD**s 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.
    - *If the guests do not belong to any domain (as in the case of Linux/Solaris guests)* : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the *ADMIN USER* against *ADMIN PASSWORD* , and confirm the password by retyping it in the *CONFIRM PASSWORD* text box.

      If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations* . Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key- based Authentication* refer to the Monitoring VMware Infrastructures 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*.
    - **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.

12. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG 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 enable/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 abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Total memory: Indicates the total memory of this VM.	MB	
	Used memory: Indicates the used memory of this VM.	MB	
	Free memory: Indicates the free memory of the VM.	MB	This measure typically indicates the amount of memory available for use by applications running on the target VM. On Unix operating systems (AIX and Linux), the operating system tends to use parts of the available memory for caching files, objects, etc. When applications require additional memory, this is released from the operating system cache. Hence, to understand the true free memory that is available to applications, the eG agent reports the sum of the free physical memory and the operating system cache memory

			size as the value of the *Free physical memory* measure while monitoring AIX and Linux guest operating systems.
	Memory utilized: Indicates the percent usage of memory by this VM.	Percent	Ideally, the value of this measure should be low. While sporadic spikes in memory usage could be caused by one/more rogue processes on the VM, a consistent increase in this value could be a cause for some serious concern, as it indicates a gradual, but steady erosion of valuable memory resources. If this unhealthy trend is not repaired soon, it could severely hamper VM performance, causing anything from a slowdown to a complete system meltdown. You can use the detailed diagnosis of this measure to figure out which processes on the VM are consuming memory excessively.
	Available memory: Indicates the amount of memory, immediately available for allocation to a process or for system use.	MB	Not all of the *Available memory* is *Free memory*. Typically, *Available memory* is made up of the Standby List, Free List, and Zeroed List. When Windows wants to trim a process' working set, the trimmed pages are moved (usually) to the Standby List. From here, they can be brought back to life in the working set with only a soft page fault (much faster than a hard fault, which would have to talk to the disk). If a page stays in the standby List for a long time, it gets freed and moved to the Free List. In the background, there is a low priority thread (actually, the only thread with priority 0) which takes pages from the Free List and zeros them out. Because of this, there is usually very little in the Free List. All new allocations always come from the Zeroed List, which is memory pages that have been overwritten with zeros. This is a standard part of the OS' cross-process security, to prevent any process ever seeing data from another. If the Zeroed List

			is empty, Free List memory is zeroed and used or, if that is empty too, Standby List memory is freed, zeroed, and used. It is because all three can be used with so little effort that they are all counted as "available". A high value is typically desired for this measure. **This measure will be available for Windows 2008 VMs only.**
	Modified memory: Indicates the amount of memory that is allocated to the modified page list.	MB	This memory contains cached data and code that is not actively in use by processes, the system and the system cache. This memory needs to be written out before it will be available for allocation to a process or for system use. Cache pages on the modified list have been altered in memory. No process has specifically asked for this data to be in memory, it is merely there as a consequence of caching. Therefore it can be written to disk at any time (not to the page file, but to its original file location) and reused. However, since this involves I/O, it is not considered to be Available physical memory. **This measure will be available for Windows 2008 VMs only.**
	Standby memory: Indicates the amount of memory assigned to the standby list.	MB	This memory contains cached data and code that is not actively in use by processes, the system and the system cache. It is immediately available for allocation to a process or for system use. If the system runs out of available free and zero memory, memory on lower priority standby cache page lists will be repurposed before memory on higher priority standby cache page lists. Typically, Standby memory is the aggregate of Standby Cache Core Bytes,Standby Cache Normal Priority Bytes, and Standby

			Cache Reserve Bytes. Standby Cache Core Bytes is the amount of physical memory, that is assigned to the core standby cache page lists. Standby Cache Normal Priority Bytes is the amount of physical memory, that is assigned to the normal priority standby cache page lists. Standby Cache Reserve Bytes is the amount of physical memory, that is assigned to the reserve standby cache page lists. **This measure will be available for Windows 2008 VMs only.**
	Cached memory: This measure is an aggregate of *Standby memory* and *Modified memory*.	MB	**This measure will be available for Windows 2008 VMs only.**

Note:

While monitoring Linux guest operating systems, you may observe discrepancies between the value of the *Physical memory utilized* measure and the memory usage percentages reported per process by the detailed diagnosis of the same measure. This is because, while the *Physical memory utilized* measure takes into account the memory in the OS cache of the Linux VM, the memory usage percent that the detailed diagnosis reports per process does not consider the OS cache memory.

2.5.13 Disk Alignment – VM Test

In a SAN environment, the smallest hardware unit used by a SAN storage array to build a LUN out of multiple physical disks is called a chunk or a stripe. To optimize I/O, chunks are usually much larger than sectors. Thus, a SCSI I/O request that intends to read a sector in reality reads one chunk.

