Monitoring Nutanix Acropolis

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Nutanix solution is a converged storage and compute solution which leverages local components and creates a distributed platform for virtualization. The solution is a bundled hardware and software appliance which houses 2 or 4 nodes. Each node runs an industry-standard hypervisor - namely, VMware ESXi, Microsoft Hyper-V, or Acropolis Hypervisor (AHV). To provide total performance visibility into a Nutanix powered data center, monitoring of the Acropolis Hypervisor is necessary.

eG Enterprise v 6.2 provides comprehensive 'In-N-Out' monitoring, diagnosis and reporting for Nutanix Acropolis. All of the capabilities supported for other hypervisors such as VMware ESXi, Citrix XenServer and Microsoft Hyper-V are now supported for Nutanix Acropolis.

Both the server virtualization and desktop virtualization models of Acropolis can be monitored using eG.

This document discusses both these models and how eG Enterprise monitors them.

Chapter 2: How eG Enterprise Monitors Nutanix Acropolis?

eG Enterprise employs its tried, tested, and patented 'In-N-Out' monitoring approach to monitor the Nutanix Acropolis server.

Once a Nutanix Acropolis sxerver is managed, eG Enterprise starts to track the performance of the hypervisor and all the VMs hosted on it. REST API calls to the Acropolis hypervisor are used to track the performance and utilization of the hypervisor resources. VMs running on the hypervisor are auto-discovered and their relative resource usage patterns are tracked to identify resource consuming VMs (the outside view of the VMs). At the same time, the same eG monitor that monitors the hypervisors also connects to each of the VMs and obtains an inside view of each VM that highlights the applications/processes running in the VMs that are responsible for the resource usage.

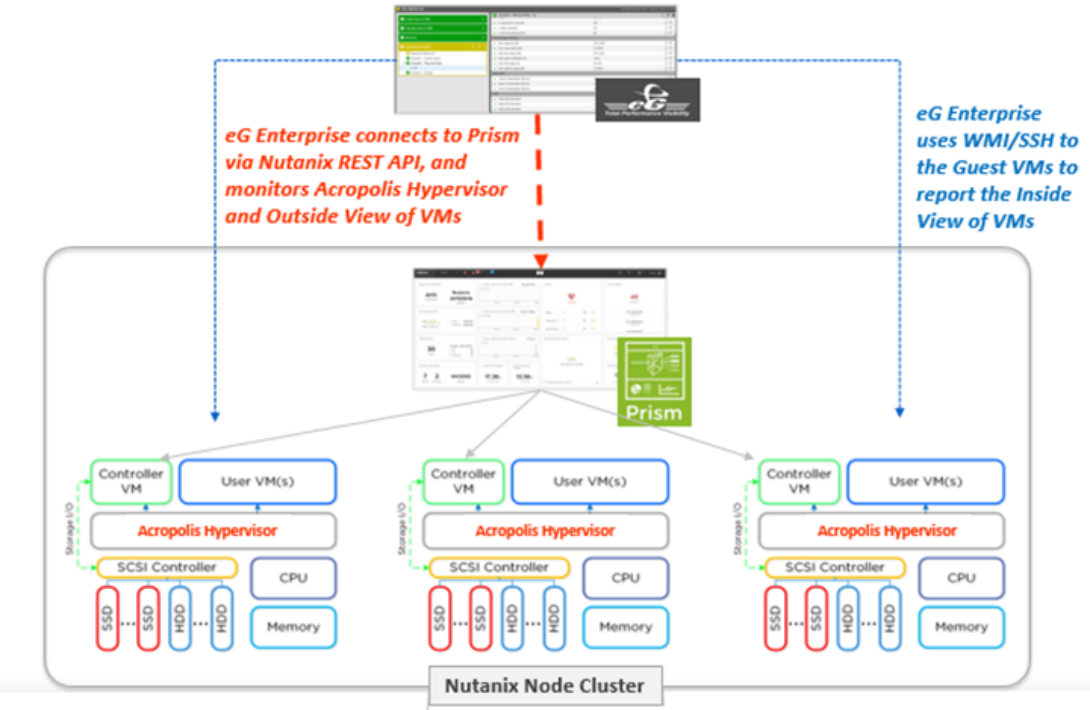


Figure 2.1: How eG Enterprise monitors Nutanix Acropolis

2.1 Pre-requisites for Monitoring Nutanix Acropolis Hypervisor

Before attempting to monitor a Nutanix Acropolis server, make sure the pre-requisites detailed here are fulfilled.

- General Pre-requisites
- Pre-requisites for Obtaining the 'Inside View' of VMs, using the eG VM Agent
- Pre-requisites for Obtaining the 'Inside View' of VMs, without using the eG VM Agent
- Pre-requisites for Monitoring Nutanix Acropolis Hypervisor

2.1.1 General Pre-requisites

- Enable the remote agent to communicate with the eG manager port (default: 7077).
- Ensure that the remote agent, if installed on a Windows host, runs using *domain administrator* privileges.
- Ensure that the remote agent has IP connectivity to the Nutanix Prism.
- Ensure that the remote agent has web access to the **WEBPORT** (port 9440, by default) configured for the Nutanix Prism.
- All the tests that the remote agent executes should be configured with the IP address of the Nutanix Prism, and the name and password of a user who is assigned a *Viewer* role on the Prism. It is recommended that you create a special user for this purpose on the Prism and assign the *Viewer* role to him/her. The steps for creating such a user are as follows:
  - Open a browser and connect to the Prism console using the URL: *http://<Prism_console_IP>:<Prism_Port>/console*. If the Prism is SSL-enabled, then the URL will be: *https://<Prism_console_IP>:<Prism_Port>/console*
  - Login to the console as a Cluster administrator or User administrator.
  - Figure 2.2 will then appear.

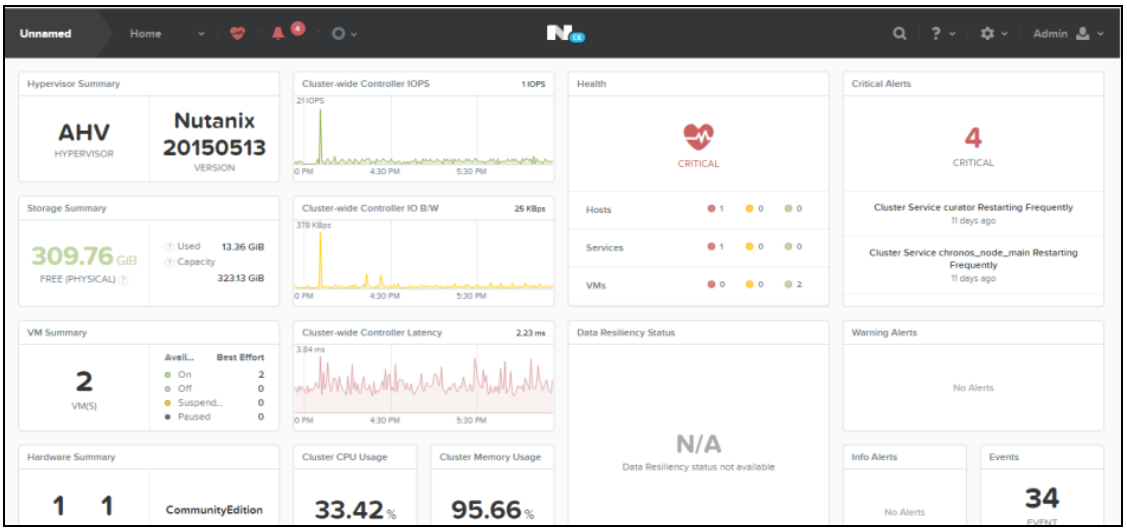


Figure 2.2: The Prism console

- In the console tool bar, click on the down-arrow next to the ⚙ tool to view the menu depicted by Figure 2.3. From the menu, choose the **User Management** option.

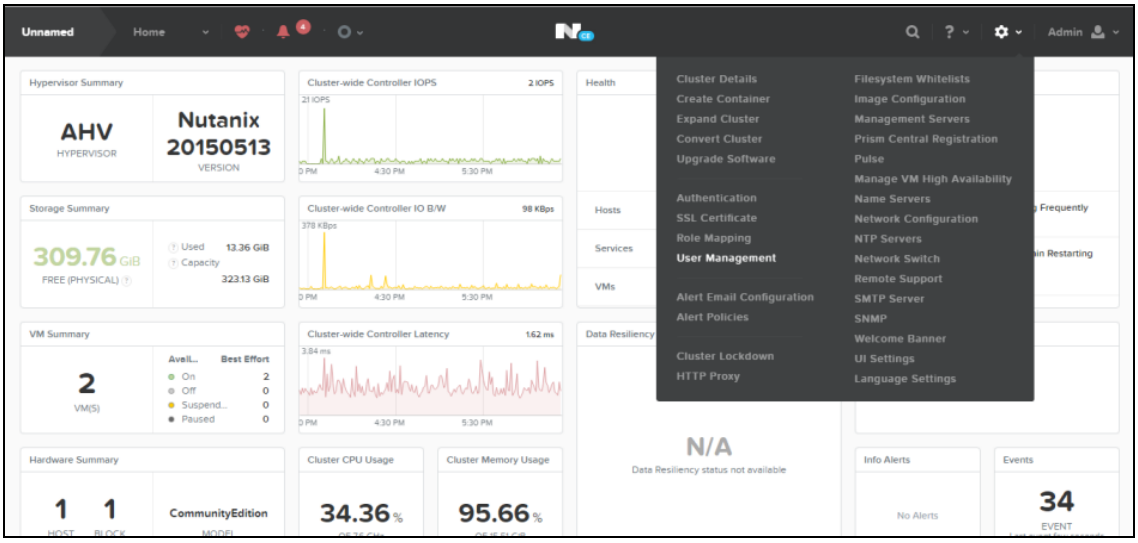


Figure 2.3: Choosing the User Management option

- Figure 2.4 will then appear. Click the **New User** button in Figure 2.4 to create a new user.

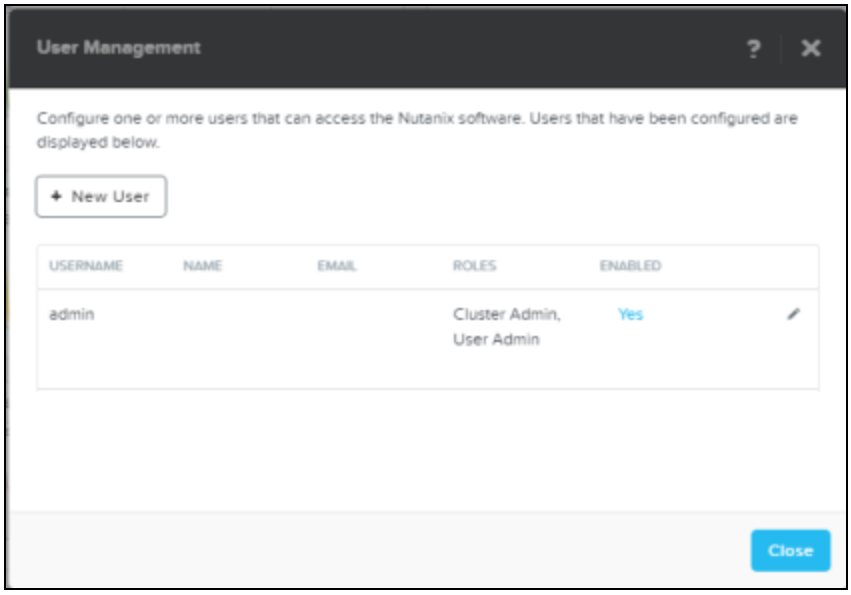


Figure 2.4: List of users who are already registered with Prism

- When Figure 2.5 appears, provide the details of the new user.

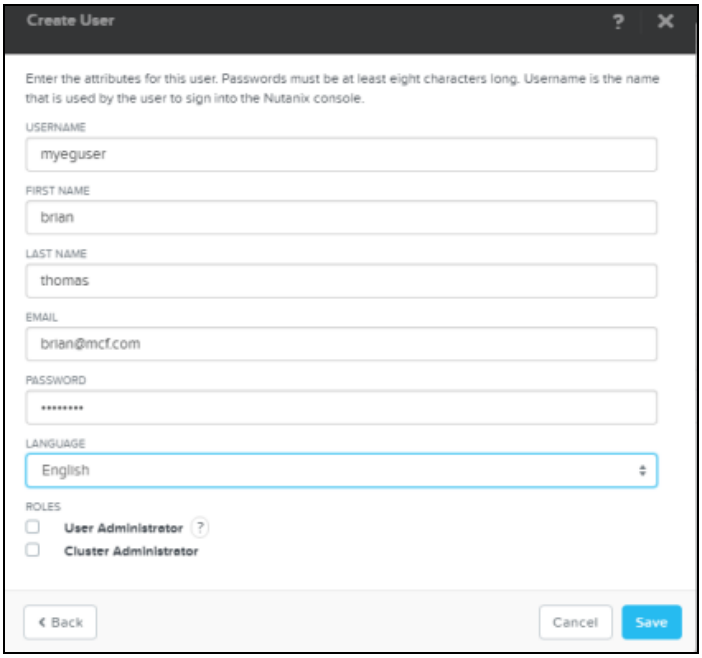


Figure 2.5: Providing the details of the new user

- When configuring the new user, make sure that the **User Administrator** and **Cluster Administrator** check boxes in Figure 2.5 are deselected. This is because, any user who is not assigned either of these roles will automatically assume the *Viewer* role.

- Finally, click the **Save** button in Figure 2.5 to save the changes.
- Figure 2.6 will then appear, wherein you can see that the new user has been successfully added, and that the Viewer role has been automatically assigned to this user.

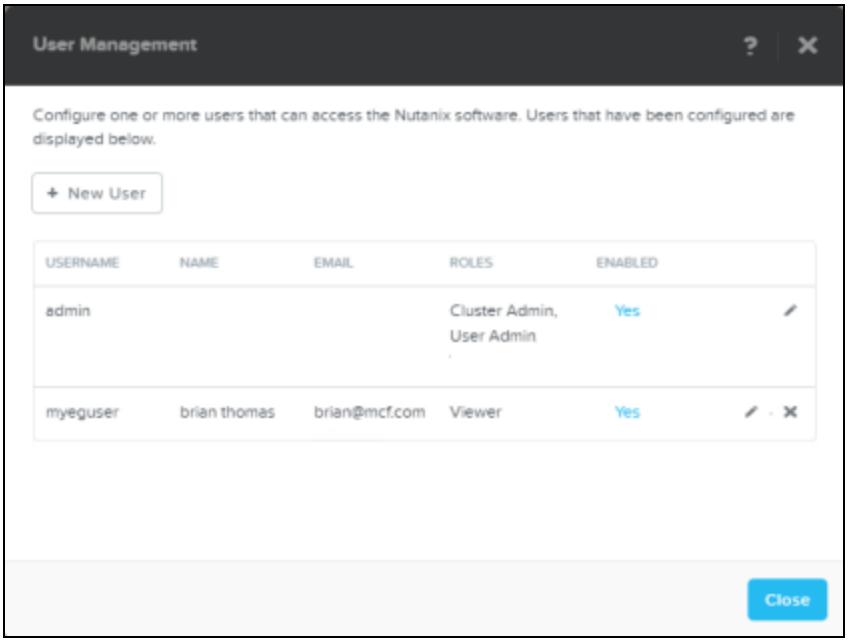


Figure 2.6: The new user's listing

- To monitor the Nutanix Acropolis server v5.5, the **JRE 1.8** should be available on the target server.

2.1.2 Pre- requisites for Obtaining the 'Inside View' of 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 the Section **2.3**, using the eG VM Agent topic.
- 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)**.

2.1.3 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$** share should be enabled for all Windows-based virtual guests being monitored and the administrative account must have permissions to this share drive. Refer to Enabling ADMIN$ Share Access on Windows Virtual Guests 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 operating systems, the firewall on the guest should be explicitly configured to allow Windows File and Print Sharing services.
- For monitoring a Windows VM, TCP port 139 must be accessible from the remote agent to the VM.
- 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:

  a. Login to the eG manager.
  b. Edit the **eg_tests.ini** file (in the **<EG_INSTALL_DIR>\manager\config** directory) on the eG manager host.
  c. 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*.
  d. 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*
  e. Finally, save the file.
- For obtaining the “inside view” of Windows VMs, the *eGurkhaAgent* service of the eG remote agent (on Windows) should be configured to run using *domain administrator* privileges. Refer to the Administering eG Enterprise document for the procedure.
- Set the **INSIDE VIEW USING** flag for all the “inside view” tests to **Remote connection to VM (Windows)**.

2.2 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 ESX 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 following pre-requisites need to be fulfilled:

a. The **ADMIN$** share will have to be available on the Windows guests

b. The Windows Firewall should be configured to allow Windows File and Print Sharing

The sections to come discuss the procedure to be followed for fulfiliing the 2 requirements above.

2.3 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**.

2.3.1 Installing the eG VM Agent

- Manually install the eG VM Agent on every Windows VM using the executable that eG Enterprise provides;

- 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;
- Connect to each Windows VM and silently install the eG VM Agent on it, without using the executable that eG Enterprise provides.

The first and fourth installation options alone are discussed here.

2.3.1.1 Using the Executable Provided by eG Enterprise

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 2.7 then appears. Click on the **Next** button in Figure 2.7 to continue.

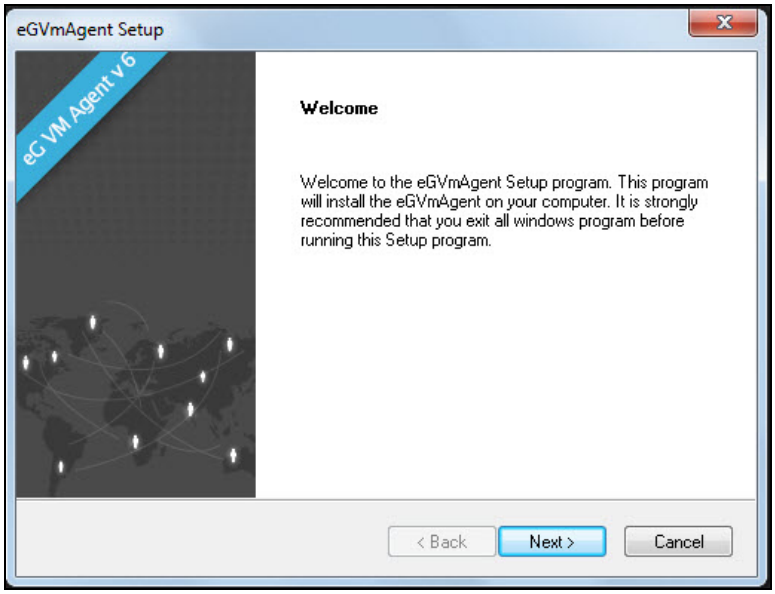


Figure 2.7: Welcome screen of the eG VM Agent installation wizard

3. When Figure 2.8 appears, click on **Yes** to accept the displayed license agreement.

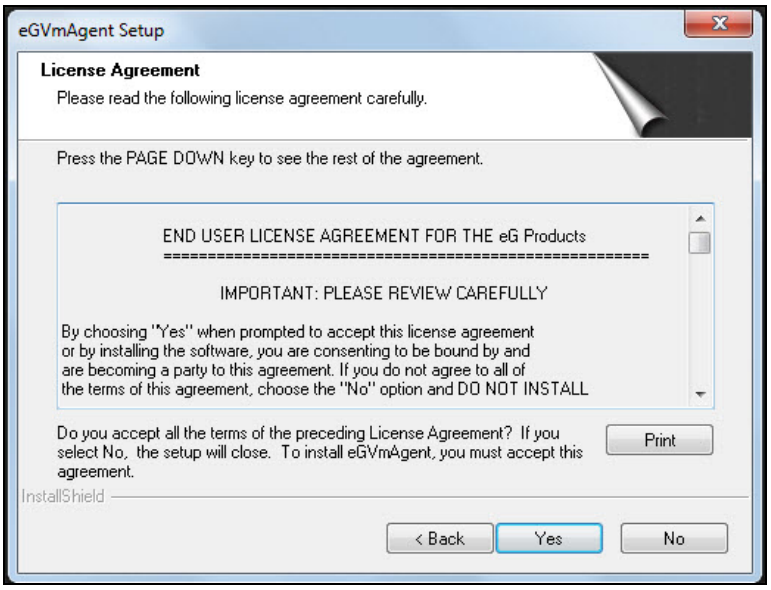


Figure 2.8: Accepting the license agreement

4. Use the **Browse** button in Figure 2.9 to indicate the location in which the agent should be installed, and click the **Next** button to proceed.

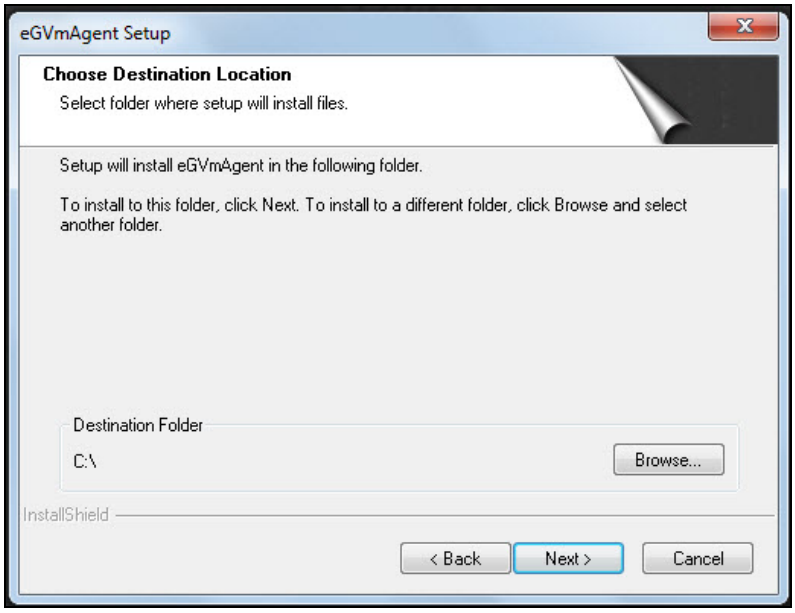


Figure 2.9: Specifying the install directory of the eG VM Agent

5. Next, specify the port at which the VM agent listens for requests from the eG agent. The default port is 60001. After port specification, click on the **Next** button in Figure 2.10 to proceed.

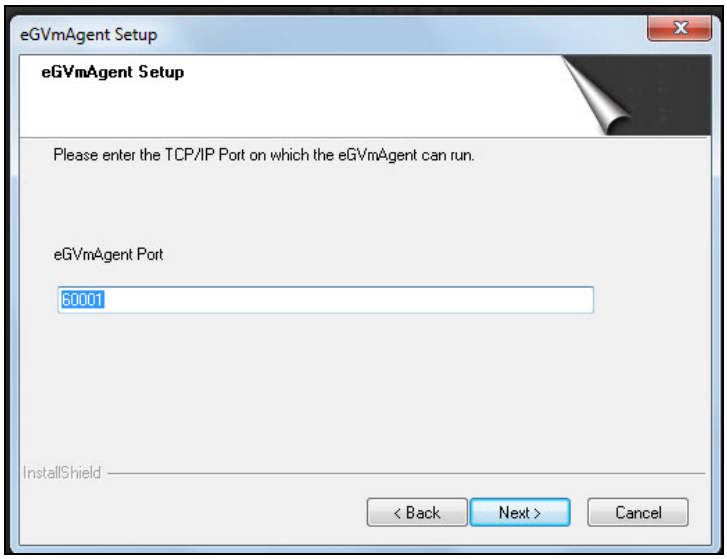


Figure 2.10: Specifying the VM agent port

6. A summary of your specifications then follows (see Figure 2.11). Click **Next** to proceed.

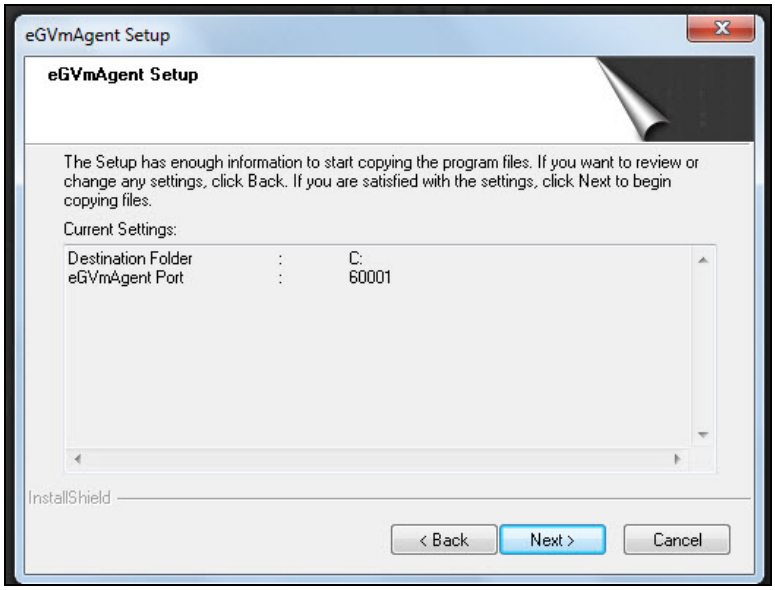


Figure 2.11: A summary of your specifications

7. Finally, click the **Finish** button in Figure 2.12 to complete the installation.

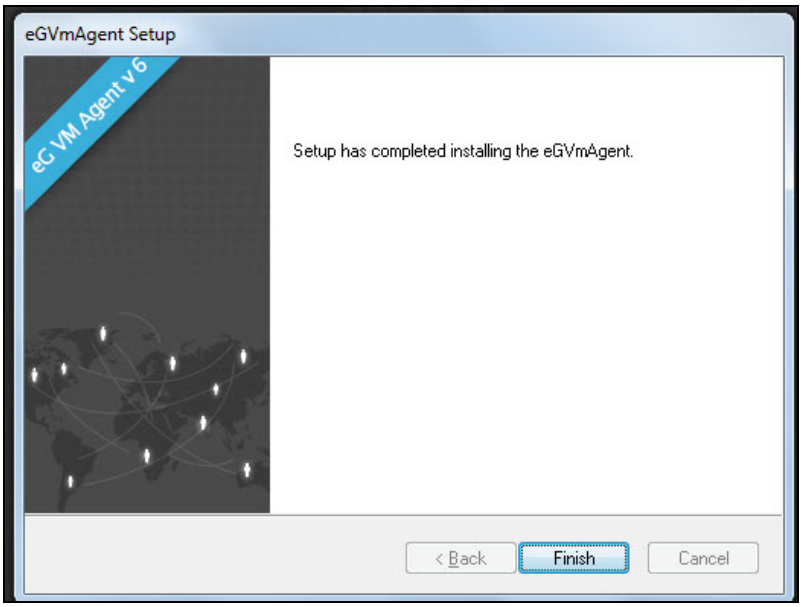


Figure 2.12: Finishing the installation

2.3.1.2 Silent Installation of the eG VM Agent

To silently install the eG VM agent on Windows VMs, follow the broad steps outlined below:

1. Creating silent mode script for eGVmagent installation
2. Installing eGVmAGent in silent mode

Each of these steps have been discussed elaborately below.

2.3.1.2.1 Creating a Silent Mode Script

For this, follow the procedure detailed below:

1. Login to a target Windows VM.
2. From the command prompt, run the following command to launch the normal mode installation of the eG VM Agent.

   *eGVMAgent_**<32/64>**.exe /a /r /f1**"<Full path to the script file into which the installation inputs will be stored>"***

   For example:

   eGVMAgent_x64.exe /a /r /f1"C:\script\eGVMAgent.iss"

3. Upon execution, this command will automatically create a script file of the given name in the location mentioned in the command.
4. Command execution will also begin the normal mode installation of the eG VM Agent. Provide inputs as and when necessary to proceed with the installation.
5. These inputs will be automatically recorded in the script file that was created in step 3.

2.3.1.2.2 Installing the eG VM Agent in the Silent Mode

Follow the steps given below to install the eG VM Agent in the silent mode:

1. Login to the Windows VM where the script file containing the inputs for installation resides.
2. Copy the script file from this VM to the Windows VM on which you want to install the eG VM Agent in the silent mode.
3. Copy the eG VM Agent installation executable also to the target Windows VM.
4. Next, on the target Windows VM, run the following command from the command prompt:

   *eGVMAgent_**<32/64>**.exe /a /s /f1"**<Full path to the script file containing the inputs for the installation>**"*

   For example:

   eGVmAgent_x64.exe /a /s /f1"C:\script\eGVMAgent.iss"

5. Upon successful execution, this command will automatically install the eG VM Agent on the target Windows VM.
6. You can then repeat steps 1-5 on each Windows VM where you want to install the eG VM Agent.

2.4 Configuring the eG Agent to Monitor NVIDIA Graphics Processing Units (GPUs)

Citrix XenServer employs the NVIDIA GRID Virtual GPU (vGPU) technology to provide exceptional graphics performance for virtual desktops. NVIDIA GRID vGPU enables multiple Virtual Machines (VM) to have simultaneous, direct access to a single physical GPU, using the same NVIDIA graphics drivers that are deployed on non-virtualized Operating Systems. Under the control of NVIDIA's GRID Virtual GPU Manager, which runs in XenServer's Control Domain (dom0), GRID physical

GPUs are capable of supporting multiple virtual GPU devices (vGPUs) that can be assigned directly to VMs.

To determine whether/not the vGPUs assigned to a VM are adequate for the graphic processing requirements of the that VM, administrators must understand whether/not memory-intensive I/O operations are performed on that VM and if so, how they impact vGPU usage. To perform this check, administrators can periodically run the **GPU – VM** test on every VM.

For this test to run and report metrics, the **NVWMI** must be installed on every VM.

NVIDIA WMI (NVWMI) is a graphics and display management and control technology that interfaces to Microsoft's Windows Management Instrumentation infrastructure, specific to NVIDIA graphics processing units (GPUs). This allows scripts and programs to be created that configure specific GPU related settings, perform automated tasks, retrieve and display a range of information related to the GPU as well as many other administrative tasks and functions.

The following NVIDIA products support NVWMI:

- NVIDIA Quadro K600
- Quadro K6000
- Quadro K5000
- Quadro K4000
- Quadro K2000D
- Quadro K2000
- Quadro FX 5800
- Quadro FX 580
- Quadro FX 570
- Quadro FX 5600
- Quadro FX 4800
- Quadro FX 4700 X2
- Quadro FX 4600
- Quadro FX 380 Low Profile
- Quadro FX 3800
- Quadro FX 380
- Quadro FX 3700
- Quadro FX 370

- Quadro FX 3450
- Quadro FX 1800
- Quadro FX 1700
- Quadro CX
- Quadro 7000
- Quadro 6000
- Quadro 600
- Quadro 5000
- Quadro 410
- Quadro 4000 for Mac
- Quadro 4000
- Quadro 400
- Quadro 2000D
- Quadro 2000
- NVIDIA NVS 510
- NVS 450
- NVS 420
- NVS 315
- NVS 310
- NVS 300
- NVS 295
- NVS 290
- Quadro Plex S Series
- Quadro Plex Model IV
- Quadro Plex D Series
- Quadro Plex 7000

NVWMI can be installed in the following three ways:

- When the NVIDIA GPU driver is installed
- Via a standalone install
- Via command line install

Note:

NVWMI is only supported on Windows 7 and later operating systems.

Each of these installation options are detailed in the sub-sections.

Chapter 3: Configuring eG Enterprise to Monitor Nutanix Acropolis

This topic details the steps for administering the eG manager to monitor a Nutanix Acropolis server. The broad steps to achieve this are as follows:

- Discovering the Nutanix Acropolis servers using the Nutanix Prism
- Managing the discovered Nutanix Acropolis server
- Configuring the tests for the Nutanix Acropolis server

3.1 Discovering Nutanix Acropolis

The eG manager is capable of automatically discovering the Nutanix environment via the Nutanix Prism. To configure this discovery, do the following:

1. Login to the eG administrative interface.
2. Follow the Components -> Discovery menu sequence in the Admin tile menu.
3. In the **DISCOVERY** tree that appears next, expand the **Setting**s sub-node of the **Manager Discovery** node, and select the **Virtual Platforms** node within. The right panel will then change to display the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page.

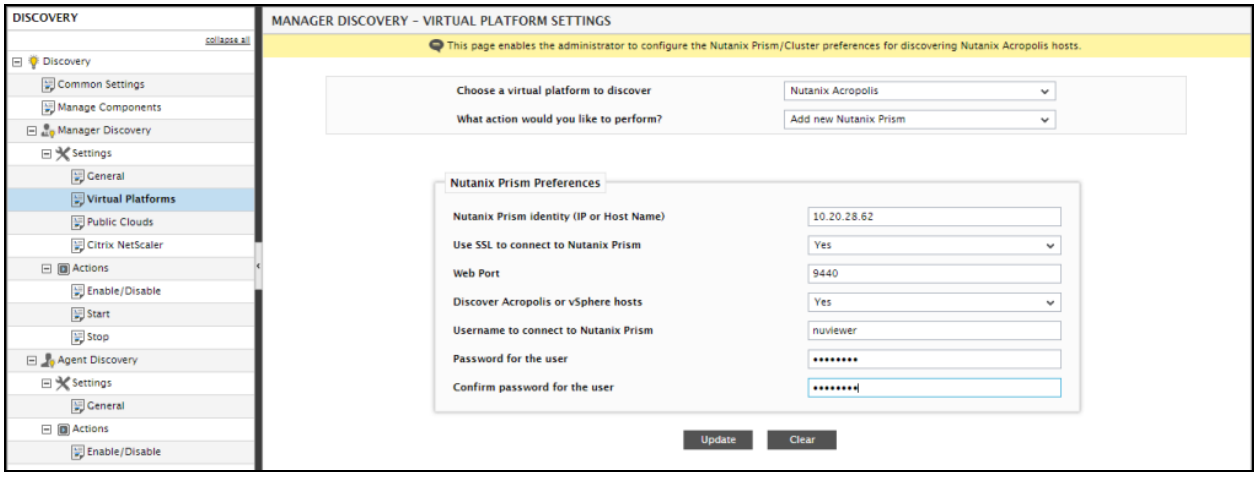


Figure 3.1: Adding a Nutanix Prism for discovery

4. To discover a Nutanix Acropolis server / VDI server, from the **Choose a virtual platform to discove**r drop-down, select *Nutanix Acropolis* or *Nutanix Acropolis VDI* (as the case may be).
5. If the Nutanix Acropolis server has to be discovered using a new Nutanix Prism, you will first need to add the Nutanix Prism to the eG Enterprise system. For that, select the *Add new Nutanix Prism* option from the **What action would you like to perform?** drop-down.
6. Then, specify the following in the **Nutanix Prism Preferences** section:
   - In the **Nutanix Prism Identity** text box, specify the IP or hostname of the Nutanix Prism that you want to use for discovery.
   - If the Prism being added is SSL-enabled, then set the **SSL** flag to *Yes*.
   - Then, enter the **Web Port** at which the Prism listens. By default, this is *9440*.
   - The eG manager can discover vSphere, Hyper-V, and Acropolis hosts using the Nutanix Prism. In addition, you can also use the Nutanix Prism to monitor the performance of the Acropolis hosts (not Hyper-V or vSphere hosts) and the VMs operating on it. If you want to use the Prism being added to only discover hypervisors (vSphere, Hyper-V, and Acropolis), then set the **Discover hypervisors** flag to **Yes**. On the other hand, if you do not want to use the Prism for discovery, but may want to use it for monitoring an Acropolis server later, then set this flag to **No**.
   - In order to perform the discovery/monitoring, the eG manager should connect to the Prism as a user who is assigned the *Viewer* role. Provide the credentials of this user in the **Username to connect to Nutanix Prism** and **Password for the user** text boxes. Confirm this password by retyping it in the **Confirm password for the user** text box.
   - Finally, click the **Update** button to save the changes. If the **Discover hypervisors** flag above is set to **Yes,** then clicking on **Update** will instantly trigger discovery.

Note:

Once discovery is triggered, all the Nutanix Acropolis servers that are managed by the Nutanix Prism will be discovered as both *Nutanix Acropolis* and *Nutanix Acropolis VDI* servers in eG.

3.2 Managing the Nutanix Acropolis Server

Nutanix Acropolis and Acropolis VDI servers that are auto-discovered using the Nutanix Prism can be managed with the help of the MANAGE/UNMANAGE page in the eG admin interface. Servers that are not auto-discovered can be manually added using the ADD/MODIFY page in the eG admin interface. This topic discusses both these procedures.

To manage an auto-discovered Acropolis server, do the following:

1. Follow the Components -> Manage/Unmanage menu sequence in the Infrastructure tile of the Admin menu.
2. When Figure 1 appears, select *Nutanix Acropolis* as the **Component type**. All Acropolis servers that were recently discovered will be displayed in the **Unmanaged Components** list. **Note that to view and manage Acropolis VDI servers, you will have to select 'Nutanix Acropolis VDI' as the Component type.**

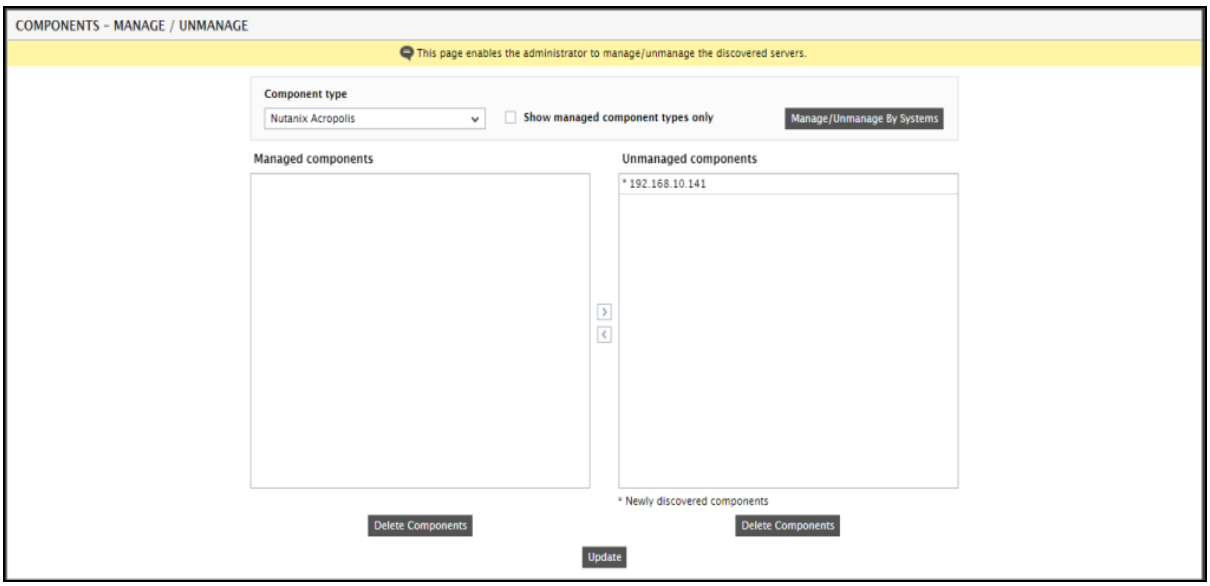


Figure 3.2: Viewing the discovered Acropolis servers

3. Select the server you want to manage from the **Unmanaged Components** list and click the **<** button to manage it. This will transfer your selection to the **Managed Components** list (see Figure 2).

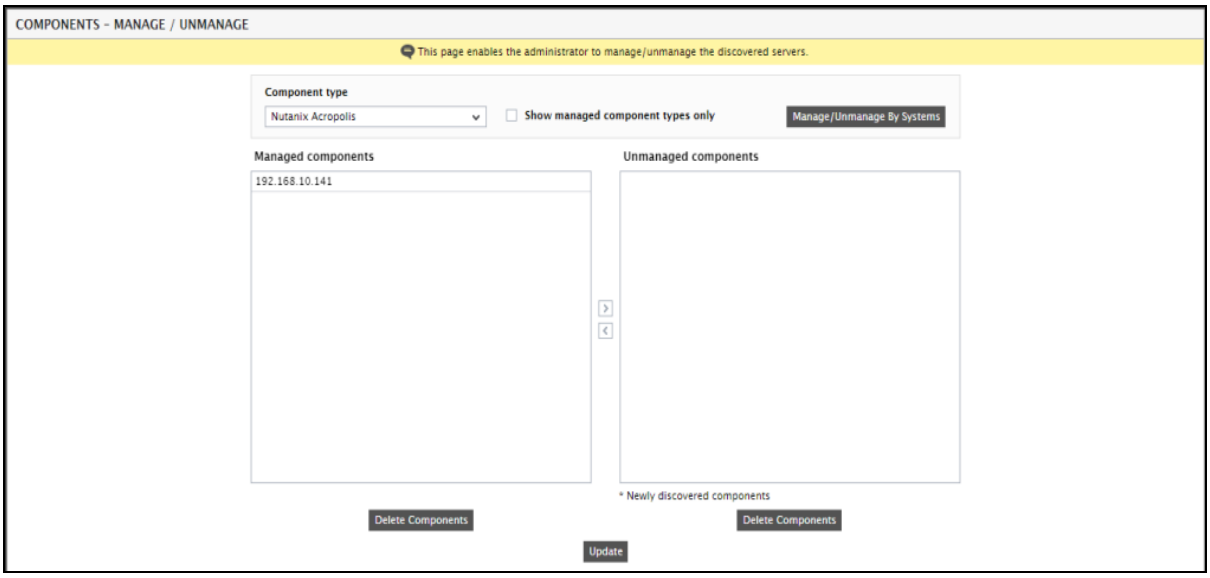


Figure 3.3: Managing the Acropolis server

4. Finally, click the **Update** button in Figure 2 to save the changes.

To manage an Acropolis server that is not auto-discovered, do the following:

1. Follow the Components -> Add/Modify menu sequence in the Infrastructure tile of the Admin menu.
2. In the page that appears next, select *Nutanix Acropolis* as the **Component type**. **Note that to add an Acropolis VDI server, you will have to select 'Nutanix Acropolis VDI' as the Component type**. Then, click the Add New Component button. This will invoke Figure 3.

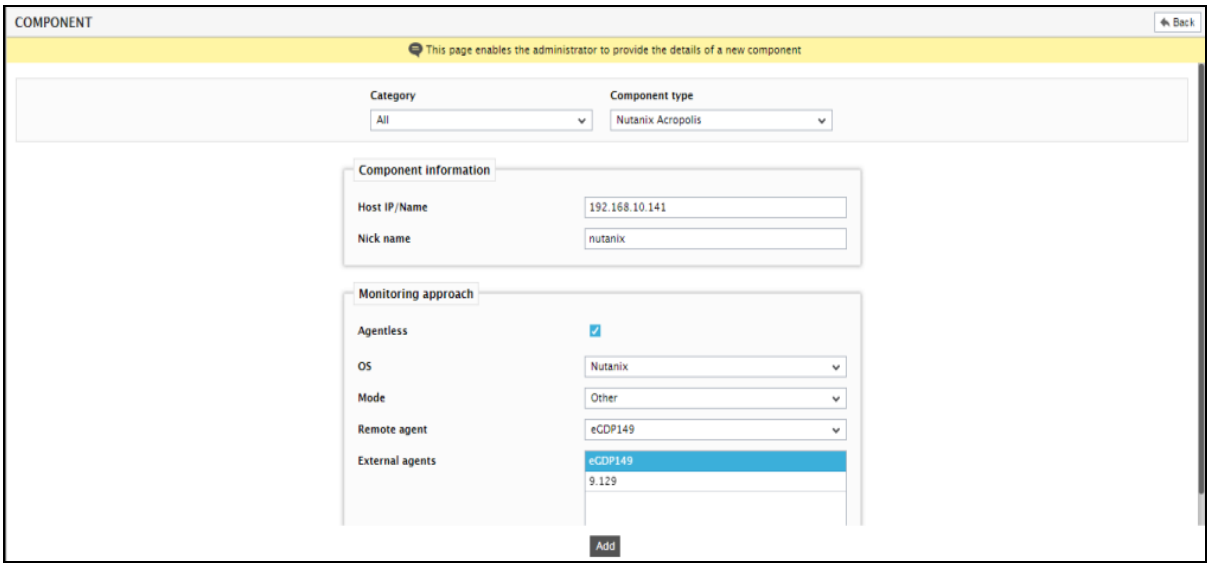


Figure 3.4: Manually adding a Nutanix Acropolis server

3. Specify the following in Figure 3:

- Provide the **Host IP/Name** of the Acropolis server to be monitored.
- Specify the **Nickname** of the server.
- By default, eG monitors Nutanix Acropolis in an agentless manner only. This is why, the **Agentless** flag is enabled by default.
- Select *Nutanix* as the **OS** and then indicate the **Mode** of monitoring. The eG agent runs Rest API commands on Prism to pull metrics from the Acropolis server. Therefore, select *Other* as the **Mode**.
- Pick the **Remote Agent** that should monitor the server**.**
- Also assign an **External Agent** for external monitoring of the server.
- Click the **Update** button to save the changes.

3.3 Configuring Tests for the Nutanix Acropolis Server

Once the Acropolis server is managed in eG, sign out of the eG administrative interface. When doing so, you will be prompted to manually configure the tests associated with the Acropolis server.