On top of this, in a Windows environment, NTFS is formatted in blocks ranging from 1MB to 8MB. The file system used by the guest operating system optimizes I/O by grouping sectors into so called clusters (allocation units).

Figure 2.10 shows these three layers at issue. There are the SAN blocks at the bottom, then the VMFS blocks in the middle, and then the NTFS blocks used by the Windows VM.

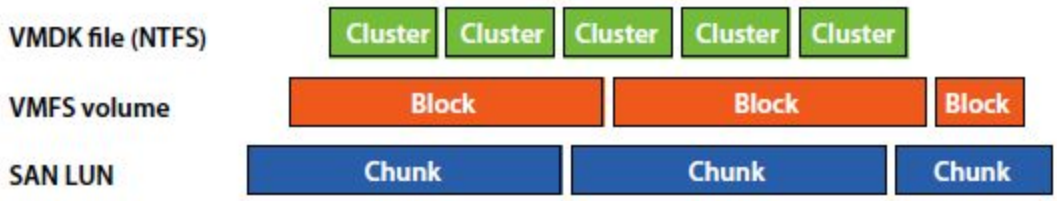


Figure 2.10: The SAN, VMFS, and NTFS blocks

If these three layers are not aligned, your SAN may be working harder than it needs to. For example, a call to read a single NTFS block may require the SAN to read three blocks as shown below:

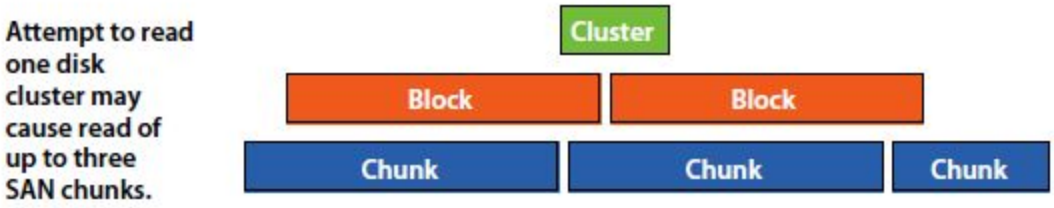


Figure 2.11: Unaligned partitions

An unaligned partition therefore, results in a track crossing and an additional I/O, incurring a penalty on latency and throughput. The additional I/O (especially if small) can impact system resources significantly on some host types.

What would hence be ideal is for the three layers in Figure 2.12 above to be aligned so that a single NTFS block requires only one SAN block to be read as illustrated below:

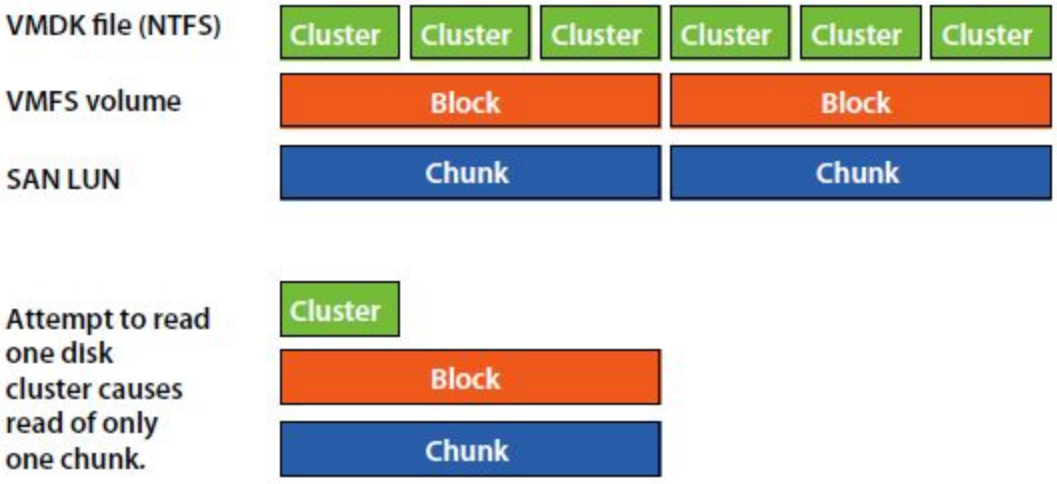


Figure 2.12: Aligned partitions

An aligned partition ensures that the single I/O is serviced by a single device, eliminating the additional I/O and resulting in overall performance improvement.

Therefore, whenever users to Windows VMs complaint that the VM is running slower than usual, you may want to check the disk alignment to determine whether the slowdown can be attributed to one/more unaligned disk partitions. This test enables you to perform such a check.