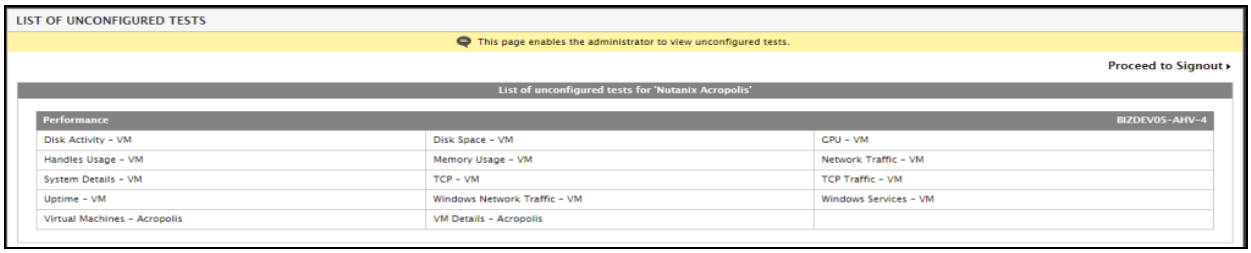


Figure 3.5: The list of unconfigured tests for the Acropolis server

Click on any test to configure it. Say, you click on the Disk Activity - VM test to configure it. Figure 2 will then appear.

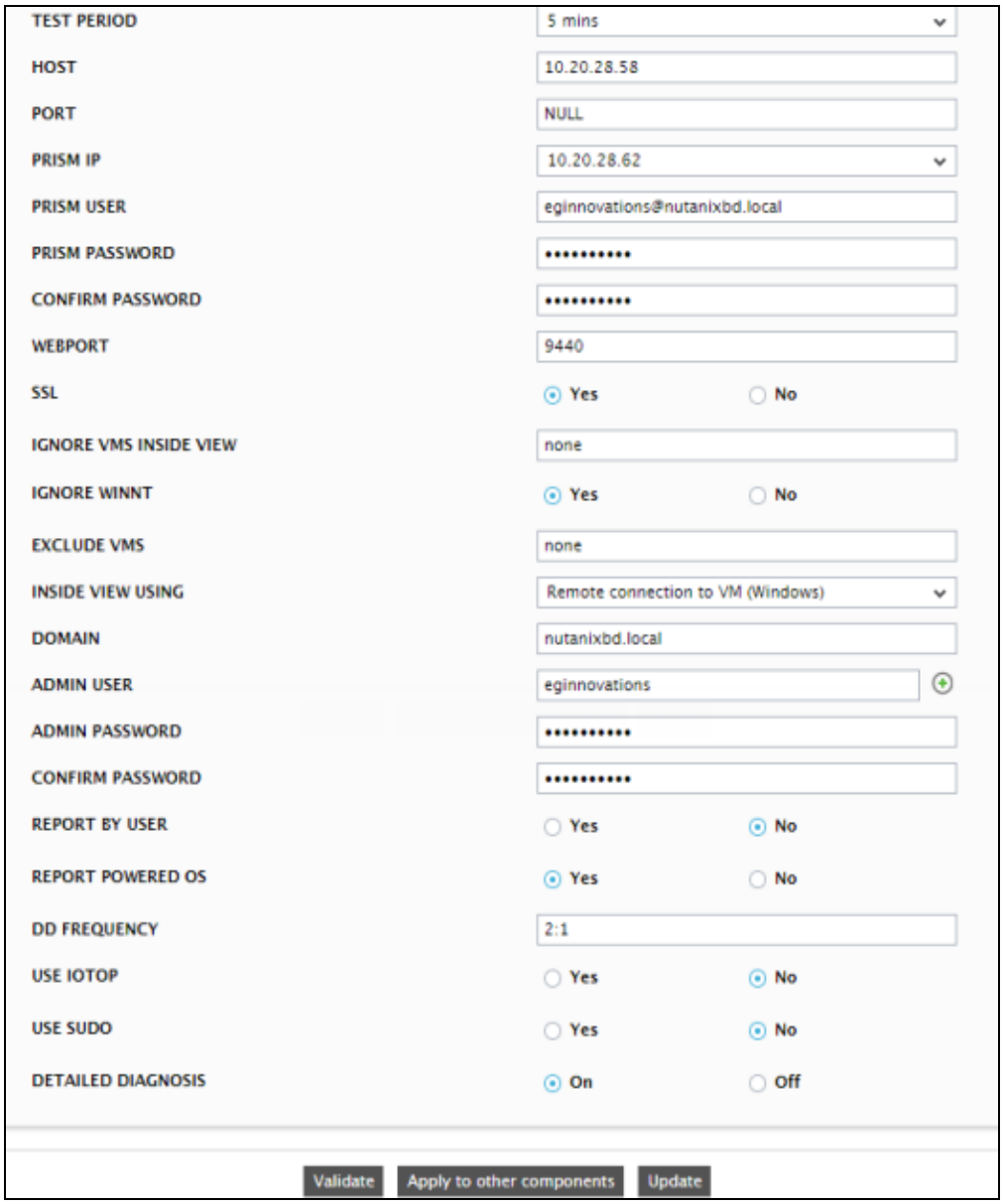


Figure 3.6: Configuring the Disk Activity - VM test

To know how to configure this test, refer to the Disk Activity - VM Test topic.

Finally, click the Update button to save the test configuration. Configuring a single test will automatically configure all other Acropolis tests. You can now sign out of the eG administrative interface, and then log into the eG monitor interface to view the layer model of the Nutanix Acropolis server and the performance metrics reported by the tests mapped to each layer. For details regarding the same, refer to the Monitoring the Nutanix Acropolis Server topic.

Chapter 4: Monitoring the Nutanix Acropolis Server

eG Enterprise provides a specialized model for monitoring Nutanix Acropolis servers with VMs that host server applications.

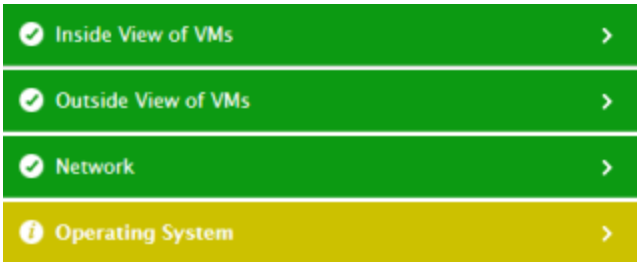


Figure 4.1: Layer model of the Nutanix Acropolis server

Each layer of this model is mapped to tests that report on the resource usage of the hypervisor and the VMs inside-out, and point you to resource-hungry VMs and applications. Using the metrics reported by this model, administrators can find quick and accurate answers to the following performance queries:

- Is the Acropolis server available over the network? If so, how responsive is the server to requests?
- Is the content cache sized enough to handle requests, or are cache hits very low?
- How much memory did deduplication save in the content cache?
- Are any physical disks marked for removal? Has data from that disk been migrated?
- Which physical disk is currently offline?
- Is any physical disk being over-utilized?
- Are there any latent physical disks?
- How is the I/O performance of the physical disks?
- Is I/O load balanced across all physical disks?
- Is any physical disk consuming bandwidth excessively when processing I/O?
- How is the I/O load on the storage?
- Is the storage processing I/O requests quickly?
- Is too much bandwidth being consumed when processing I/O?

- Is the AHV sized with adequate storage resources? If not, what type of storage is running short of space - the SSDs? or the SATA HDDs?
- How many VMs are operating on the Acropolis server? What is their IP address and which OS are they running?
- Which VMs are currently powered off or suspended?
- Which VMs have been newly added and which ones were recently removed from the server?
- Which VM is the CVM of a cluster?
- Is any VM consuming the physical CPU, memory, network, and I/O resources of the Acropolis server, abnormally?
- Which VM is utilizing the CPU, memory, network, and I/O resources allocated to it, excessively? Which process on the VM is causing this abnormal resource consumption?

This chapter will discuss each layer of Figure 1 in great detail.

4.1 The Operating System Layer

Using the tests mapped to this layer, you can determine whether/not the server is sized with sufficient CPU, memory, and storage resources to handle the I/O load on the server.

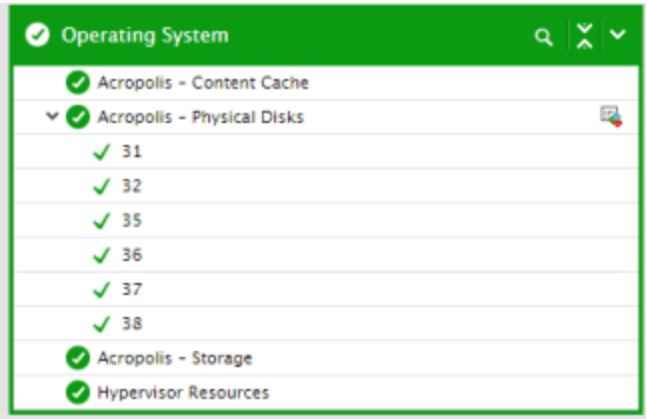


Figure 4.2: The tests mapped to the Operating System layer

4.1.1 Acropolis - Content Cache Test

The Content Cache (aka “Elastic Dedupe Engine”) is a deduped read cache which spans both the CVM’s memory and SSD. Upon a read request of data not in the cache (or based upon a particular fingerprint) the data will be placed in to the single-touch pool of the content cache which completely sits in memory where it will use LRU until it is ejected from the cache. Any subsequent read request

will “move” (no data is actually moved, just cache metadata) the data into the memory portion of the multi-touch pool which consists of both memory and SSD. From here there are two LRU cycles, one for the in-memory piece upon which eviction will move the data to the SSD section of the multi-touch pool where a new LRU counter is assigned. Any read request for data in the multi-touch pool will cause the data to go to the peak of the multi-touch pool where it will be given a new LRU counter.

Figure 4.3 below provides a high-level overview of the content cache:

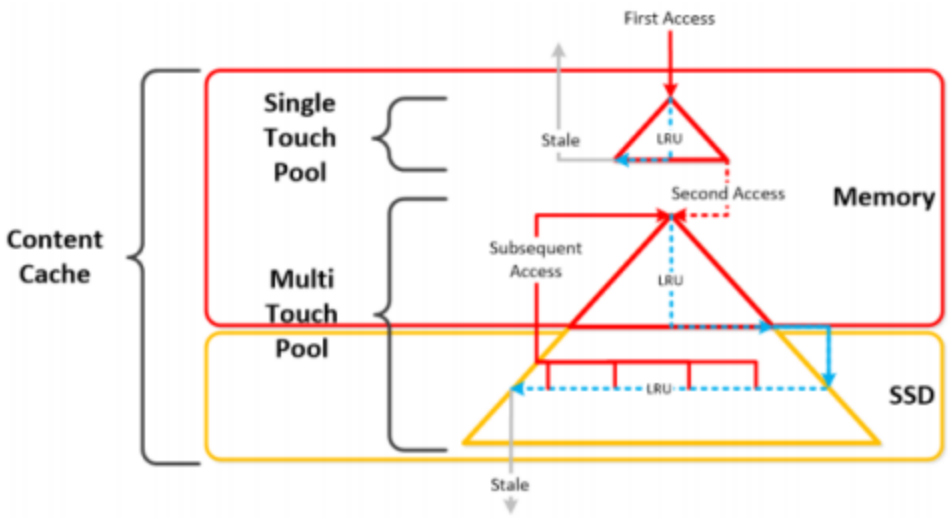


Figure 4.3: A high-level overview of the content cache

If the content cache is not sized right, then the cache will not be able to hold frequently accessed data, and will hence be unable to service many read requests. This could increase direct disk accesses and related overheads, thereby degrading overall storage performance. To ensure peak storage performance therefore, the usage of the cache should be continuously monitored, cache misses should be promptly captured, and the reasons for the same should be diagnosed. This is exactly what the Acropolis - Content Cache test helps perform.

This test closely monitors the content cache, tracks the cache hit ratio, and alerts administrators if the ratio dips below acceptable limits. In addition, the test also monitors how the cache memory is utilized in the single-touch and multi-touch pools, thus pointing administrators to sizing deficiencies that could be contributing to the high rate of cache misses (if any). Using the pointers provided by this test, administrators can right size the cache and improve cache and overall storage efficiency.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Section **Chapter 3** topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.
   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the

list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Section **Chapter 3** topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Cache hits:	Indicates the number of times read requests were served from this cache during the last measurement period.	Number	Ideally, the value of this measure should be close to or equal to the value of the *Cache lookups* measure.
Cache hit ratio:	Indicates the ratio of cache hits to cache lookups.	Percent	Ideally, the value of this measure should be over 80%. If so, then it indicates that almost all read requests were served by the cache. This means that direct disk accesses and related processing overheads were minimal. A value less than 50% signifies ineffective cache usage. In other words, most of the cache lookups did not result in cache hits. One of

Measurement	Description	Measurement Unit	Interpretation
			the key reasons for this could be poor cache size. If the cache does not have enough memory resources to hold data, it may not be able to service read requests. This will increase direct disk accesses, which are I/O-intensive operations.
Physical memory usage:	Indicates the amount of real memory that is consumed by the data in the content cache.	MB	A consistent increase in the value of this measure could mean that cache misses are high, owing to which new data is being continuously written to the cache. In the process, more memory is being consumed.
Cache lookups:	Indicates the number of times the cache was looked up for serving read requests during the last measurement period.	Number	
Saved memory usage:	Indicates the amount of content cache memory saved due to deduplication.	MB	Performance tier deduplication removes duplicate data in the content cache (SSD and memory) to reduce the footprint of an application's working set. This enables more working data to be managed in the content cache. Therefore, higher the value of this measure, more significant will be the performance improvements.
Logical SSD usage:	Indicates the logical SSD memory used to cache data without deduplication.	MB	
Logical memory	Indicates the logical	MB	

Measurement	Description	Measurement Unit	Interpretation
usage:	memory used to cache data without deduplication.		
SSD usage:	Indicates the real SSD memory used to cache data.	MB	If data in the single-touch pool of the content cache is accessed, it is moved to the in-memory portion of the multi-touch pool. Here again, it follows an LRU cycle, based on which the 'oldest objects'in memory are identified and moved to the SSD portion of the multi-touch pool. If the data in SSD is accessed, it is moved to the top of the multi-touch pool, from where it will be served. Any increase in the usage of the SSD portion of the multi-touch pool can be attributed to the addition of data that is not- so- frequently accessed. If the SSD is not sized right, then data will be discarded from the pool sooner than desired. In the absence of enough data, cache misses will increase, and so will the overheads of direct disk accesses.
SSD usage saved:	Indicates the memory saved in SSD owing to deduplication.	MB	Performance tier deduplication removes duplicate data in the content cache (SSD and memory) to reduce the footprint of an application's working set. This enables more working data to be managed in the content cache. Therefore, higher the value of this measure, more significant will be the performance improvements.

4.1.2 Acropolis - Physical Disks Test

Monitoring each physical disk grouped in a storage pool provides administrators with insights into the status, configuration, and usage of each disk. This in turn enables administrators to isolate disks that are running out of free space and those that are experiencing serious processing bottlenecks, so that such disks can be marked for resizing or tuning. Using the **Acropolis - Physical Disks** test, administrators can receive such useful physical disk-level performance insights!

For each physical disk, this test reports the current status, type, and mode of the test. In addition, the test measures the space usage and I/O processing ability of each disk, and warns administrators of a probable space contention, a potential overload, or a possible processing snag on a disk. This way, the test enables administrators to ensure high disk performance and availability.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each physical disk of the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list,

then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

10. **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	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this disk.		The values that this measure can report, their description, and their corresponding numeric values are detailed in the table below: Measure Value / Description / Numeric Value Detachable / Disk is not being used and can be removed. / 0 Normal / Disk is operating normally. / 1 Data migration initiated / Data is being migrated to other disks. / 2 Marked for removal / Data migration is in progress / 3 **Note:**

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>By default, this measure reports the Measure Values listed in the table above to indicate disk status. In the graph of this measure however, status is represented using the numeric equivalents only.

Use the detailed diagnosis of the Status measure to view the UUID of the disk and the cluster to which it is attached.</td></tr>
<tr><td>Disk type</td><td>Indicates the disk type.</td><td></td><td>The values that this measure can report and their corresponding numeric values are detailed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>SSD</td><td>0</td></tr><tr><td>HDD</td><td>1</td></tr></table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate the disk type. In the graph of this measure however, the disk type is represented using the numeric equivalents only.

Use the detailed diagnosis of the Status measure to view the UUID of the disk and the cluster to which it is attached.</td></tr>
<tr><td>Mode</td><td>Indicates whether the disk is currently online or offline.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Offline</td><td>0</td></tr><tr><td>Online</td><td>1</td></tr></table>Note:
By default, this measure reports the Measure Values listed in the table above to indicate the disk mode. In the graph of this measure however, the mode is indicated using the numeric equivalents only.</td></tr>
<tr><td>Is marked for removal?</td><td>Indicates whether/not the disk is ready to be removed.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Off</td><td>0</td></tr><tr><td>On</td><td>1</td></tr></table>Note:
By default, this measure reports the Measure Values listed in the table above to indicate whether/not the disk is ready to be removed. In the graph of this measure however, the same is indicated using the numeric equivalents only.</td></tr>
<tr><td>Is data migrated?</td><td>Indicates whether/not the data in this disk is migrated.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>No</td><td>0</td></tr>
<tr><td>Yes</td><td>1</td></tr>
</table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate whether/not the data is migrated. In the graph of this measure however, the same is indicated using the numeric equivalents only.
</td></tr>
<tr><td>Is self encrypting drive?</td><td>Indicates whether/not this is a self-encrypting drive.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:

<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>No</td><td>0</td></tr>
<tr><td>Yes</td><td>1</td></tr>
</table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate whether/not the disk is a self-encrypting drive. In the graph of this measure however, the same is indicated using the numeric equivalents only.
</td></tr>
<tr><td>Disk capacity</td><td>Indicates the total capacity of this disk.</td><td>GB</td><td></td></tr>
<tr><td>Disk used space</td><td>Indicates the amount of space in this disk that is currently in use.</td><td>GB</td><td>A low value is desired for this measure.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Disk free space	Indicates the amount of space in this disk that is still unused.	GB	A high value is desired for this measure.
Disk space utilization	Indicates the percentage of disk capacity that is being utilized.	Percent	A value close to 100% indicates that the disk is rapidly running out of space.
Percent free space in disk	Indicates of percentage of disk capacity that is free and is available for use.	Percent	A value less than 50% indicates that the disk is rapidly running out of space.
Disk logical usage	Indicates the amount of logical storage space in this disk that is in use currently.	GB	
Total I/O latency	Indicates the average time taken by this disk to process I/O requests.	Secs	Ideally, the value of this measure should be very low. A high value or a steady increase in this value could indicate an I/O processing bottleneck on this disk. In such a case, compare the value of the *Read IO latency* and *Write IO latency* measures to figure out when the slowness is worst - when processing read requests? or write requests?
Read IO latency	Indicates the average time taken by this disk to process read I/O requests.	Secs	If the *Total I/O latency* measure reports an abnormally high value, then compare the value of these measures to figure out where the slowness is maximum - when processing read requests? or write requests?

Measurement	Description	Measurement Unit	Interpretation
Write IO latency	Indicates the average time taken by this disk to process write I/O requests.	Secs	
Total IO bandwidth	Indicates the bandwidth per second used by this disk when processing I/O requests.	KB/Sec	A high value for this measure denotes that this disk is processing bandwidth-intensive I/O. In such situations, you may want to compare the value of the *Read IO bandwidth* and *Write IO bandwidth* measures to know what type of I/O requests are truly contributing to the excessive bandwidth consumptions - read requests? or write requests?
Read IO bandwidth	Indicates the bandwidth per second used by this disk when processing read I/O requests.	KB/Sec	If the value of the *Total IO bandwidth* measure is high, then you may want to compare the value of the *Read IO bandwidth* and *Write IO bandwidth* measures to know what type of I/O requests are truly contributing to the excessive bandwidth consumption - read requests? or write requests?
Write IO bandwidth	Indicates the bandwidth per second used by this disk when processing write I/O requests.	KB/Sec	
Total IOPS	Indicates the number of I/O operations performed currently on this disk.	Number	This measure is a good indicator of the level of I/O activity on the Nutanix storage. A steady and significant increase in the value of this measure could indicate a potential I/O overload. In such situations, you may want to compare the value of the *Read IOPS* and *Write IOPS* measures to know what type of IO operations are contributing to the overload.

Measurement	Description	Measurement Unit	Interpretation
Read IOPS	Indicates the number of read I/O operations performed currently on this disk.	Number	If the value of the *Total IOPS* measure is unusually high, then compare the value of these measures to know what is contributing to the unusual I/O activity levels - read requests? or write requests?
Write IOPS	Indicates the number of write I/O operations performed currently on the container.	Number	

Use the detailed diagnosis of the *Status* measure to view the UUID of the disk and the cluster to which it is attached.

Details of Disk

DISK ID	STORAGEPOOL UUID	CLUSTER UUID
Sep 21, 2016 17:54:50		
43	c98e4eee-8d23-4378-b85a-e251ccee9290	000529b7-ca39-ffa0-0000-00000000a45c

Figure 4.4: The detailed diagnosis of the Status measure

4.1.3 Acropolis - Storage Test

Nutanix combines compute (CPU) resources with storage resources delivered via SSDs and directly-attached (DAS) SATA HDD media drives. The VMs operating on the Nutanix Acropolis hypervisor use these aggregated storage resources for their operations. The lack of adequate, well-tuned storage resources can therefore severely impair VM operations and availability. To avoid this, a Nutanix administrator has to continuously measure overall storage performance and accurately determine the following:

- How is the I/O load on the storage?
- Is the storage processing I/O requests quickly ?
- Is too much bandwidth being consumed when processing I/O?
- Is the AHV sized with adequate storage resources? If not, what type of storage is running short of space - the SSDs? or the SATA HDDs?

The Acropolis - Storage test helps administrators monitor overall storage health and rapidly leads them to the problem areas by providing quick and accurate answers to the aforesaid.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that vCenter server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the

Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total I/O latency	Indicates the average time taken by the storage to process I/O requests.	Secs	Ideally, the value of this measure should be very low. A high value or a steady increase in this value could indicate an I/O processing bottleneck on the storage. In such a case, compare the value of the *Read IO latency* and *Write IO latency* measures to figure out when the slowness is worst - when

Measurement	Description	Measurement Unit	Interpretation
			processing read requests? or write requests?
Read IO latency	Indicates the average time taken by the storage to process read I/O requests.	Secs	If the *Total I/O latency* measure reports an abnormally high value, then compare the value of these measures to figure out where the slowness is maximum - when processing read requests? or write requests?
Write IO latency	Indicates the average time taken by the storage to process write I/O requests.	Secs	
Total IO bandwidth	Indicates the bandwidth per second used by the storage when processing I/O requests.	KB/Sec	A high value for this measure denotes that the storage is processing bandwidth- intensive I/O. In such situations, you may want to compare the value of the *Read IO bandwidth* and *Write IO bandwidth* measures to know what type of I/O requests are truly contributing to the excessive bandwidth consumptions - read requests? or write requests?
Read IO bandwidth	Indicates the bandwidth per second used by the storage when processing read I/O requests.	KB/Sec	If the value of the *Total IO bandwidth* measure is high, then you may want to compare the value of the *Read IO bandwidth* and *Write IO bandwidth* measures to know what type of I/O requests are truly contributing to the excessive bandwidth consumption - read requests? or write requests?
Write IO bandwidth	Indicates the bandwidth per second used by the storage when processing write I/O requests.	KB/Sec	
Total IOPS	Indicates the number of I/O operations	Number	This measure is a good indicator of the level of I/O activity on the

Measurement	Description	Measurement Unit	Interpretation
	performed currently on the storage.		Nutanix storage. A steady and significant increase in the value of this measure could indicate a potential I/O overload. In such situations, you may want to compare the value of the Read IOPS and Write IOPS measures to know what type of IO operations are contributing to the overload.
Read IOPS	Indicates the number of read I/O operations performed currently on the storage.	Number	If the value of the *Total IOPS* measure is unusually high, then compare the value of these measures to know what is contributing to the unusual I/O activity levels - read requests? or write requests?
Write IOPS	Indicates the number of write I/O operations performed currently on the container.	Number	
Disk capacity	Indicates the total storage capacity.	GB	
Used space	Indicates the amount of storage space used by the monitored hypervisor and its VMs.	GB	A low value is desired for this measure.
Free space	Indicates the amount of storage space that is still unused.	GB	A high value is desired for this measure.
Disk space utilization	Indicates the percentage of storage capacity currently in use.	Percent	A value close to 100% indicates that the storage resources are being depleted rapidly. To know what type of storage resources are being over- utilized, compare the value of the SSD disk space usage and DAS-SATA disk space usage measures of this test.