Target of the test : Oracle VM Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each disk partition on each Windows VM of the Oracle VM Server being monitored

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** – The port at which the **HOST** listens. By default, this is NULL. 4. **ORACLE VM MANAGER, ORACLE VM MANAGER USER, ORACLE VM MANAGER PASSWORD,** and **CONFIRM PASSWORD** – This test remotely connects to the Oracle VM Manager that manages the monitored Oracle VM Server and uses the web services API of the Oracle VM Manager to pull out metrics of interest. To enable this test to communicate with the web services API, you first need to configure the test with the IP address or host name of the Oracle VM Manager. This can be done using the **ORACLE VM MANAGER** text box. Then, you need to configure the test with the credentials of a user with Admin rights to the Oracle VM Manager. Use the **ORACLE VM MANAGER** user and **ORACLE VM MANAGER PASSWORD** parameters to configure these credentials. Finally, confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 5. **SSL** – By default, the Oracle VM Manager is SSL-enabled. Accordingly, the **SSL** flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Oracle VM Manager via HTTPS by default. 6. **WEBPORT** - By default,, the Oracle VM Manager listens on 7002. This implies that while monitoring an Oracle VM server via an SSL-enabled Oracle VM Manager, the eG agent, by default, connects to port 7002 of the Oracle VM Manager to pull out metrics. In some environments however, this default port may not apply. In such a case, against the **WEBPORT** parameter, you can specify the exact port at which the Oracle VM Manager in your environment listens so that the eG agent communicates with that port. 7. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comma-separated list of VMs to be excluded from monitoring in the exclude vms text box. Instead of VMs, VM name patterns can also be provided here in a comma-separated

list. For example, your exclude vms specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside and outside views of all VMs on a virtual host by default. By providing a comma-separated list of VMs/VM name patterns in the exclude vms text box, you can make sure the eG agent stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.

8. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Oracle environments might not have permissions to internally monitor one/more VMs. The eG agent can be configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the ignore vms inside view parameter. Against this parameter, you can provide a comma-separated list of VM names, or VM name patterns, for which the inside view need not be obtained. For instance, your ignore vms inside view specification can be: **xp,*lin*,win*,vista*. Here, the * (asterisk) is used to denote leading and trailing spaces (as the case may be). By default, this parameter is set to *none* indicating that the eG agent obtains the inside view of all VMs on an Oracle VM server by default.
   Note:
   While performing VM discovery, the eG agent will not discover the operating system of the VMs configured in the **IGNORE VMS INSIDE VIEW**text box.
9. **IGNORE WINNT** - By default, the eG agent does not support the *inside view* for VMs executing on **Windows NT** operating systems. Accordingly, the **IGNORE WINNT** flag is set to **Yes** by default.
10. **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:
    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 (Windows) on every Windows VM; this VM agent allows the eG agent to collect "inside view" metrics from the Windows VMs without domain administrator rights. 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.

- **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 do not belong to any domain (as in the case of Linux/Solaris guests)* : In this case, specify "none" in the *DOMAIN* field, and specify a local administrator account name in the *ADMIN USER* 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. Then, proceed to provide the password of the **ADMIN USER** against **ADMIN PASSWORD**, and confirm the password by retyping it in the **CONFIRM PASSWORD** text box.

  If key-based authentication is implemented between the eG agent and the SSH daemon of a Linux guest, then, in the admin user text box, enter the name of the user whose **<USER_HOME_DIR>** (on that Linux guest) contains a **.ssh** directory with the *public key file* named **authorized_keys**. The admin password in this case will be the *passphrase* of the *public key*; the default *public key file* that is bundled with the eG agent takes the password *eginnovations*. Specify this as the admin password if you are using the default private/public key pair that is bundled with the eG agent to implement key-based authentication. On the other hand, if you are generating a new public/private key pair for this purpose, then use the *passphrase* that you provide while generating the pair. For the detailed procedure on *Implementing Key-based Authentication* refer to the *Monitoring VMware Infrastructures* document.

- **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 PASSWORD**s 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.
- **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*.

12. **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 **DD FREQUENCY**.

13. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG 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 enable/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 abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Disk partition alignment status: Indicates whether this disk partition is aligned or not.		If the partition is unaligned, this test reports the value *Partition is not aligned*. For an aligned partition, this test reports the value *Partition is aligned*. The numeric values that correspond to the above- mentioned measure values are described in the table below: **Measure Value** / **Numeric Value** Partition is aligned — 100 Partition is not aligned — 0 **Note:** By default, this measure reports one of the **Measure Values** listed in the table above. The graph of this measure however will represent the disk alignment status using the numeric equivalents - 100 or 0. If a partition is found to be misaligned, you

			can use the detailed diagnosis of this test to figure out the caption, device ID, logical partition name, and block size of the faulty partition.

3

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 **Oracle VM 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.