Measurement	Description	Measurement Unit	Interpretation
Percent free space	Indicates of percentage of storage capacity that is currently free and available for use.	Percent	A value less than 50% indicates that the storage resources are being depleted rapidly. To know what type of storage resources are being over- utilized, compare the value of the SSD disk space usage and DAS-SATA disk space usage measures of this test.
Logical usage	Indicates the amount of logical storage space that is in use currently.	GB	
SSD disk capacity	Indicates the total storage capacity across all SSDs.	GB	
SSD used space	Indicates the amount of storage space used by all SSDs.	GB	A low value is desired for this measure.
SSD free space	Indicates the amount of storage space that is still unused in the SSDs.	GB	A high value is desired for this measure.
SSD disk space usage	Indicates the percentage of SSD storage capacity currently in use.	Percent	A value close to 100% indicates that the storage space in the SSDs is being depleted rapidly.
SSD free space available	Indicates of percentage of SSD storage capacity that is currently free and available for use.	Percent	A value less than 50% indicates that the storage space in the SSDs is being depleted rapidly.
DAS- SATA disk capacity	Indicates the total storage capacity across all directly attached SATA HDDs.	GB	
DAS- SATA used space	Indicates the total amount of storage space	GB	A low value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
	used by all directly attached SATA HDDs.		
DAS- SATA free space	Indicates the amount of storage space that is still unused in the directly attached SATA HDDs.	GB	A high value is desired for this measure.
DAS- SATA disk space usage	Indicates the percentage of the storage capacity of directly attached SATA HDDs that is currently in use.	Percent	A value close to 100% indicates that the storage space in the HDDs is being depleted rapidly.
DAS- SATA free space available	Indicates of percentage of the storage capacity of directly attached SATA HDDs that is currently free and available for use.	Percent	A value less than 50% indicates that the storage space in the HDDs is being depleted rapidly.

4.1.4 Hypervisor Resources Test

The Nutanix Acropolis host and the VMs operating on it share the compute and storage resources of the Nutanix platform. This is why, if one/more VMs on a host hog these resources, it will not only impact the performance of the other VMs of that host, but will also degrade the host performance as well. Likewise, a resource contention at the host-level can also adversely impact VM performance. To ensure that the host and VMs perform at peak capacity at all times, administrators should track how the AHV host and its VMs use the physical resources, proactively capture a potential resource contention, and precisely pinpoint the reason for the same - is it because of excessive resource usage by the AHV host? or are one/more VMs on the host resource-hungry? This is what the Hypervisor Resources test helps achieve. This test reports how the physical CPU and memory resources are used by an AHV host , and alerts you to erratic usage patterns. In the event of abnormal resource usage, the test also points you to the resource-starved VMs on the host, and thus reveals what is causing the usage anomaly - the VMs? or resource-intensive processing at the host-level?

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP**

list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a *Nutanix Acropolis* server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.
10. **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.

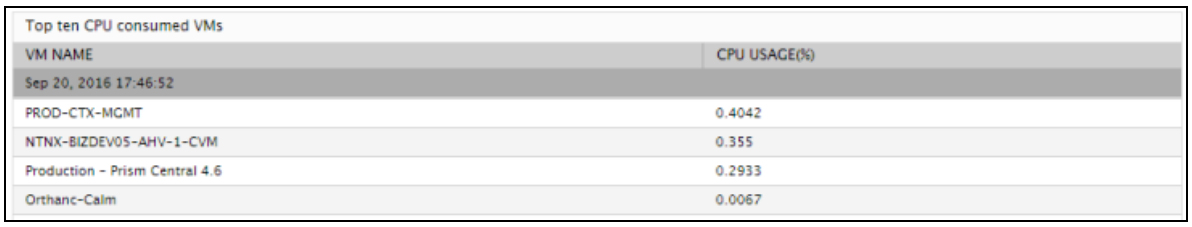
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU cores	Indicates the number of CPU cores on the host.	Number	
CPU sockets	Indicates the number of CPU sockets on the host.	Number	
CPU frequency	Indicates the frequency per CPU core.	GHz	
CPU capacity	Indicates the total CPU capacity of this host across all cores.	GHz	
CPU usage	Indicates the percentage of CPU resources used by the host and the VMs.	Percent	A value close to 100% is a cause for concern, as it signals a potential CPU contention on the host. In such a case, use the detailed diagnosis of this measure to view the top-10 CPU-consuming VMs on the host. From this, you can instantly identify the VM that is hogging the CPU resources. If no VM appears to be consuming CPU excessively, then you can conclude that resource-intensive processing at the host-level is causing the contention.
Memory capacity	Indicates the total memory capacity of the host.	GB	
Memory used	Indicates the total amount of memory used by the VMs and the host.	GB	A low value is desired for this measure.
Available memory	Indicates the amount of physical memory still	GB	A high value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
	unused on the host.		
Memory utilization	Indicates the percentage of memory used by the VMs and the host.	Percent	A value close to 100% is indicative of excessive memory utilization. In such a situation, use the detailed diagnosis of this measure to view the top- 10 memory consuming VMs on the host. From this, you can instantly identify the VM that is hogging the memory resources. If no VM appears to be consuming memory excessively, then you can conclude that memory- intensive processing at the host- level is causing the contention.
Available memory	Indicates the percentage of memory that is still unused on the host.	Percent	Ideally, the value of this measure should be high. A consistent drop in this value is indicative of excessive memory usage. In such a case, use the detailed diagnosis of the Memory utilization measure to isolate the cause of the memory drain.
Oplog disk size	Indicates the current size of the oplog.	GB	The OpLog is similar to a filesystem journal and is built as a staging area to handle bursts of random writes, coalesce them, and then sequentially drain the data to the extent store. A portion of the metadata disk is reserved for the oplog, and you can change the size through the nCLI.
Oplog disk usage	Indicates the percentage of allocated space that is used by the	Percent	A value close to 100% indicates that the oplog is running out of space. This can happen if data is

Measurement	Description	Measurement Unit	Interpretation
	oplog.		rapidly written to the oplog but is not drained from the log just as quickly. You may want to consider resizing the oplog to ensure that there is always room for writing more data.

Use the detailed diagnosis of the *CPU usage* measure to view the top-10 CPU-consuming VMs on the host. From this, you can instantly identify the VM that is hogging the CPU resources.

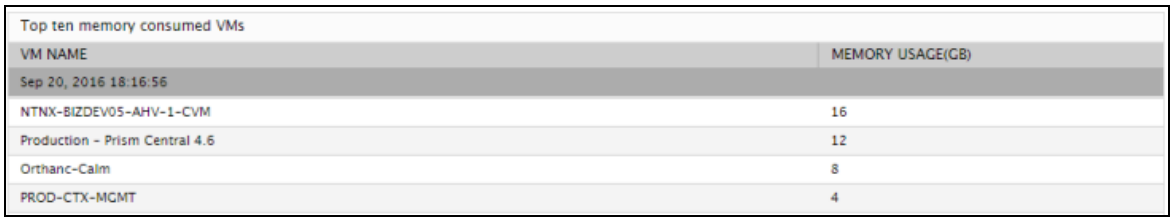


Top ten CPU consumed VMs

VM NAME	CPU USAGE(%)
Sep 20, 2016 17:46:52	
PROD-CTX-MGMT	0.4042
NTNX-BIZDEV05-AHV-1-CVM	0.355
Production - Prism Central 4.6	0.2933
Orthanc-Calm	0.0067

Figure 4.5: The detailed diagnosis of the CPU usage measure

Use the detailed diagnosis of the *Memory utilization* measure to view the top-10 memory consuming VMs on the host. From this, you can instantly identify the VM that is hogging the memory resources.



Top ten memory consumed VMs

VM NAME	MEMORY USAGE(GB)
Sep 20, 2016 18:16:56	
NTNX-BIZDEV05-AHV-1-CVM	16
Production - Prism Central 4.6	12
Orthanc-Calm	8
PROD-CTX-MGMT	4

Figure 4.6: The detailed diagnosis of the Memory utilization measure

4.2 The Network Layer

Periodically check the availability and responsivness of the Acropolis server over the network using the **Network** test mapped to this layer. Since this test is already discussed in the **Monitoring Network Elements** document, let us proceed to the next layer.

Figure 4.7: The test mapped to the Network layer

4.3 The Outside View of VMs Layer

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 Acropolis server, so as to minimize the impact it has on the other guests on the current Acropolis 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.

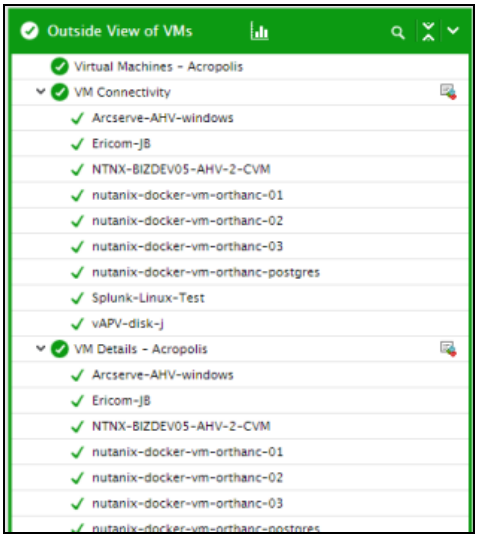


Figure 4.8: The tests mapped to the Outside View of VMs layer

4.3.1 VM Details - Acropolis Test

This test monitors the amount of the physical server's resources that each guest managed by a Nutanix prism is taking up. Using the metrics reported by this test, administrators can determine which virtual guest is taking up most CPU, which guest is generating the most network traffic, which guest is over-utilizing memory, and which guest is eroding disk space.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every VM on the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism

server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to

Section **4.3.1**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **REPORT POWERED ON** - You can set the **REPORT POWERED ON** status to **YES**, so that the test reports an additional measure, *Is VM powered on?*, revealing whether a guest OS is currently running or not. The default status of this flag is set to **Yes** for a Nutanix Acropolis server. However, the default status of this flag is **No** in the case of Nutanix Acropolis VDI server; this is because, in such environments, the virtual desktops will be in the powered-off state most of the time.

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	Description	Measurement Unit	Interpretation
VM power- on state:	Indicates the current state of the virtual machine.		The table below displays the States that can be reported by this measure, and their numeric equivalents: State / Value Off / 0 On / 1 Suspended / 2 **Note:** By default, this measure reports one of the **State**s listed in the table above. The graph of this measure however will represent the VM status using the numeric equivalents - '0' to '7'.
Is controller VM	Indicates whether/not this VM is the controller VM	Number	The Nutanix CVM is what runs the Nutanix software and serves all of the I/O operations for the hypervisor and all VMs running on that host. Prism service runs on every CVM with an elected Prism Leader which is responsible for handling HTTP requests. If this measure reports the value 0, it indicates that the VM is not a controller VM, whereas the value 1 indicates that it is a controller VM.
Current sessions	Indicates the number of sessions that are	Number	The value of this measure reveals the guest OS that is currently busy.

Measurement	Description	Measurement Unit	Interpretation
	currently active on the guest.		The detailed diagnosis of this metric lists the VM name, user of that particular VM, and operating system of VM.
CPU reserved	Indicates the amount of CPU power reserved for this VM.	GHz	
Virtual CPU utilization	Indicates the percentage of virtual CPU resources used by this VM.	Percent	Compare the value of this measure across VMs to know which VM is using the allocated CPU resources excessively.
Physical CPU utilization	Indicates the percentage of physical CPU that is used by the VM.	Percent	Ideally, a VM should use only a small percentage of the physical CPU resources of the Nutanix Acropolis host. High CPU usage by a VM could cause other VMs to contend for limited CPU resources, thereby adversely impacting the performance of the other VMs and the applications executing on them.
Virtual CPUs	Indicates the number of virtual CPUs allocated to this VM.	Number	Compare the value of this measure across VMs to know which VM has been allocated the maximum number of virtual CPUs.
Disk capacity	Indicates the total disk capacity available to this VM.	GB	
Used space	Indicates the amount of disk space used by this VM.	GB	
Disk space utilization	Indicates the percentage of disk space used by this VM.	Percent	Comparing the value of this measure across VMs will reveal the VM that is consuming too much disk

Measurement	Description	Measurement Unit	Interpretation
			space.
Virtual disks	Indicates the number of virtual disks in the VM.	Number	Use the detailed diagnosis of this measure to view the details of the virtual disks.
Memory reserved capacity	Indicates the amount of memory reserved for this VM.	GB	
Memory capacity	Indicates the total amount of memory available to this VM.	GB	
Memory usage	Indicates the amount of allocated memory capacity currently being used by this VM.	GB	
Free memory	Indicates the amount of free memory available to this VM.	GB	Compare the value of this measure across VMs to know which VM is running out of free memory.
Memory utilization	Indicates the percentage of allocated memory capacity currently being utilized by this VM.	Percent	Compare the value of this measure across VMs to know which VM is using memory excessively.
Percent free memory	Indicates the percentage of free memory available in the VM.	Percent	Compare the value of this measure across VMs to know which VM is running short of free memory.
Network adapters	Indicates the number of network adapters available to this VM.	Number	
Data received	Indicates the amount of data received by this VM.	GB	

Measurement	Description	Measurement Unit	Interpretation
Data transmitted	Indicates the amount of data transmitted by this VM.	GB	
Total IOPS	Indicates the number of I/O operations per second (IOPS) on this VM.	Number	This measure is a good indicator of the level of I/O activity on each VM. Compare the value of this measure to know which VM is experiencing an I/O overload.
Read IOPS	Indicates the number of read I/O operations per second on this VM.	Number	If the value of the *Total IOPS* measure is high for a VM, then compare the value of these measures for that VM to know where the bottleneck lies - when reading or writing?
Write IOPS	Indicates the number of write I/O operations per second on this VM.	Number	
Total IO latency	Indicates the average I/O latency of this VM.	Seconds	Compare the value of this measure across VMs to know which VM is the slowest in processing I/O requests.
Read IO latency	Indicates the average read I/O latency for this VM.	Seconds	If the value of the *Total IO latency* measure is high for a VM, then compare the value of these measures for that VM to know where the bottleneck lies - when reading or writing?
Write IO latency	Indicates the average write I/O latency for this VM.	Seconds	
Total IO bandwidth	Indicates the bandwidth consumed when processing I/O requests to this VM.	KB/Sec	Compare the value of this measure to know which VM is consuming maximum I/O bandwidth.
Read I/O bandwidth	Indicates the amount of bandwidth consumed	KB/Sec	If the value of the *Total IO bandwidth* measure is unusually

Measurement	Description	Measurement Unit	Interpretation
	by this VM when processing read I/O requests.		high for a VM, then compare the value of these measures for that VM to know when maximum bandwidth was consumed - when reading or writing?
Write I/O bandwidth	Indicates the amount of bandwidth consumed by this VM when processing write I/O requests.	KB/Sec	

4.3.2 Configuring Users for VM Monitoring

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

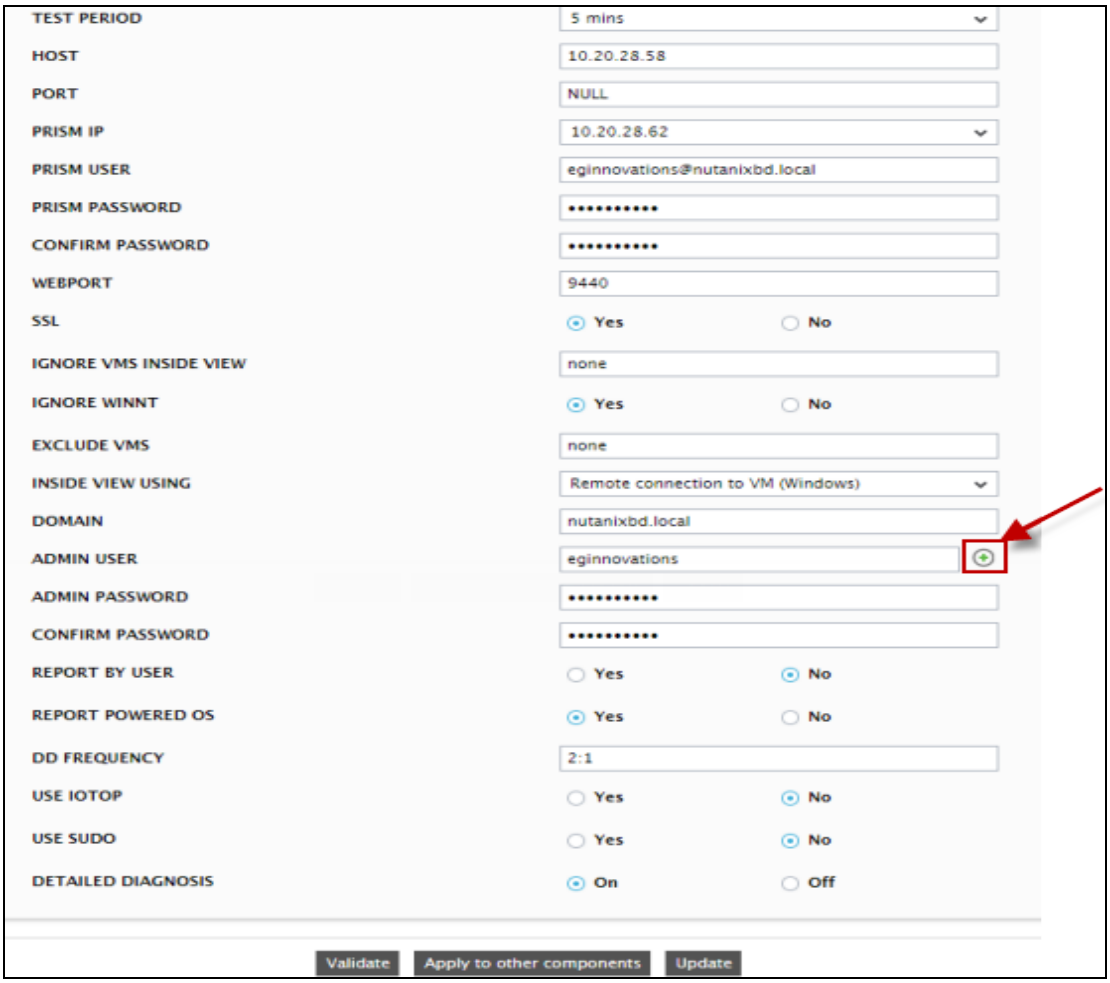


Figure 4.9: Configuring a sample Acropolis test

Upon clicking, Figure 4.10 will appear, using which the VM user details can be configured.

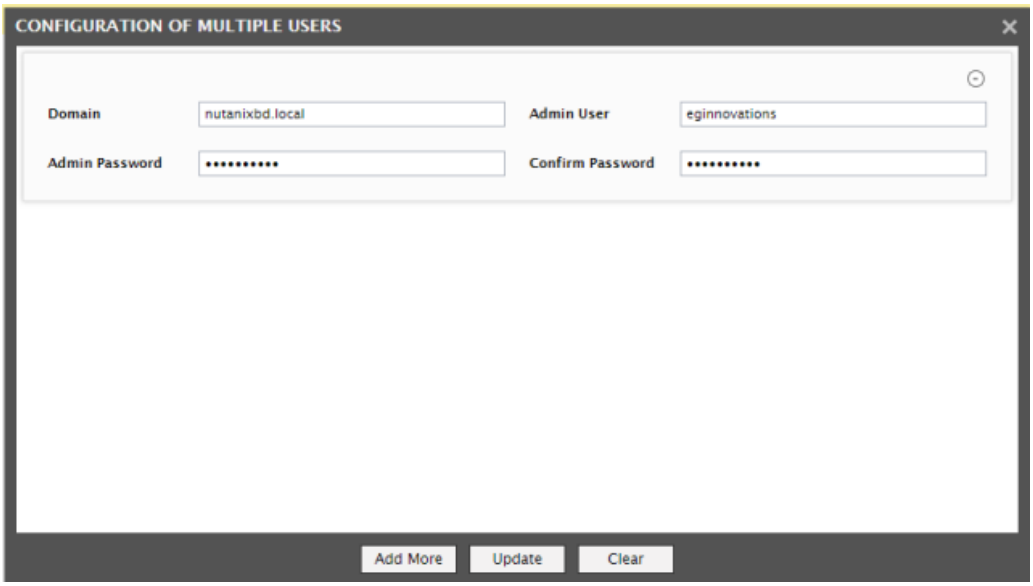


Figure 4.10: The VM user configuration page

To add a user specification, do the following:

1. First, provide the name of the **Domain** to which the VMs belong (see Figure 4.10). If one/more VMs do not belong to any domain, then, specify *none* here.
2. The eG agent must be configured with user privileges that will allow the agent to communicate with the VMs in a particular domain and extract statistics. If *none* is specified against **Domain**, then a local user account can be provided against **Admin User**. On the other hand, if a valid **Domain** name has been specified, then a domain administrator account can be provided in the **Admin User** 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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

3. The password of the specified **Admin User** should be mentioned in the **Admin Password**text box.
4. Confirm the password by retyping it in the **Confirm Password** text box.
5. To add more users, click on the **Add More** button in Figure 4.10. This will allow you to add one more user specification as depicted by Figure 4.11.

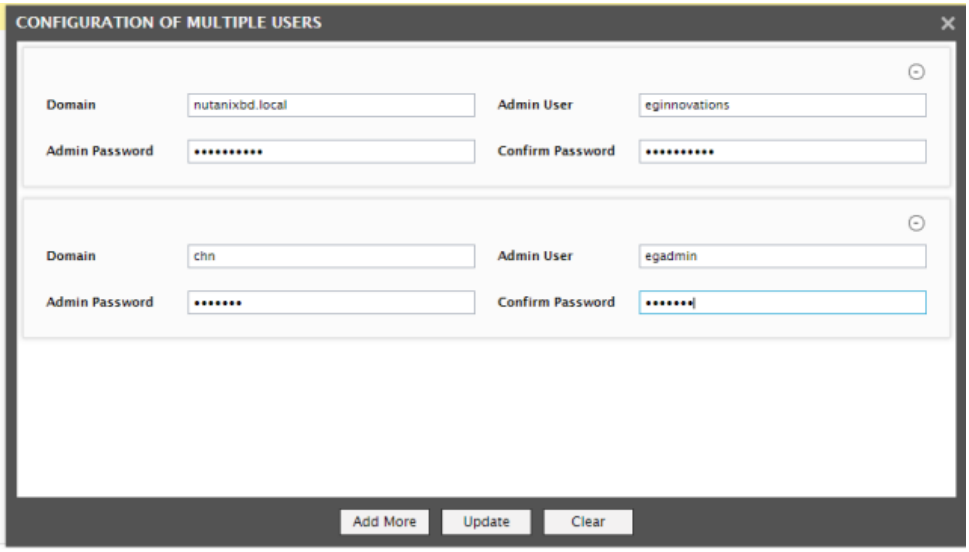


Figure 4.11: Adding another user

6. In some virtualized environments, the same **Domain** could be accessed using multiple **Admin User** names. For instance, to login to a **Domain** named *chn*, the eG agent can use the **Admin User** name *egadmin* or the **Admin User** name *eguser*. You can configure the eG agent with the credentials of both these users as shown by Figure 4.12.

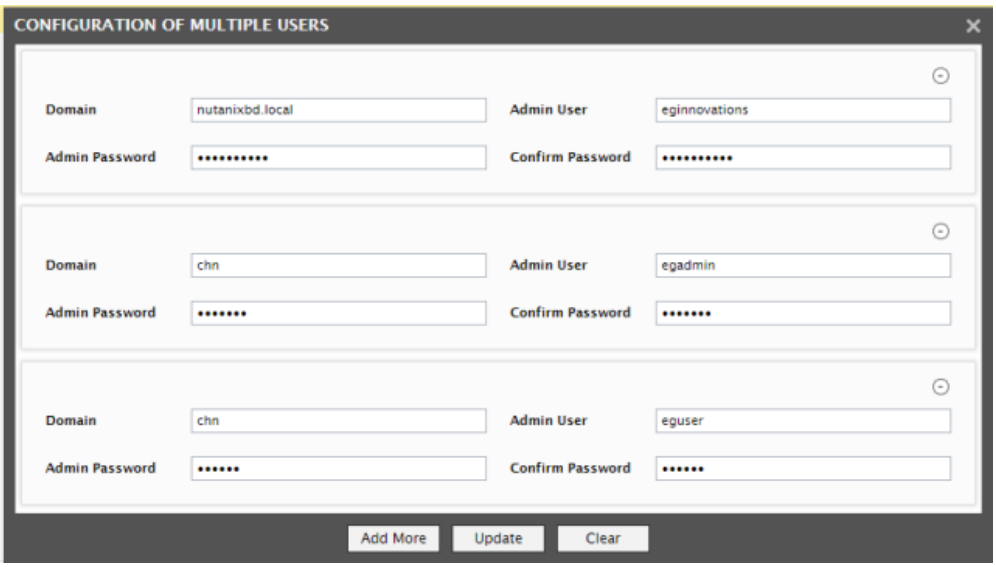


Figure 4.12: Associating a single domain with different admin users

7. When this is done, then, while attempting to connect to the domain, the eG agent will begin by using the first **Admin User** name of the specification. In the case of Figure 4.12, this will be *egadmin*. If, for some reason, the agent is unable to login using the first **Admin User** name, then it will try to login again, but this time using the second **Admin User** name of the specification - i.e., *eguser* in our example (see Figure 4.12). If the first login attempt itself is successful, then the agent will ignore the second **Admin User** name.
8. To clear all the user specifications, simply click the **Clear** button in Figure 4.12.
9. To remove the details of a particular user alone, just click the ⊖ button in Figure 4.12.
10. To save the specification, just click on the **Update** button in Figure 4.12. This will lead you back to the test configuration page, where you will find the multiple domain names, user names, and passwords listed against the respective fields (see Figure 4.13).

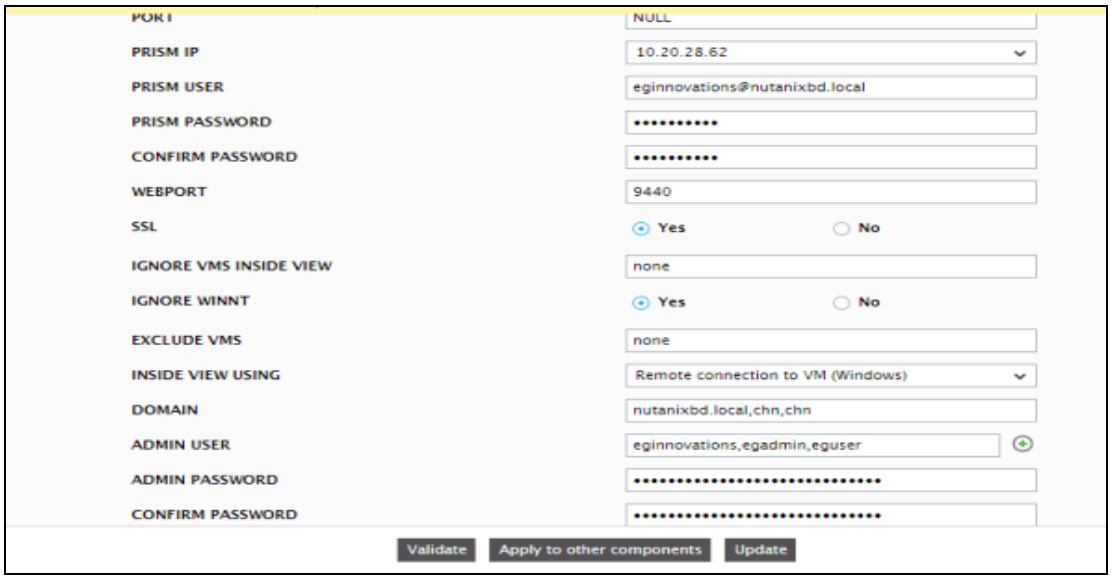


Figure 4.13: The test configuration page displaying multiple domain names, user names, and passwords

4.3.3 Virtual Machines – Acropolis Test

Live migration is supported on an Acropolis Hypervisor (AHV) cluster. Live migration is the ability to move a running VM from one host (node) to another in the same cluster, without any downtime or loss of connectivity. Live migration can be initiated manually or automatically. While manual migration can be initiated via the Prism interface, automatic VM migration is triggered by the Acropolis Dynamic Resource Scheduler or the VM High Availability (VMHA) capability of an Acropolis cluster. The scheduler monitors each individual node's CPU and memory utilization. In the event where a node's CPU allocation breaches its threshold (currently 85% of host CPU), the scheduler automatically migrates VMs off that host to re-balance the workload. VMHA, if enabled for a cluster, ensures that critical VMs are automatically restarted on another Acropolis Hypervisor (AHV) host in the cluster if a host fails.

Where migration is automatic, administrators may want to keep close track of VM movement, so that they can accurately tell on which host a VM is operating at a given point in time. The **Virtual Machines - Acropolis** test provides administrators with this insight. This test indicates whether any guests have migrated to or from the virtual server, and if so, which ones are those. In addition, the test also enables administrators to determine how many guests have registered with the Acropolis server, and how many of these are currently running. Additionally, for VDI environments, the test reports the number and names of VMs with users logged in and the ones without any users logged in; this way, unused VMs that are unnecessarily hogging resources.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **ISVDISERVER** - By default, this flag is set to **NO** indicating that the test is being configured to execute for a *Nutanix Acropolis*model and not a *Nutanix Acropolis VDI* model. This distinction needs to be made, since this test reports 2 additional measures for a *Nutanix Acropolis VDI* server - namely, *VMs with users* and *VMs without users*.**DD FOR REGISTERED VMS**
5. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
6. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

7. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

8. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

9. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

10. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

11. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

12. **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.

13. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

14. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.3.3**.

- **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*.

15. **DD FOR TOTAL VMS** – By default, this flag is set to **No**. This means that the test will not report detailed metrics for the *Total VMs* measure by default. In large virtualized environments characterized by hundreds of VMs, this default setting will make sure that there is no unnecessary strain on the eG database. You can, if you so need, enable the test to report detailed metrics for this measure by setting this flag to **Yes**.
16. **DD FOR POWEREDON VMS** – By default, this flag is set to **Yes**. This means that the test will report the complete list of powered on VMs as part of the detailed diagnosis of the *Powered on VMs* measure. To disable this capability for the *Powered on VMs* measure, set this flag to **No**.
17. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a *Nutanix Acropolis* server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.
18. **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	Description	Measurement Unit	Interpretation
Total VMs	Indicates the total number of VMs that have been registered with the Nutanix Prism.	Number	To know which VMs are registered with the Prism, use the detailed diagnosis capability of this measure (if enabled). Note that detailed metrics will be available for this measure only if the **DD FOR TOTAL VMS** flag is set to **Yes**.
Powered on VMs	Indicates the number of	Number	To know which are the VMs that

Measurement	Description	Measurement Unit	Interpretation
	VMs that are currently powered on.		are powered on, use the detailed diagnosis capability of this measure (if enabled).
Powered off VMs	Indicates the number of powered off VMs on the monitored hypervisor.	Number	
Suspended VMs	Indicates the number of VMs that are currently suspended.	Number	
VMs with users	Indicates the number of powered on guests with users logged in.	Number	To know which guests the users have logged into, use the detailed diagnosis capability of this measure (if enabled). Note that this measure will not be available for the *Nutanix Acropolis* model.
Guests without users	Indicates the number of powered on guests without any users logged in.	Number	Note that this measure will not be available for the *Nutanix Acropolis* model.
Added VMs	Indicates the number of VMs that were newly added to the Nutanix Acropolis server during this measurement period.	Number	The detailed diagnosis of these measures, if enabled, lists the virtual machines that were migrated to or from (as the case may be) the Nutanix Acropolis server.
Removed VMs	Indicates the number of VMs that were newly removed from the Nutanix Acropolis server during this measurement period.	Number	

The detailed diagnosis of the *Powered on VMs* measure, provides the complete list of VMs that are currently powered on.

Details of VMs powered on

VM NAME	IP ADDRESS	OS
Sep 19, 2016 15:27:37		
NTNX-BIZDEV05-AHV-1-CVM	10.20.28.54	N/A
Production - Prism Central 4.6	10.20.18.51	N/A
PROD-CTX-MGMT	10.20.28.221	N/A
Orthanc-Calm	N/A	N/A

Figure 4.14: The detailed diagnosis of the Powered on VMs measure of a Nutanix Acropolis server

The detailed diagnosis of the Added VMs measure displays the IP address and operating system of those VMs that were recently migrated to the host.

Details of newly added VMs

VM NAME	IP ADDRESS	OS
Sep 19, 2016 06:35:20		
NTNX-BIZDEV05-AHV-1-CVM	10.20.28.54	N/A
Production - Prism Central 4.6	10.20.18.51	N/A
PROD-CTX-MGMT	10.20.28.221	N/A
Orthanc-Calm	N/A	N/A

Figure 4.15: The detailed diagnosis of the Added VMs measure

The detailed diagnosis of the Removed VMs measure displays the IP address and operating system of the VMs that were recently removed/migrated from the host.

Removed VM Details

VM NAME	IP ADDRESS	OS
Sep 18, 2016 15:56:16		
NTNX-BIZDEV05-AHV-1-CVM	10.20.28.54	N/A
Production - Prism Central 4.6	10.20.18.51	N/A
PROD-CTX-MGMT	10.20.28.221	N/A
Orthanc-Calm	N/A	N/A

Figure 4.16: The detailed diagnosis of the Removed VMs measure

4.3.4 VM Connectivity Test

Sometimes, a VM could be in a powered-on state, but the failure of the VM operating system or any fatal error in VM operations could have rendered the VM inaccessible to users. In order to enable administrators to promptly detect such 'hidden' anomalies, the eG agent periodically runs a

connectivity check on each VM using this test, and reports whether the VM is accessible over the network or not.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each VM configured on the Acropolis serverbeing 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis

discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.
12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.
13. **PACKETSIZE** - The size of packets used for the test (in bytes).
14. **PACKETCOUNT** - The number of packets to be transmitted during the test.
15. **TIMEOUT** - How long after transmission should a packet be deemed lost (in seconds).
16. **PACKETINTERVAL** - Represents the interval (in milliseconds) between successive packet transmissions during the execution of the network test for a specific target.
17. **REPORTUNAVAILABILITY** – By default, this flag is set to **No**. This implies that, by default, the test will

not report the unavailability of network connection to any VM. In other words, if the Network availability measure of this test registers the value 0 for any VM, then, by default, this test will not report any measure for that VM; under such circumstances, the corresponding VM name will not appear as a descriptor of this test. You can set this flag to **Yes**, if you want the test to report and alert you to the unavailability of the network connection to a VM.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Avg network delay:	Indicates the average delay between transmission of packet to a VM and receipt of the response to the packet at the source.	Secs	An increase in network latency could result from misconfiguration of the router(s) along the path, network congestion, retransmissions at the network, etc.
Min network delay:	The minimum time between transmission of a packet and receipt of the response back.	Secs	A significant increase in the minimum round-trip time is often a sure sign of network congestion.
Packet loss:	Indicates the percentage of packets lost during transmission from source to target and back.	Percent	Packet loss is often caused by network buffer overflows at a network router or by packet corruptions over the network. The detailed diagnosis for this measure provides a listing of routers that are on the path from the external agent to target server, and the delays on each hop. This information can be used to diagnose the hop(s) that could be causing excessive packet loss/delays.
Network availability of VM:	Indicates whether the network connection is available or not.	Percent	A value of 100 indicates that the VM is connected. The value 0 indicates that the VM is not connected. Typically, the value 100 corresponds to a Packet loss of 0.

4.4 The Inside View of VMs Layer

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 Acropolis 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 mapped to the **Inside View of VMs** layer provide an “inside” view of the workings of each of the guests - these tests execute on an host, but 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 4.17: The tests mapped to the Inside View of VMs layer

4.4.1 System Details - VM Test

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

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every combination of *virtual_guest:processor* or *guest_user:processor*.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed

against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to

Section **4.4.1**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **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.
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	Description	Measurement Unit	Interpretation
Virtual CPU utilization:	This measurement indicates the percentage of CPU utilized by the processor.	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 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

Measurement	Description	Measurement Unit	Interpretation
			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.
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 4.18). 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.

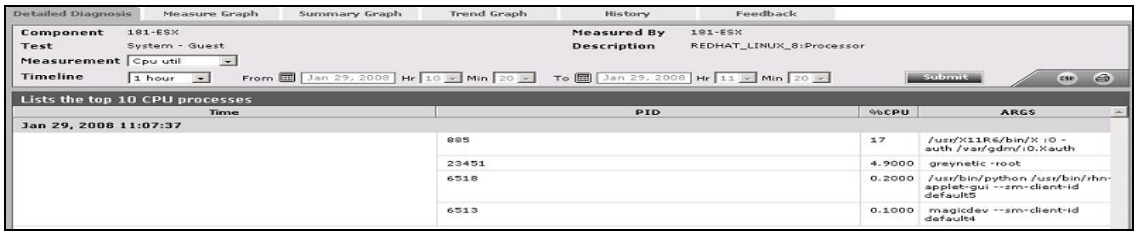


Figure 4.18: The top 10 CPU consuming processes

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.

4.4.2 Disk Activity - VM Test

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

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every combination of *virtual_guest:disk_partition* or *guest_user:disk_partition*.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes

will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.2**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **USE SUDO** –**This parameter is of significance to Linux and Solaris VMs only**. By default, the **USE SUDO** parameter is set to **No**. This indicates that, by default, this test will report the detailed diagnosis for the *Percent virtual disk busy* measure of each disk partition being monitored by executing the */usr/bin/iotop* command or */usr/sbin/iotop* command. However, in some highly secure virtualized environments, this command cannot be executed directly on a Linux. In such cases, set this parameter to **Yes**. This will enable the eG agent to execute the *sudo/usr/bin/iotop* command or *sudo/usr/sbin/iotop* and retrieve the detailed diagnosis of the *Percent virtual disk busy* measure.

17. **USE IOTOP** – The **Disk Activity – VM** test uses the *iotop* command to collect detailed diagnostics on disk activity from Linux VMs. By default, this flag is set to **No**, indicating that the test will not use the *iotop* command – this in turn implies that this test will not report detailed diagnostics for Linux VMs by default. If you want the test to report detailed metrics on disk activity on Linux VMs, set this flag to **Yes.**

18. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

19. **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	Description	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 percentage 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	Secs	

Measurement	Description	Measurement Unit	Interpretation
	disk.		
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	Writes/Sec	A dramatic increase in this value may be indicative of an I/O

Measurement	Description	Measurement Unit	Interpretation
	local disk per second.		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.

The detailed diagnosis of the *Percent virtual disk busy* measure, if enabled, provides information such as the Process IDs executing on the disk, the Process names, the rate at which I/O read and write requests were issued by each of the processes, and the rate at which data was read from and written into the disk by each of the processes. In the event of excessive disk activity, the details provided in the detailed diagnosis page will enable users to figure out which process is performing the I/O operation that is keeping the disk busy. **The detailed diagnosis for this test is available for Windows guests only, and not Linux guests**.

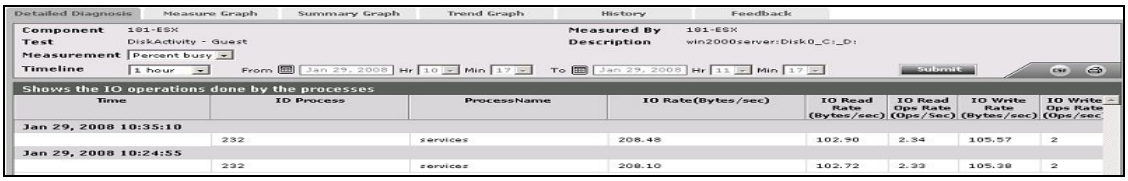


Figure 4.19: The detailed diagnosis of the Percent virtual busy measure

4.4.3 Disk Space - VM Test

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

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every combination of *virtual_guest:disk_partition* or *guest_user:disk_partition*.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to

use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
    - **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that

along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.3**.

- **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*.

14. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	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	

Measurement	Description	Measurement Unit	Interpretation
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 partition of a system; for the Total descriptor, this measure reports the percentage of disk space used 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.

4.4.4 Domain Time Sync – VM Test

Time synchronization is one of the most important dependencies of windows. A time protocol is responsible for determining the best available time information and converging the clocks to ensure that a consistent time is maintained across systems. By default, windows support a tolerance of plus or minus five minutes for clocks. If the time variance exceeds this setting, clients will be unable to authenticate and in the case of domain controllers, replication will not occur. It implements a time synchronization system based on Network Time Protocol (NTP).

NTP is a fault-tolerant, highly scalable time protocol and it is used for synchronizing computer clocks by using a designated reference clock. A reference clock is some device or machinery that spits out the current time. The special thing about these things is accuracy. Reference clocks must be accurately following some time standard. NTP will compute some additional statistical values based on the current time reported by the reference clock, which will describe the quality of time it sees. Among these values are: offset (or phase), jitter (or dispersion), frequency error, and stability. Thus each NTP server will maintain an estimate of the quality of its reference clocks and of itself.

This test reports the time difference between the reference clock and that of the target environment, and thus helps assess the quality of time seen by the Windows VM. With the help of this test, you can also easily determine whether the reference time changed recently.

Note:

This test reports metrics for Windows VMs only.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence: Agents -> Tests -> Enable/Disable, pick *Nutanix Acropolis VDI* as the **Component type**, set *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.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every user to each Windows virtual desktop on the Nutanix Acropolis 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to

monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while

monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.
12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.4**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
NTP offset:	Indicates the time difference between the local clock and the designated reference clock.	Secs	For a tiny offset, NTP will adjust the local clock; for small and larger offsets, NTP will reject the reference time for a while. In the latter case, the operating system's clock will continue with the last corrections effective while the new reference time is being rejected. After some time, small offsets (significantly less than a second) will be slewed (adjusted slowly), while larger offsets will cause the clock to be stepped (set anew). Huge offsets are rejected, and NTP will terminate itself, believing something very strange must have happened.

4.4.5 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 : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on guest/currently logged-in user on the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.

4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page.

Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.5**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will

report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **HANDLES GROWTH LIMIT** - This defines the upper limit of the handles opened by any process. By default, this parameter is set to 8000.
17. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a *Nutanix Acropolis* server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.
18. **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	Description	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.

Measurement	Description	Measurement Unit	Interpretation
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 parameter - **HANDLES GROWTH LIMIT**.	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 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.

The detailed diagnosis of the *Handles used by processes* measure, if enabled, lists the names of top-10 processes in terms of handle usage, the number of handles each process uses, the process ID, and the ID of the parent process.

List of top 10 processes in a VM that are holding handles

Time	Process Name	Handles used	Process ID	Parent PID
Jan 29, 2009 12:00:49				
	System	3359	0	4
	js	1718	540	6420
	svchost	1208	540	1012
	lsass	1112	492	552
	csrss	1097	420	468
	winlogon	564	420	492
	ImaSrv	559	540	3696
	Rtvscan	536	540	3936
	tomcat	485	540	6572
	services	482	492	540

Figure 4.20: The detailed diagnosis of the Handles used by processes measure

The detailed diagnosis of the *Processes using handles above limit in VM* measure, if enabled, lists the details of processes that are using more handles than the configured limit.

List of processes in a VM that are using handles above the configured handle growth value

Time	Process Name	Handles used	Process ID	Parent PID
Jan 29, 2009 17:54:18	eGRSvc	62410	412	11512

Figure 4.21: The detailed diagnosis of the Processes using handles above limit in VM measure

4.4.6 GPU - VM Test

GPU-accelerated computing is the use of a graphics processing unit (GPU) together with a CPU to accelerate scientific, analytics, engineering, consumer, and enterprise applications. GPU-accelerated computing enhances application performance by offloading compute-intensive portions of the application to the GPU, while the remainder of the code still runs on the CPU. Architecturally, while a CPU has only few cores and handles few hundred threads at a time, a GPU is composed of hundreds of cores that can handle thousands of threads simultaneously and render a flawless rich graphics experience.

Now, imagine if you could access your GPU-accelerated applications, even those requiring intensive graphics power, anywhere on any device. **NVIDIA GRID** makes this possible. With NVIDIA GRID, a virtualized GPU designed specifically for virtualized server environments, data center managers can bring true PC graphics-rich experiences to users.

The NVIDIA GRID GPUs will be hosted in enterprise data centers and allow users to run virtual desktops or virtual applications on multiple devices connected to the internet and across multiple operating systems, including PCs, notebooks, tablets and even smartphones. Users can utilize their online-connected devices to enjoy the GPU power remotely.

In VDI/virtualized server environments, the NVIDIA GRID delivers GPU resources to virtual desktops/VMs. This way, graphics can be rendered on a virtual machine's (VM's) host server rather than on a physical end-point device. This technology now makes it possible to use virtual desktop technology to support users accessing graphics intensive workloads. There are two modes of making GPU resources available to virtual desktops:

- **Dedicated GPU or GPU Pass-through Technology:** NVIDIA GPU pass-through technology lets you create a virtual workstation that gives users all the benefits of a dedicated graphics processor at their desk. By directly connecting a dedicated GPU to a virtual machine through the hypervisor, you can now allocate the full GPU and graphics memory capability to a single virtual machine without any resource compromise.

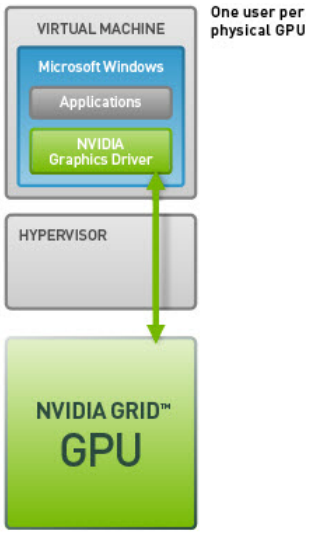


Figure 4.22: Dedicated GPU Technology

- **Shared GPU or Virtual GPU (vGPU) Technology:** GRID vGPU is the industry's most advanced technology for sharing true GPU hardware acceleration between multiple virtual desktops—without compromising the graphics experience. With GRID vGPU technology, the graphics commands of each virtual machine are passed directly to the GPU, without translation by the hypervisor. This allows the GPU hardware to be time-sliced to deliver improved shared virtualized graphics performance. The GRID vGPU manager allows for management of user profiles. IT managers can assign the optimal amount of graphics memory and deliver a customized graphics profile to meet the specific needs of each user. Every virtual desktop has dedicated graphics memory, just like they would at their desk, so they always have the resources they need to launch and run their applications.

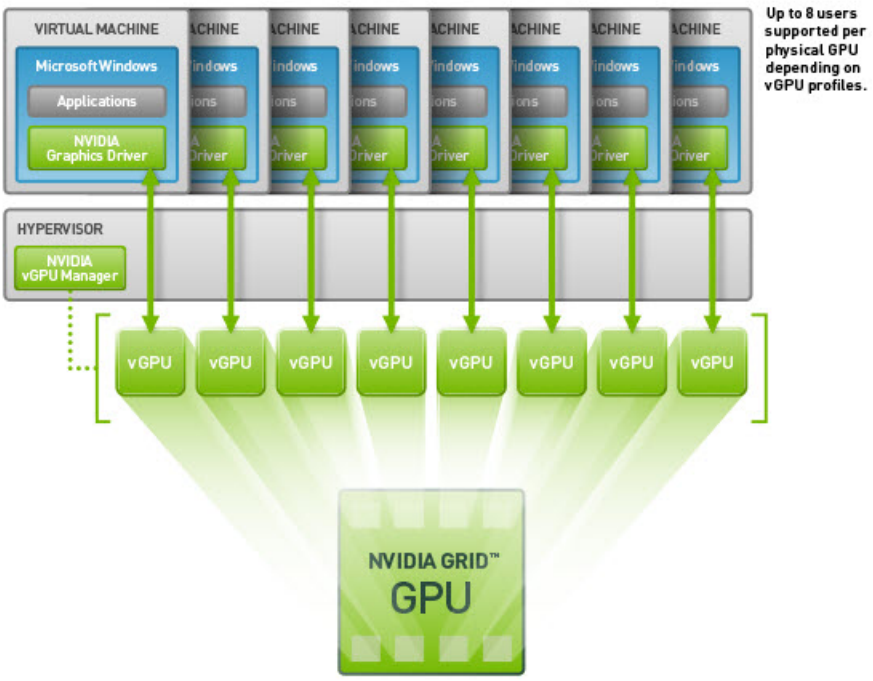


Figure 4.23: Shared vGPU Technology

In GPU-enabled virtualized environments, if users to VMs/virtual desktops complain of slowness when accessing graphic applications, administrators must be able to instantly detect the slowness and figure out its root-cause – is it because adequate GPU resources are not allocated to the VMs/virtual desktops? Is it because of excessive utilization of GPU memory and processing resources by a few VMs/virtual desktops? Or is it because the GPU clock frequencies are improperly set for one/more GPUs used by a VM/virtual desktop?

- The VMs/virtual desktops have been allocated enough vGPUs;
- The vGPUs are configured with enough graphics memory;
- The vGPU clock frequencies are rightly set;
- The GPU technology in use – i.e., the GPU Pass-through technology or the Shared vGPU technology – is ideal for the graphics processing requirements of the environment;

Measures to right-size the host and fine-tune its GPU configuration can be initiated based on the results of this analysis. This is exactly what the **GPU – VM** test helps administrators achieve!

This test tracks the rate at which each vGPU processes frames, and thus pinpoints those vGPUs that are experiencing a processing bottleneck. The test also monitors the memory usage on each vGPU and helps administrators identify the vGPUs where memory is over-used. The test also reveals how each of these VMs/virtual desktops use each of the allocated vGPUs, thus enabling

administrators to determine whether/not the allocated vGPUs are sufficient for the current and future processing requirements of the VMs/virtual desktops. In the process, the test also pinpoints those VMs/virtual desktops that are over-utilizing the graphical processors assigned to them. Also, to make sure that the assigned vGPUs are functioning without a glitch, the power consumption, temperature, and clock frequency of each vGPU is also checked at periodic intervals, so that abnormalities can be quickly detected.

Note:

This test will report metrics for only those Windows VMs where the **NVWMI** is installed. The steps for installing **NVWMI** and configuring the eG agent to use it have been detailed in the *Configuring the eG Agent for Monitoring the Usage of NVIDIA GPU* document.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results every vGPU assigned to each Windows VM on the Nutanix Acropolis 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option

from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and

ADMIN PASSWORD parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
    - **If the guests belong to different domains** - In this case, you might want to provide

multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.6**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.
16. **IGNORESERVICES** - Provide a comma-separated list of services that need to be ignored while monitoring.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Cooler rate:	Indicates the percentage of device cooler rate for this GPU	Percent	

Measurement	Description	Measurement Unit	Interpretation
	of this VM/virtual desktop.		
Virtual GPU compute utilization:	Indicates the proportion of time over the past sample period during which one or more kernels was executing on this vGPU of this VM/virtual desktop.	Percent	A value close to 100% indicates that the GPU of the VM/virtual desktop is busy processing graphic requests almost all the time. In a Shared vGPU environment a vGPU may be in use almost all the time, if the VM/virtual desktop it is allocated to runs graphic- intensive applications. A resource- hungry VM/virtual desktop can impact the performance of other VMs/virtual desktops on the same server. If you find that only a single VM/virtual desktop has been consistently hogging the GPU resources, you may want to switch to the Dedicated GPU mode, so that excessive GPU usage by that VM/virtual desktop has no impact on the performance of other VMs/virtual desktops on that host. If all GPUs assigned to a VM/virtual desktop are found to be busy most of the time, you may want to consider allocating more GPU resources to that VM/virtual desktop.
Power consumption:	Indicates the current power usage of this GPU allocated to this VM/virtual desktop.	Watts	A very high value is indicative of excessive power usage by the GPU. Compare the value of this measure across GPUs to know which VM's/virtual desktop's GPU is

Measurement	Description	Measurement Unit	Interpretation
			consuming power excessively.
Core GPU temperature:	Indicates the current temperature of this GPU allocated to this VM/virtual desktop.	Celsius	Ideally, the value of this measure should be low. A very high value is indicative of abnormal GPU temperature. Compare the value of this measure across VMs/virtual desktops to identify that VM/virtual desktop for which GPU temperature soared since the last reading. To reduce the heat output of the GPU and consequently its temperature, you may consider performing underclocking. For instance, it is possible to set a GPU to run at lower clock rates when performing everyday tasks (e.g. internet browsing and word processing), thus allowing the card to operate at lower temperature and thus lower, quieter fan speeds.
Total framebuffer memory:	Indicates the total size of frame buffer memory of this GPU of this VM/virtual desktop.	MiB	Frame buffer memory refers to the memory used to hold pixel properties such as color, alpha, depth, stencil, mask, etc.
Used frame buffer memory:	Indicates the amount of frame buffer memory on-board this GPU that is being used by this VM/virtual desktop.	MiB	Frame buffer memory refers to the memory used to hold pixel properties such as color, alpha, depth, stencil, mask, etc. Properties like the screen resolution, color level, and refresh speed of the

Measurement	Description	Measurement Unit	Interpretation
			frame buffer can impact graphics performance. Also, if *Error-correcting code (ECC)* is enabled, the available frame buffer memory may be decreased by several percent. This is because, ECC uses up memory to detect and correct the most common kinds of internal data corruption. Moreover, the driver may also reserve a small amount of memory for internal use, even without active work on the GPU; this too may impact frame buffer memory. For optimal graphics performance therefore, adequate frame buffer memory should be allocated to the VM/virtual desktop.
Free frame buffer memory:	Indicates the amount of frame buffer memory on-board this GPU that is yet to be used by this VM/virtual desktop.	MiB	
Frame buffer memory utilization:	Indicates the percentage of total frame buffer memory that has been allocated to this VM/virtual desktop.	Percent	Ideally, the value of this measure should be low. A value close to 100% is indicative of excessive usage of frame buffer memory. Properties like the screen resolution, color level, and refresh speed of the frame buffer can impact graphics performance.

Measurement	Description	Measurement Unit	Interpretation
			Also, if Error-correcting code (ECC) is enabled, the frame buffer memory usage will increase by several percent. This is because, ECC uses up memory to detect and correct the most common kinds of internal data corruption. Moreover, the driver may also reserve a small amount of memory for internal use, even without active work on the GPU; this too may impact frame buffer memory usage. For optimal graphics performance therefore, adequate frame buffer memory should be allocated to the VM/virtual desktop.
Virtual memory:	Indicates the virtual memory of this GPU device of this VM/virtual desktop.	MB	
GPU memory utilization:	Indicates the percentage of time over the past sample period during which memory on this GPU was read/written on by this VM/virtual desktop.	Percent	A value close to 100% is a cause for concern as it indicates that the graphics memory on a GPU is almost always in use. In a Shared vGPU environment, memory may be consumed all the time if one/more VMs/virtual desktops utilize the graphics memory excessively and constantly. If you find that only a single VM/virtual desktop has been consistently hogging the graphic memory resources, you may want to switch to the Dedicated GPU mode,

Measurement	Description	Measurement Unit	Interpretation
			so that excessive memory usage by that VM/virtual desktop has no impact on the performance of other VMs/virtual desktops on that host. If the value of this measure is high almost all the time for most of the GPUs, it could mean that the VM/virtual desktop is not sized with adequate graphics memory.
Total BAR1 memory:	Indicates the total size of the BAR1 memory of this GPU allocated to this VM/virtual desktop.	MiB	BAR1 is used to map the frame buffer (device memory) so that it can be directly accessed by the CPU or by 3rd party devices (peer-to-peer on the PCIe bus).
Used BAR1 memory:	Indicates the amount of BAR1 memory on this GPU that is being used by this VM/virtual desktop.	MiB	For better user experience with graphic applications, enough BAR1 memory should be available to the VM/virtual desktop.
Free BAR1 memory:	Indicates the total size of BAR1 memory of this GPU that is still not used by this VM/virtual desktop.	MiB	
BAR1 memory utilization:	Indicates the percentage of the allocated BAR1 memory that is currently being utilized by this VM/virtual desktop.	Percent	A value close to 100% is indicative of excessive usage of the BAR1 memory by a VM/virtual desktop. For best graphics performance, this value should be low. To ensure that, adequate BAR1 memory should be allocated to the VM.
Power management:	Indicates whether/not power management is		Many **NVIDIA** graphics cards support multiple performance levels

Measurement	Description	Measurement Unit	Interpretation
	enabled for this GPU of this VM/virtual desktop.		so that the server can save power when full graphics performance is not required. The default Power Management Mode of the graphics card is Adaptive. In this mode, the graphics card monitors GPU usage and seamlessly switches between modes based on the performance demands of the application. This allows the GPU to always use the minimum amount of power required to run a given application. This mode is recommended by NVIDIA for best overall balance of power and performance. If the power management mode is set to Adaptive, the value of this measure will be Supported. Alternatively, you can set the Power Management Mode to Maximum Performance. This mode allows users to maintain the card at its maximum performance level when 3D applications are running regardless of GPU usage. If the power management mode of a GPU is Maximum Performance, then the value of this measure will be Maximum. The numeric values that correspond to these measure values are discussed in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Supported</td><td>1</td></tr>
<tr><td>Maximum</td><td>0</td></tr>
</table>
Note:

By default, this measure will report the Measure Values listed in the table above to indicate the power management status. In the graph of this measure however, the same is represented using the numeric equivalents only.</td></tr>
<tr><td>Power limit:</td><td>Indicates the power limit configured for this GPU of this VM/virtual desktop.</td><td>Watts</td><td>This measure will report a value only if the value of the ‘Power management’ measure is ‘Supported’.

The power limit setting controls how much voltage a GPU can use when under load. Its not advisable to set the power limit at its maximum – i.e., the value of this measure should not be the same as the value of the Max power limit measure - as it can cause the GPU to behave strangely under duress.</td></tr>
<tr><td>Default power limit:</td><td>Indicates the default power management algorithm’s power ceiling for this GPU.</td><td>Watts</td><td>This measure will report a value only if the value of the ‘Power management’ measure is ‘Supported’.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Enforced power limit:	Indicates the power management algorithm's power ceiling for this GPU of this VM/virtual desktop.	Watts	**This measure will report a value only if the value of the 'Power management' measure is 'Supported'.** The total board power draw is manipulated by the power management algorithm such that it stays under the value reported by this measure.
Min power limit:	The minimum value that the power limit be set to for this GPU of this VM/virtual desktop.	Watts	**This measure will report a value only if the value of the 'Power management' measure is 'Supported'.**
Max power limit:	The maximum value that the power limit for this GPU of this VM/virtual desktop can be set to.	Watts	**This measure will report a value only if the value of the 'Power management' measure is 'Supported'.** If the value of this measure is the same as that of the Power limit measure, then the GPU may behave strangely.
Core clock:	Indicates current frequency of the graphics clock on this GPU of this VM/virtual desktop.	MHz	GPU has many more cores than your average CPU but these cores are much simpler and much smaller so that many more actually fit on a small piece of silicon. These smaller, simpler cores go by different names depending upon the tasks they perform. Stream processors are the cores that perform a single thread at a slow rate. But since GPUs contain

Measurement	Description	Measurement Unit	Interpretation
			numerous stream processors, they make overall computation high. The streaming multiprocessor clock is how fast the stream processors run. The memory clock is how fast the memory on the card runs. The GPU core clock is the speed at which the GPU assigned to the VM/virtual desktop operates. By correlating the frequencies of these clocks – i.e., the value of these measures - with the memory usage, power usage, and overall performance of the GPU, you can figure out if overclocking is required or not. Overclocking is the process of forcing a GPU core/memory to run faster than its manufactured frequency. Overclocking can have both positive and negative effects on GPU performance. For instance, memory overclocking helps on cards with low memory bandwidth, and with games with a lot of post-processing/textures/filters like AA that are VRAM intensive. On the other hand, speeding up the operation frequency of a shader/streaming processor/memory clock, without properly analyzing its need and its effects, may increase its thermal output in a linear fashion. At the same time, boosting voltages will cause the generated heat to sky rocket. If improperly managed, these increases in temperature can cause permanent physical damage to the core/memory or even “heat death”.

Measurement	Description	Measurement Unit	Interpretation
Memory clock:	Indicates current memory clock frequency on this GPU of this VM/virtual desktop.	MHz	
Streaming multiprocessor clock:	Indicates the current frequency of the streaming multiprocessor clock on this GPU of this VM/virtual desktop.	MHz	
Frame rate:	Indicates the rate at which frames are processed by this GPU of this VM/virtual desktop.	Frames/Sec	FPS is how fast your graphics card can output individual frames each second. It is the most time-tested and ideal measure of performance of a GPU. Higher the value of this measure, healthier is the GPU. This measure will be reported only if the 'Dedicated GPU' or 'GPU Pass-through' technology is used to deliver GPU resources to virtual desktops/VMs.
Fan speed:	Indicates the percent of maximum speed that this GPU's fan is currently intended to run at.	Percent	This measure will be reported only if the 'Dedicated GPU' or 'GPU Pass-through' technology is used to deliver GPU resources to virtual desktops/VMs. The value of this measure could range from 0 to 100%. An abnormally high value for this measure could indicate a problem condition – eg., a sudden surge in the temperature of the GPU that

Measurement	Description	Measurement Unit	Interpretation
			could cause the fan to spin faster. Note that the reported speed is only the intended fan speed. If the fan is physically blocked and unable to spin, this output will not match the actual fan speed. Many parts do not report fan speeds because they rely on cooling via fans in the surrounding enclosure. By default the fan speed is increased or decreased automatically in response to changes in temperature.
Compute processes:	Indicates the number of processes having compute context on this GPU of this VM.	Number	Use the detailed diagnosis of this measure to know which processes are currently using the GPU. The process details provided as part of the detailed diagnosis include, the PID of the process, the process name, and the GPU memory used by the process. Note that the GPU memory usage of the processes will not be available in the detailed diagnosis, if the Windows platform on which XenApp operates is running in the WDDM mode. In this mode, the Windows KMD manages all the memory, and not the NVIDIA driver. Therefore, the NVIDIA SMI commands that the test uses to collect metrics will not be able to capture the GPU memory usage of the processes.
Volatile single bit errors:	Indicates the number of volatile single bit errors	Number	**This measure will be reported only if the 'Dedicated GPU' or**

Measurement	Description	Measurement Unit	Interpretation
	in this GPU of this VM/virtual desktop.		**'GPU Pass-through' technology is used to deliver GPU resources to virtual desktops/VMs**. Volatile error counters track the number of errors detected since the last driver load. Single bit ECC errors are automatically corrected by the hardware and do not result in data corruption. Ideally, the value of this measure should be 0.
Volatile double bit errors:	Indicates the total number of volatile double bit errors in this GPU of this VM/virtual desktop.	Number	**This measure will be reported only if the 'Dedicated GPU' or 'GPU Pass-through' technology is used to deliver GPU resources to virtual desktops/VMs**. Volatile error counters track the number of errors detected since the last driver load. Double bit errors are detected but not corrected. Ideally, the value of this measure should be 0.
Aggregate single bit errors:	Indicates the total number of aggregate single bit errors in this GPU of this VM/virtual desktop.	Number	**This measure will be reported only if the 'Dedicated GPU' or 'GPU Pass-through' technology is used to deliver GPU resources to virtual desktops/VMs**. Aggregate error counts persist indefinitely and thus act as a lifetime counter. Single bit ECC errors are automatically corrected by the hardware and do not result in data

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>corruption.

Ideally, the value of this measure should be 0.</td></tr>
<tr><td>Aggregate double bit errors:</td><td>Indicates the total number of aggregate double bit errors in this GPU of this VM/virtual desktop.</td><td>Number</td><td>This measure will be reported only if the ‘Dedicated GPU’ or ‘GPU Pass-through’ technology is used to deliver GPU resources to virtual desktops/VMs.

Aggregate error counts persist indefinitely and thus act as a lifetime counter. Double bit errors are detected but not corrected.

Ideally, the value of this measure should be 0.</td></tr>
<tr><td>Mode:</td><td>Indicates the mode using which the GPU resources were delivered to this VMs.</td><td></td><td>The values that this measure can take and their corresponding numeric values are as follows:
<table><tr><th>Measure Value</th><th>Numeric Values</th></tr><tr><td>Pass through</td><td>0</td></tr><tr><td>Shared</td><td>1</td></tr><tr><td>Unavailable (GPU card is not allocated to any VM)</td><td>2</td></tr></table>Note:

By default, this test reports the Measure Values listed in the table above to indicate the mode of GPU delivery. In the graph of this</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			measure however, the same is represented using the numeric equivalents only.
Physical GPU compute utilization:	Indicates the proportion of time over the past sample period during which one or more kernels were executing on the physical GPU of this VM/virtual desktop.	Percentage	**This measure will report metrics only for the Tesla GPU card.** A value close to 100% indicates that the physical GPU is busy processing graphic requests from this VM almost all the time. In a Shared vGPU environment a vGPU may be in use almost all the time, if the VM/virtual desktop it is allocated to run graphic- intensive applications. A resource- hungry VM/virtual desktop on a server can impact the performance of other VMs/virtual desktops on the same server. If you find that only a single VM/virtual desktop has been consistently hogging the GPU resources, you may want to switch to the Dedicated GPU mode, so that excessive GPU usage by that VM/virtual desktop has no impact on the performance of other VMs/virtual desktops on that host. If all GPUs assigned to a VM/virtual desktop are found to be busy most of the time, you may want to consider allocating more GPU resources to that VM/virtual desktop.

As stated earlier, by default, clicking on the **Inside view of VMs** layer of a managed Nutanix Acropolisserver, leads you to a page displaying the current status of the virtual guests executing on that server. If you want to override this default setting - i.e., if you prefer to view the tests mapped to the **Inside View of VMs** layer first, and then proceed to focus on individual guest performance, follow the steps given below:

- Edit the **eg_ui.ini** file in the **<EG_INSTALL_DIR>\manager\config** directory
- Set the **LAYERMODEL_LINK_TO_VIRTUAL** flag in the file to **false**; this is set to **true** by default.
- Save the **eg_ui.ini** file.

Doing so ensures that as soon as the **Inside View of VMs** layer is clicked, the list of tests mapped to that layer appears, as depicted by Figure 4.24.

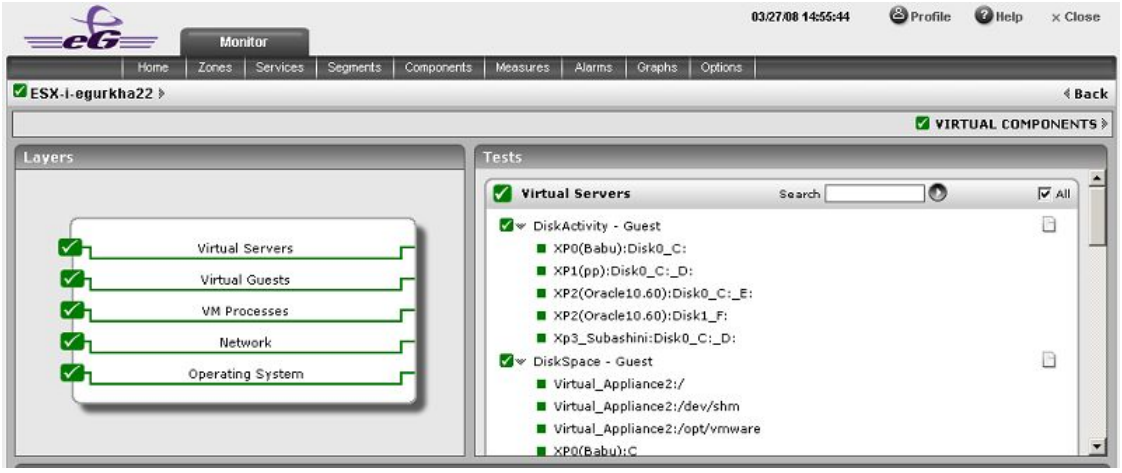


Figure 4.24: The tests mapped to the Inside View of VMs layer

If you now want the **Server view** of Figure 1, simply click on **SERVERS** link above the list of tests in Figure 4.24.

Clicking on any of the guests in the **Server view** leads you to Figure 4.25 that displays all the performance metrics extracted from that guest, in real-time. You are thus enabled to cross-correlate across the various metrics, and quickly detect the root-cause of current/probable disturbances to the internal health of a guest. To view the time-of-day variations in a measure, you can view its graph by clicking on that measure in Figure 4.25.

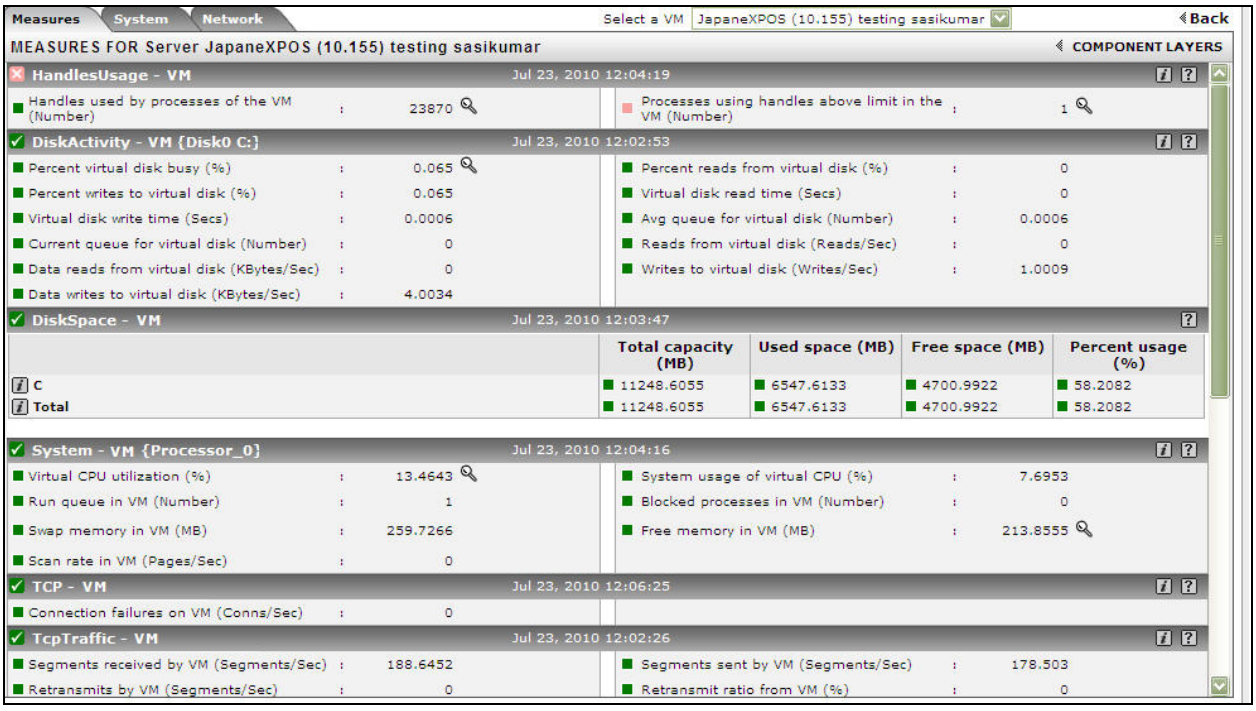


Figure 4.25: Measures pertaining to a chosen guest on a Nutanix Acropolis server

To view real-time graphs of pre-configured measures (pertaining to the Nutanix Acropolis server and the guests operating on it), click on the **LIVE GRAPH** link in Figure 1. Alternatively, you can click on the icon that appears in the **Tests** panel (see Figure 1) when the **Outside View of VMs** layer is clicked. The graph display that appears subsequently (see Figure 4.26) has been organized in such a way that next to every host-pertinent measure graph, the closely related guest-specific measure graph appears. This way, you can easily compare and correlate how well the physical CPU resources are being utilized by both the Nutanix Acropolis host and the guests. On the basis of this analysis, you can proactively isolate potential performance issues, and also determine the root-cause of the issue - is it the Nutanix Acropolis hypervisor? or is it the VM? If you access this page from the **LIVE GRAPH** link in Figure 1, then, by default, you will view live graphs pertaining to the Nutanix Acropolis server. However, you can select a different virtualized component-type and a different virtualized component using the **type** and **ComponentName** lists (respectively) in Figure 4.26.

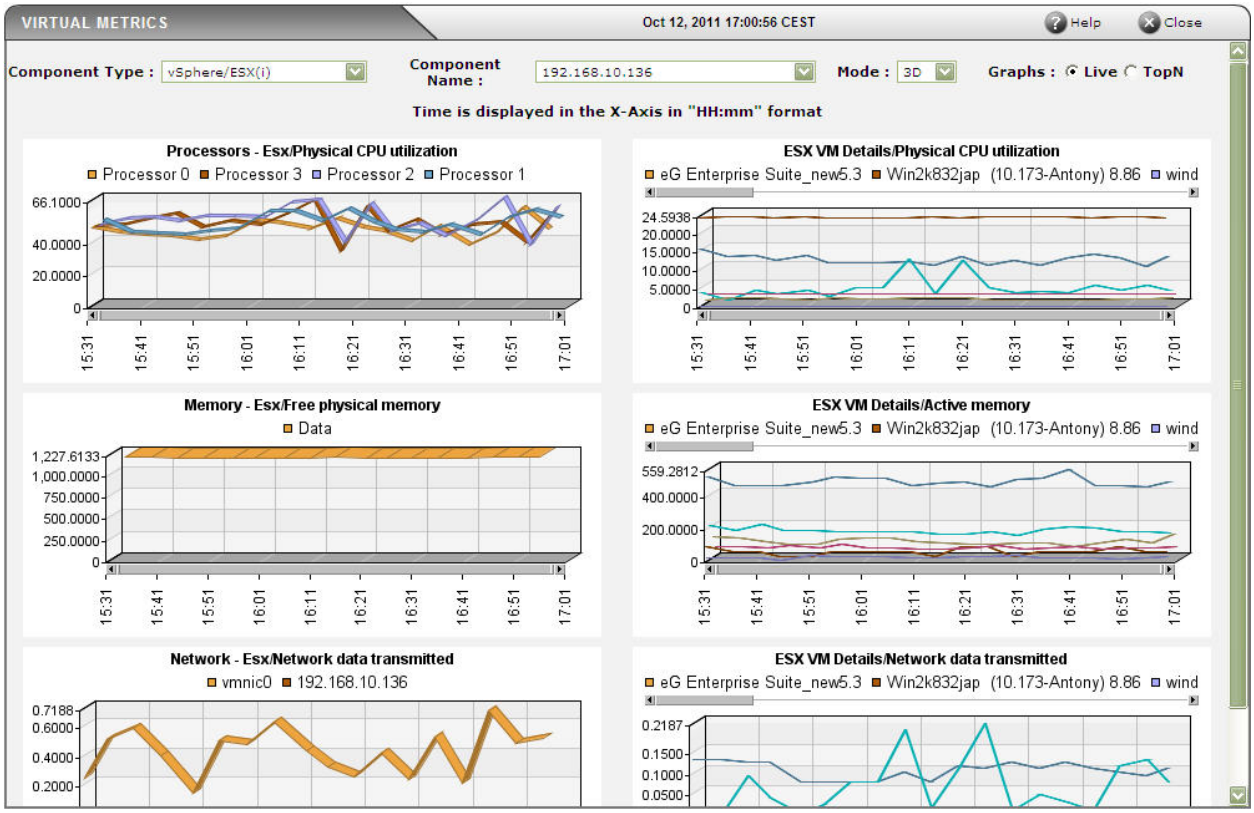


Figure 4.26: Live graph of the Nutanix Acropolis server

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

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

Note:

- For **AutoVirtualMapping** to work, the detailed diagnosis frequencies set globally (i.e., using the Configure -> Diagnosis menu sequence) should not be set to *0:0*.
- As long as the **Identify agents only using nick names** flag in the **MANAGER SETTINGS** page of the eG administrative interface (Configure -> Manager Settings menu sequence) is **Yes** (which is the default), eG Enterprise can automatically identify the server applications executing on a Nutanix Acropolis hypervisor, using the host/nick names that are mapped to the IP addresses discovered on the host. If the **Identify agents only using nick names** flag is set to **No** instead, then make sure that, while managing a server application executing in a virtualized environment, the hostname of the virtual machine is specified as the nick name of the corresponding server application. If more than one server application is executing on the same virtual machine, then any one of those server applications should have the virtual machine name as its nick name.

To disable auto-discovery, set this value to **false.** In such a case, once a Nutanix Acropolis server is added, then, when adding any new server application using the eG administrative interface, you will be prompted to manually set an association between the server application being added and the Acropolis server. In the example depicted by Figure 4.27, the **VIRTUAL ENVIRONMENT** flag is set to **YES** indicating that the Oracle server is running on a guest operating system. The name of the virtual host on which the component is hosted is indicated in the **VIRTUAL SERVERS** selection.

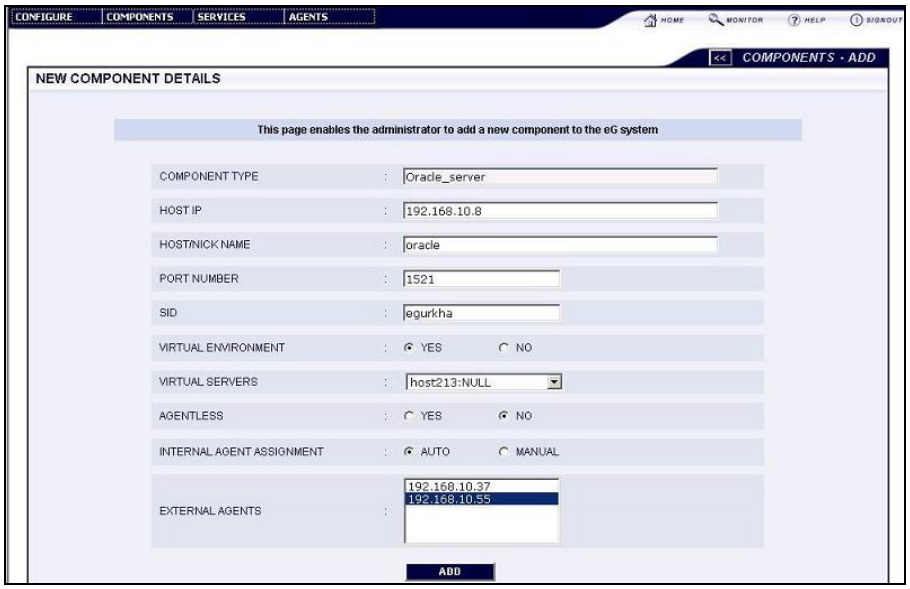


Figure 4.27: Adding a server application to a virtual environment

The mapping of applications to Acropolis servers is used by eG Enterprise for correlation - e.g., since the application runs on the Acropolis server, it is most likely that a problem with the Acropolis server will impact the performance of the application running on one of the guests. To view this application-Acropolis server association, simply click on the **VIRTUAL COMPONENTS** link in Figure 4.24.

Note:

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

Doing so reveals Figure 4.28 depicting the Acropolis server and the server applications executing on it. By clicking on any of the components in Figure 4.28, the user can drill down into specific layers of this component for specific details on the performance of the component.

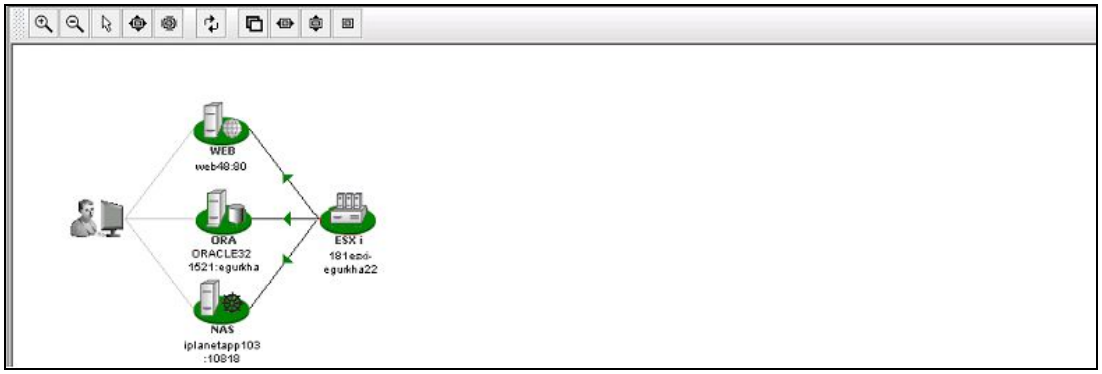


Figure 4.28: Depicts the applications that have been deployed on the guest OS of an Acropolis server

The arrows in Figure 4.28 depict the dependencies between the Acropolis host and the applications running on it. Since the applications are hosted on one of the guests running on the Acropolis host, they depend on the Acropolis host - i.e., any unusual resource usage on the Acropolis host impacts the applications running on any of the virtual guests. The dependency information between the Acropolis host and the applications hosted on it is used by eG Enterprise for end-to-end correlation.

4.4.7 Network Traffic - VM Test

This is an internal test that monitors the incoming and outgoing traffic through each Linux guest on a Nutanix Acropolis server.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every *Linux virtual_ guest:network_ interface* combination.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to theSection **Chapter 3** topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page.

Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.
11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.7**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will

report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	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).

4.4.8 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 : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on guest/currently logged-in user on the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.8**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **SEGMENTS SENT MIN** - Specify the minimum threshold for the number of segments sent/transmitted over the network. The default value is 10; in this case, the test will compute/report the *Retransmit ratio from VM* measure only if more than 10 segments are sent over the network – i.e., if the value of the *Segments sent by VM* measure crosses the value 10. On the other hand, if the *Segments sent by VM* measure reports a value less than 10, then the test will not compute/report the *Retransmit ratio from VM* measure. This is done to ensure that no false alerts are generated by the eG Enterprise system for the *Retransmit ratio from* VM measure. You can change this minimum threshold to any value of your choice.

Measurements made by the test

Measurement	Description	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:	Indicates the ratio of the rate of data retransmissions to the rate of data being sent by the guest	Percent	Ideally, the retransmission ratio should be low (< 5%). Most often retransmissions at the TCP layer have significant impact on application performance. Very often a large number of retransmissions are caused by a

Measurement	Description	Measurement Unit	Interpretation
			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.

4.4.9 Tcp - VM Test

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

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on guest/logged-in user on the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the

PRISM USER and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to

Yes by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.9**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	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:	Indicates the currently established connections.	Number	A sudden increase in the number of connections established on a guest can indicate either an increase in load to one or more of the applications executing on the guest, or that one or more of the applications are experiencing a problem (e.g., a slow down). On Microsoft Windows, the current connections metrics is the total number of TCP connections that are currently in the *ESTABLISHED* or *CLOSE_WAIT* states.
Connection drops 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

Measurement	Description	Measurement Unit	Interpretation
			connections being dropped without completion.

4.4.10 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 a Nutanix Acropolis server.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each guest discovered on the Nutanix Acropolis 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that

you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port

9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.10**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **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 on which the

remote agent is running - for agentless monitoring).

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	Description	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,

Measurement	Description	Measurement Unit	Interpretation
			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 - VM 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.
- For VMs running Windows 8 (or above), the Uptime - VM test may sometimes report incorrect values. This is because of the 'Fast Startup' feature, which is enabled by default for Windows 8 (and above) operating systems. This feature ensures that the Windows operating system is NOT SHUTDOWN COMPLETELY, when the VM is shutdown. Instead, the operating system saves the image of the Windows kernel and loaded drivers to the file, C:\hiberfil.sys, upon shutdown. When the Windows VM is later started, the operating system simply loads hiberfil.sys into memory to resume operations, instead of performing a clean start. Because of this, the Windows system will not record this event as an actual 'reboot'. As a result, the Uptime - VM test will not be able to correctly report if any reboot happened recently ; neither will it be able to accurately compute the time since the last reboot.

To avoid this, you need to disable the Fast Startup feature on VMs running Windows 8 (and above). The steps to achieve this are outlined below:

1. Login to the target Windows VM.
2. Edit the Windows Registry. Look for the following registry entry:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Power

3. Locate the **HiberbootEnabled** key under the entry mentioned above.
4. Change the value of this key to *0* to turn off Fast Startup. By default, its value will be *1*, as Fast Startup is enabled by default.

   Also, note that the Fast Startup feature does not work if the VM is "restarted"; it works only when the VM is shutdown and then started.

4.4.11 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 nonpaged pool and a paged pool. The nonpaged pool is a section of memory that cannot, under any circumstances, be paged to disk. The paged pool is a section of memory that can be paged to disk. (Just being stored in the paged pool doesn't necessarily mean that something has been paged to disk. It just means that it has either been paged to disk or it could be paged to disk.) Sandwiched directly in between the nonpaged and paged pools (although technically part of the nonpaged pool) is a section of memory called the "System Page Table Entries," or "System PTEs." The **Windows Memory - VM** test tracks critical metrics corresponding to the System PTEs and the pool areas of kernel memory of a Windows virtual machine.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Nutanix Acropolis* as the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every Windows VM guest/user on the monitored Nutanix Acropolis server.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were

added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.11**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user

who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	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	A hard page fault occurs when a program requests a data which is not in physical memory. In this case, the operating system finds the specific data on disk and restores it to the physical memory. By tracking the variations to this

Measurement	Description	Measurement Unit	Interpretation
			measure over time, you can keep tabs on hard page faults.
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 a piece of memory that was not in its working set, meaning that the guest had to retrieve it from the page file.	Pages/Sec	
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

Measurement	Description	Measurement Unit	Interpretation
			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.

4.4.12 Windows Network Traffic - VM Test

This is an internal test that monitors the incoming and outgoing traffic through each Windows guest of a Nutanix Acropolis host.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every *Windows_virtual_guest:network_interface* combination or *Windows_VM_guest_user:network_interface* combination

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.12**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	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:	Indicates the length of the output packet queue (in packets)	Number	If this is longer than 2, delays are being 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	Number	Ideally, number of inbound errors should be 0.

Measurement	Description	Measurement Unit	Interpretation
	errors preventing them from being deliverable to a higher-layer protocol.		

If the WindowsNetTraffic - VM test is not reporting measures for a VM, make sure that you have enabled the SNMP service for the VM.

4.4.13 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 : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each powered-on guest/currently logged-in user on the Nutanix Acropolis server 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current

Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the

Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.13**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.
16. **IGNORESERVICES** - Provide a comma-separated list of services that need to be ignored while monitoring. When configuring a service name to exclude, make sure that you specify the **Display Name** of the service, and not the service **Name** you see in the **Services** window on your Windows VM.
17. **TOTAL AUTO SERVICES STARTED DD** – By default, this flag is set to **No**. Accordingly, this test, by default, will not report detailed diagnostics for the *Total automatic services started* measure. To view the list of services with startup type as 'Automatic', which are in the 'Started' state in

each of the Windows VMs of the vSphere host, set this flag to **Yes**.

18. **TOTAL MANUAL SERVICES STARTED DD** - By default, this flag is set to **NO**. Accordingly, this test, by default, will not report detailed diagnostics for the *Total manual services started* measure. To view the list of services with startup type as 'Manual', which are in the 'Started' state in each of the Windows VMs of the vSphere host, set this flag to **Yes**.
19. **TOTAL MANUAL SERVICES STOPPED DD** - By default, this flag is set to **No**. Accordingly, this test, by default, will not report detailed diagnostics for the *Total manual services stopped* measure. To view the list of services with startup type 'Manual', which are in the 'Stopped' state in each of the Windows VMs of the vSphere host, set this flag to **Yes**.
20. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a *Nutanix Acropolis* server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.
21. **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	Description	Measurement Unit	Interpretation
New automatic services started:	Indicates the number of Windows services with startup type as *automatic*, which were running in the last measurement period.	Number	The detailed diagnosis of this measure lists the services (with startup type as *1*) that are running.

Measurement	Description	Measurement Unit	Interpretation
New automatic services stopped:	Indicates the number of Windows services with startup type as *automatic*, which were not running in the last measurement period.	Number	To know which services stopped, use the detailed diagnosis of this measure (if enabled).
New manual services started:	Indicates the number of Windows services with startup type as *manual*, which were running in the last measurement period.	Number	Use the detailed diagnosis of this measure to identify the *manual* services that are running.
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.
Total automatic services stopped:	Indicates the total number of Windows services with startup type as *automatic*, which are not running in this VM presently.	Number	To identify the services that stopped, use the detailed diagnosis of this measure.
Total automatic services started:	Indicates the total number of Windows services with startup type as *automatic*, which are running in this VM currently.	Number	If the **TOTAL AUTO SERVICES STARTED DD** flag is set to **Yes**, then the test will report detailed diagnostics for this measure. The detailed diagnosis will reveal the names of the services with startup type as automatic, which are running in the VM now.
Total manual services stopped:	Indicates the total number of Windows	Number	If the **TOTAL MANUAL SERVICES STOPPED DD** flag is set to **Yes**, then

Measurement	Description	Measurement Unit	Interpretation
	services with startup type as *manual*, which are not running in this VM presently.		the test will report detailed diagnostics for this measure. The detailed diagnosis will reveal the names of the services with startup type as *manual*, which are not running in the VM now.
Total manual services started:	Indicates the total number of Windows services with startup type as *manual*, which are not running in this VM presently.	Number	If the **TOTAL MANUAL SERVICES STARTED DD** flag is set to **Yes**, then the test will report detailed diagnostics for this measure. The detailed diagnosis will reveal the names of the services with startup type as *manual*, which are running in the VM now.

4.4.14 Crash Details - VM Test

Event logs on Windows VMs capture critical error conditions such as service crashes and application crashes on the VMs, application and service hangs, and service errors. Since the crash/slowness experienced by any mission-critical program/service on a Windows VM may affect the uptime of the dependent business services, administrators should be able to instantly capture these serious problem conditions, investigate the reasons for their occurrence, and promptly resolve them. This is exactly what the **Crash Details -VM** test helps administrators achieve! This test periodically scans the event logs on each Windows VM and reports the count of crashes, hangs, and errors that may have occurred recently on that VM. Detailed diagnostics provided by this test pinpoints the applications/services that crashed, hanged, or encountered errors, and thus enables quick and efficient troubleshooting.

Note:

This test will not report metrics on VMs running Windows 2000/2003/XP.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every Windows VM on the Nutanix Acropolis 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that vCenter server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were

added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **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. To know how to use the special page, refer to Section **4.4.14**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user

who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

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	Description	Measurement Unit	Interpretation
Recent application crashes	Indicates the number of application crash events that occurred on this VM during the last measurement period.	Number	An event with the ID 1000 is logged in the event log every time a program terminates unexpectedly on a virtual desktop. This measure reports the number of events in the event log with event ID 1000.

Measurement	Description	Measurement Unit	Interpretation
			Use the detailed diagnosis of this measure to know which programs and modules stopped suddenly.
Recent service crashes	Indicates the number of service crash events that occurred on thisVM during the last measurement period.	Number	An event with the ID 7031 is logged in the Service Control Manager every time a service terminates ungracefully. This measure reports the number of events in the event log with event ID 7031. Use the detailed diagnosis of this measure to know the complete details of such events.
Recent application hangs	Indicates the number of application hang events that occurred on this VM during the last measurement period.	Number	An event with the ID 1002 is logged in the Application Event Log every time an application hangs. This measure reports the number of events in the event log with event ID 1002. Use the detailed diagnosis of this measure to know the complete details of the recent application hang events.
Recent service hangs	Indicates the number of service hang events that occurred on this VM during the last measurement period.	Number	An event with the ID 7022 is logged in the Service Control Manager every time a service hangs. This measure reports the number of events in the event log with event ID 7022. Use the detailed diagnosis of this measure to know the complete details of the recent service hang events.

Measurement	Description	Measurement Unit	Interpretation
Recent service errors	Indicates the number of service errors that occurred on this VM during the last measurement period.	Number	Events with the ID 7023, 7024, and 7026 are logged in the Service Control Manager every time a service error occurs. This measure reports the number of events in the event log with the aforesaid event IDs. Use the detailed diagnosis of this measure to know the complete details of the recent service errors.

4.4.15 Page File - VM Test

When the load imposed by applications and services running on a server nears the amount of installed RAM, additional storage is necessary. The page file serves as the temporary store on disk for memory that cannot be accommodated in the physical RAM. Since it is frequently accessed for storing and retrieving data that is needed for virtual memory access by application, the location and sizing of the page files can have a critical impact on server's performance. Ideally, the server operating system and the page file should be available on different drives for optimal performance. Splitting the page file across different drives can improve performance further.

A rule of thumb in sizing the page file is to set the maximum size of the page file to 1.5 times the available RAM. While this works well for systems with smaller physical memory, for other systems, the optimal page file size has to be determined based on experience using the system and studying the typical workload.

This test tracks the usage of each of the page files on a Windows VM. Note that this test is available for VMs running on Windows servers only.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Nutanix Acropolis/ Nutanix Acropolis-VDI* as the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis/ Nutanix Acropolis-VDI server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each page file on the Nutanix Acropolis 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were

added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **REPORTTOTAL** - Set this flag to **Yes** if you want the test to report total page file usage - i.e., the aggregate usage across multiple page files. In this case therefore, a **Total** descriptor will newly appear for this test in the eG monitoring console.
10. **REPORTTOTALONLY** - If both the **REPORTTOTAL** and **REPORTTOTALONLY** flags are set to **Yes**, then the test will report only the aggregate usage across multiple page files - in other words, the test will report values for the **Total** descriptor only. Likewise, if the **REPORTTOTAL** flag is set to **No**, and the **REPORTTOTALONLY** flag is set to **Yes**, then again, the test will report current usage for the **Total** descriptor only. However, if both the **REPORTTOTAL** and **REPORTTOTALONLY** flags are set to **No**, then the test will report individual usages only. Also, if the **REPORTTOTAL** flag is set to **Yes** and the **REPORTTOTALONLY** flag is set to **No**, then both the individual and Total usages will be reported.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current usage	Indicates the current usage of a page file.	Percent	This metric should be less than 90%. If the page file does not have additional space, additional

Measurement	Description	Measurement Unit	Interpretation
			users/processes cannot be supported and system performance will suffer. To improve performance, consider resizing the page file. Microsoft Windows allows a minimum and maximum size of the page file to be specified. If the system has sufficient disk space, consider setting the page file to start out at the maximum size (by using the same value for the minimum and maximum sizes), so that system resources are not spent growing the page file size when there is a virtual memory shortage.

4.4.16 Windows Security Center Status - VM Test

Windows Security Center (WSC) is a comprehensive reporting tool that helps administrators establish and maintain a protective security layer around Windows VMs to monitor the VM's health state. The Windows Security Center also monitors third party security products such as firewall, antivirus, antimalware and antispyware, installed on the VM. In order for the security products to be compliant with Windows and successfully report status to Action Center, these products should be registered with the security center. The security products communicate any subsequent status changes to the security center using private APIs. The security center, in turn, communicates these updates to Action Center, where they are finally displayed to the end user. With Windows Security Center, administrators can check whether any security product is installed and turned on, and if the definitions of the products are up to date and real-time protection is enabled. By continuously monitoring the Windows Security Center, administrators can instantly find out whether the security products are up-to-date or out dated, and the status of security products in real-time. This is what exactly the **Windows Security Center Status - VM** test does!

This test auto-discovers the security products installed on the Windsows VMs on the target host, and for each security product reports the current definition status and the current protection status. Using these details, administrators are alerted to the systems on which the automatic updates are outdated

and virus protection turned off. By closely monitoring the status, administrators can take necessary actions before the end users become vulnerable to virus threats or malicious attacks.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Nutanix Acropolis/ Nutanix Acropolis-VDI* as the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis/ Nutanix Acropolis-VDI server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every *security product:provider combination* on each Windows VMs on the target server.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to theSection **Chapter 3** topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Section **Chapter 3** topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access

this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **4.4.16**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Signature status</td><td>Indicates the current status of this security product.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>25</td></tr><tr><td>Up to date</td><td>15</td></tr><tr><td>Out of date</td><td>10</td></tr></table>Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current state of this security product. The graph of this measure however, represents the status of a server using the numeric equivalents only.
Use the detailed diagnosis of this measure, to know about the name of Windows system on which the product is running, the file paths of product executables and the current status of the product.</td></tr>
<tr><td>Real- time protection status</td><td>Indicates the real- time protection status of this security product.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>25</td></tr><tr><td>Snoozed</td><td>20</td></tr><tr><td>On</td><td>15</td></tr><tr><td>Expired</td><td>10</td></tr><tr><td>Off</td><td>0</td></tr></table> **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current protection status of this security product. The graph of this measure however, represents the status of a server using the numeric equivalents only.

Chapter 5: Monitoring the Nutanix Acropolis VDI

In some environments, the virtual guests hosted on Nutanix Acropolis servers may be used to support desktop applications. Administrators of such virtual environments would want to know the following:

- How many desktops are powered on simultaneously on the Acropolis Server?
- Which users are logged on and when did each user login?
- How much CPU, memory, disk and network resources is each desktop taking?
- What is the typical duration of a user session?
- Who has the peak usage times?
- What applications are running on each desktop?
- Which Acropolis server is a virtual guest running on?
- When was a guest moved from an Acropolis server? Which Acropolis server was the guest moved to?
- Why was the guest migrated? What activities on the Acropolis server caused the migration?

Using the *Nutanix Acropolis VDI* model (see Chapter 5), administrators can find quick and accurate answers to all the queries above, and also receive a complete 'desktop view', which allows them to get up, close with the performance of every guest OS hosted by the Acropolis server and detect anomalies (if any) in its functioning.

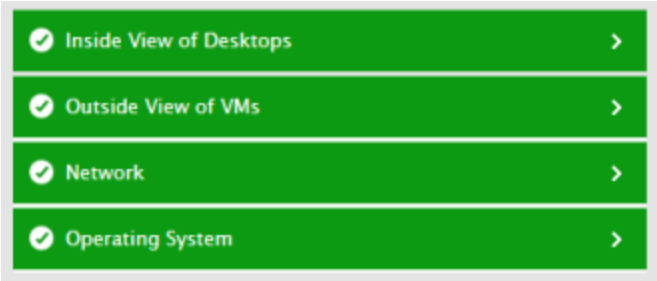


Figure 5.1: Layer model of the Nutanix Acropolis VDI server

Since the tests mapped to the **Operating System** and **Network** layer of Figure 1 are already discussed in the previous chapter, this chapter will discuss the top 2 layers alone.

5.1 The Outside View of VMs Layer

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

- Determine which of the virtual desktops 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 virtual desktops is receiving a very high rate of requests compared to the others, this guest may be a candidate for migration to another Acropolis server, so as to minimize the impact it has on the other guests on the current Acropolis 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.

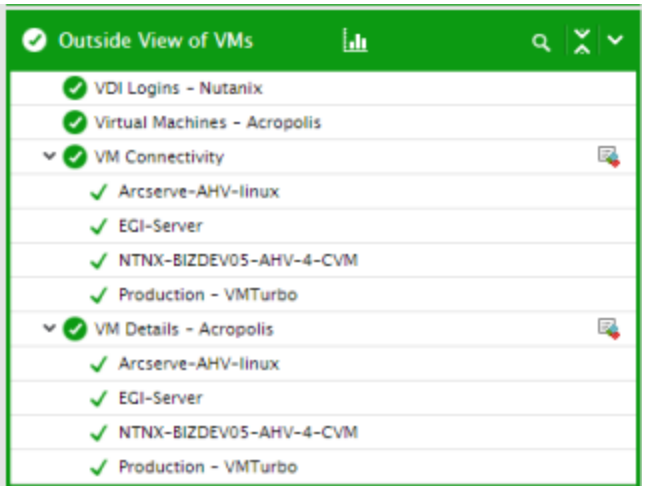


Figure 5.2: The tests mapped to the Outside View of VMs layer

5.1.1 VDI Logins Test

This test monitors the user logins to guests and reports the total count of logins and logouts.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Nutanix Acropolis hypervisor 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.1.1**.
- **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. **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	Description	Measurement Unit	Interpretation
Current sessions:	Indicates the number of user sessions that are currently active across all guests.	Number	This is a good indicator of the session load on the guests.
New logins:	Indicates the number of new logins to the guests.	Number	A consistent zero value could indicate a connection issue. Use the detailed diagnosis of this measure to know which users logged in newly.
Percent new logins:	Indicates the percentage of current sessions that logged in during the last measurement period.	Percent	
Sessions logging out:	Indicates the number of sessions that logged out.	Number	If all the current sessions suddenly log out, it indicates a problem condition that requires investigation. The detailed diagnosis of this measure lists the sessions that logged out.

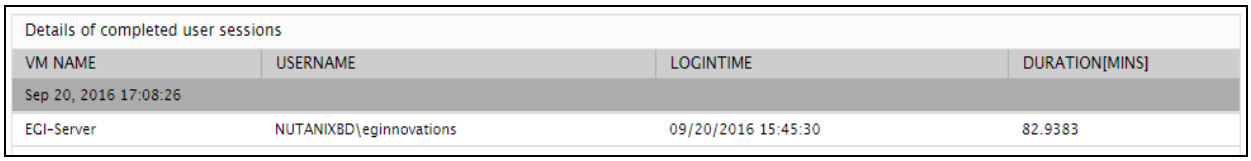
The detailed diagnosis of the New logins measure reveals the users who recently logged in, the VM each user logged into, and when they logged in.

Details of current user sessions

VM NAME	USERNAME	LOGINTIME
Sep 20, 2016 15:45:30		
EGI-Server	NUTANIXBD\eginnovations	09/20/2016 15:45:30

Figure 5.3: The detailed diagnosis of the New logins measure

The detailed diagnosis of the Sessions logging out measure reveals the users who suddenly logged out, the VM each user logged into, and when they logged in. The duration of the login is also reported as part of the detailed diagnostics. Using this information, you will be able to identify those users



Details of completed user sessions

VM NAME	USERNAME	LOGINTIME	DURATION[MINS]
Sep 20, 2016 17:08:26			
EGI-Server	NUTANIXBD\eginnovations	09/20/2016 15:45:30	82.9383

Figure 5.4: The detailed diagnosis of the Sessions logging out measure

5.1.2 VDI Applications Test

This test discovers the applications executing on the virtual desktops and reports the availability and resource-usage of each of the desktop applications.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of outputs for every distinct application executing on the virtual desktops.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-

configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor

some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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. Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.1.2**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.
16. **IS_SHOW_ALL_APPS** - To ensure that the test monitors only specific applications executing on the desktops and not all of them, set the **IS_SHOW_ALL_APPS** flag to **No**. Once this is done, then, you need to configure those applications that you want to exclude from the monitoring scope of this test. For this purpose, follow the steps given below:

    - Edit the **eg_tests.ini** file (in the {**EG_INSTALL_DIR}\manager\config** directory).
    - In the **[EXCLUDE_APPLICATIONS]** section of the file, you will find an entry of the

following format:

VmgApplicationTest={Comma-separated list of applications to be excluded}

- To the comma-separated application list that pre-exists, append the applications that you want to monitor. For instance, if your test need not monitor *notepad.exe*, and *powerpnt.exe*, then, your entry should be:

  VmgApplicationTest=.....,notepad.exe,powerpnt.exe

- Note that the exact application names should be provided, but the extensions (for instance, .exe) can be dispensed with.
- Finally, save the file.

On the other hand, if you want to monitor all the applications, then, set the **IS_SHOW_ALL_APPS** flag to **Yes**.

17. **SHOW USER APPS ONLY** – By default, this flag is set to **Yes**. Accordingly, this test will monitor only those applications/processes that are running in the user's account. To monitor all applications/processes running in the virtual desktops, regardless of the user account using which they are running, set this flag to **No**.

18. **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.

Since the remaining tests mapped to the **Outside View of VMs** layer - namely, the **VM Connectivity** test and **VM Datastores** test - have been discussed already, let us move to the **Virtual Desktop** layer.

5.2 The Inside View of Desktops Layer

The **Outside View of VMs** layer provides an "external" view of the different VM guests - the metrics reported at this layer are based on what the VMware host is seeing about the performance of the

individual guests. However, an external 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 mapped to the **Inside View of Desktopa** layer provide an "internal" 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.

By default however, clicking on the **Inside View of Virtual Desktop** layer, does not list the associated tests. Instead, Figure 5.5 appears, which displays the current state of all virtual desktops that have been configured on the monitored Acropolis server.

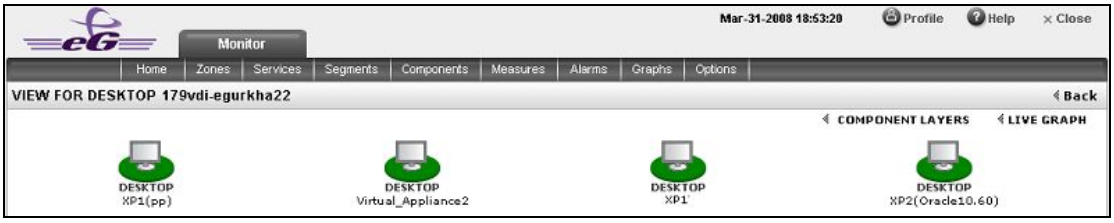


Figure 5.5: The current state of the desktops configured on the Nutanix Acropolis server host that is monitored

To return to the layer model of the *VMware VDI* server and view the tests mapped to the **Inside View of Desktops** layer, click on the **COMPONENT LAYERS** link in Figure 5.5. The tests depicted by Figure 5.6 then appears.

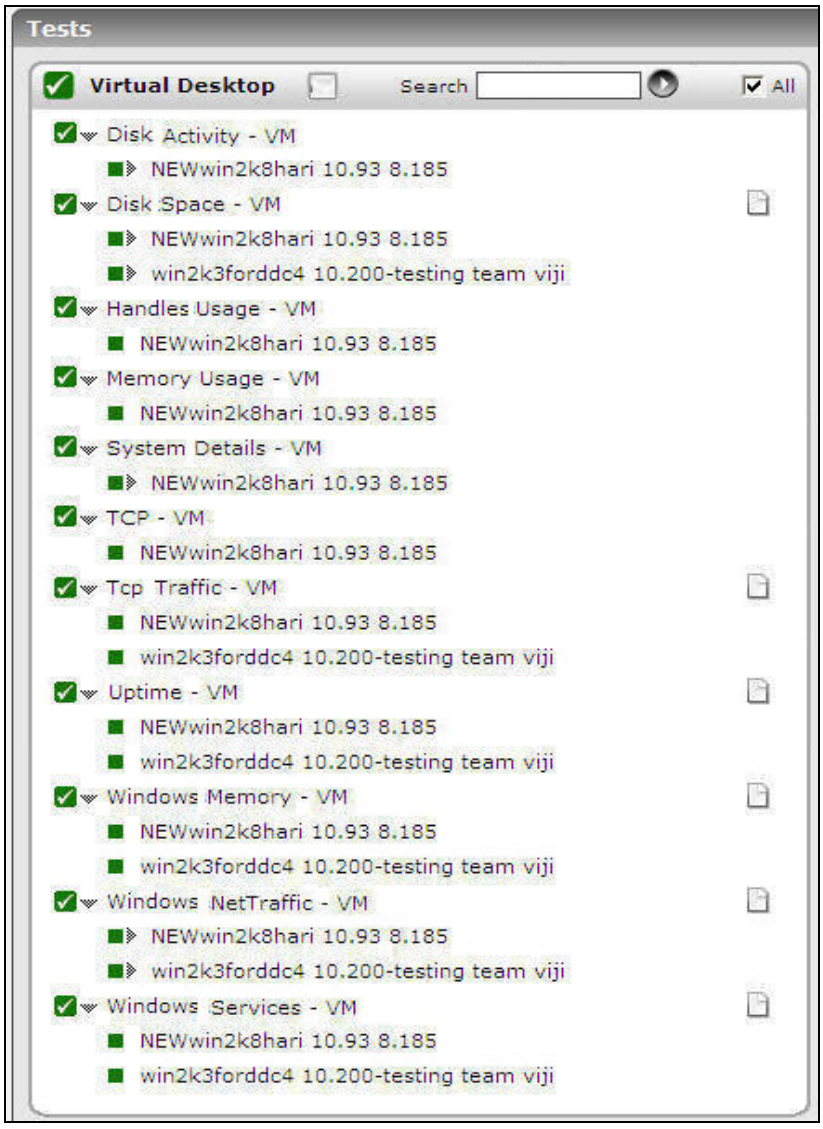


Figure 5.6: The tests associated with the Virtual Desktop layer of a VMware vSphere VDI

Almost all the tests depicted by Figure 5.6 have already been dealt with in the Monitoring the *Nutanix Acropolis* server monitoring model. The two tests that are specific to the *Nutanix Acropolis VDIr* model are the following:

- Browser Activity - VM Test
- Virtual Desktop Sessions DetailsTest
- Virtual Desktop Session Startup Details Test
- User Profile Management - VM Test
- Personal vDisk - VM Test

- PCoIP Session - VM Test
- Domain Time Sync - VM Test

5.2.1 Virtual Desktop Session Start-up Details Test

Figure 5.7 depicts a typical user logon process to a virtual desktop via XenDesktop broker.

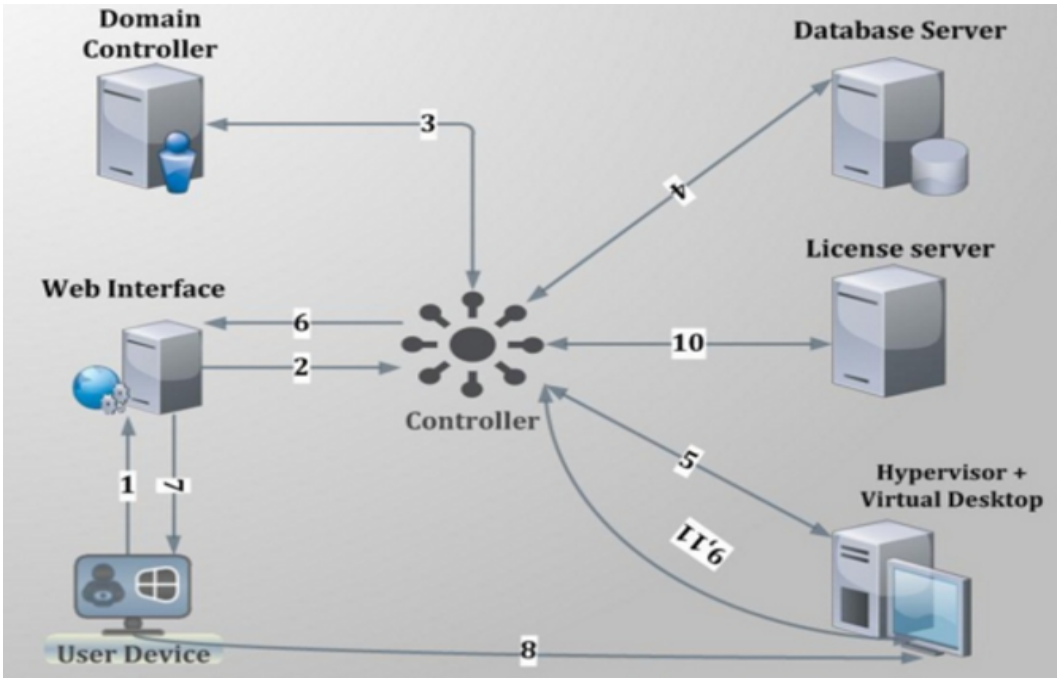


Figure 5.7: Citrix user logon process

The process depicted by Figure 5.7 above has been described below:

1. User provides his/her credentials to the web interface.
2. Web interface forwards the credentials to controller for verification process.
3. Delivery controller transfers these credentials to the domain controller to check if the user is present in the active directory.
4. Once it gets the successful confirmation from AD then controller communicates with site database to check what type of virtual desktop is available for current user.
5. Controller then interacts with the hypervisor layer to gather information about the availability of virtual desktop.

6. Controller then passes the ICA file for user and all the connection information is present inside ICA file so that client can establish the connection.
7. After all the process is complete, the user is assigned the virtual desktop.
8. The user then establishes a connection with the assigned virtual desktop.
9. The virtual desktop again communicates with controller for verification of licensing.
10. Controller checks for license from license server about what type of license is available for user in this current session. License server then communicates back with controller providing the licensing information.
11. Information obtained from license server is then passed to the virtual desktop.

From the discussion above, it can be inferred that login processing happens at two different places – at the delivery controller, and inside the virtual desktop. While login, authentication, and application brokering happen on the delivery controller, session creation and setup happens inside the virtual desktop. A problem in any of these places can result in a poor user experience. Inevitably, these issues result in service desk calls and complaints that "Citrix is slow." Diagnosing login problems has traditionally been a difficult, time-consuming, manual process due to the large number of steps involved. The key to resolving user experience issues therefore, lies in tracking each user's sessions end-to-end, ascertaining the time spent by the session at each step of the logon process – be it on the delivery controller or on the virtual desktop– and accurately identifying where and at what step of the logon process, the slowdown occurred.

To determine the time taken by the entire logon process of a user, isolate logon slowness, and understand where the process was bottlenecked – whether on the delivery controller or on the virtual desktop – use the **User Logon Performance** test mapped to the Citrix XA/XD Site component. If the **User Logon Performance** test reveals a problem in session start-up on the virtual desktop, then use the **Virtual Desktop Session Start-up Details** test.

With the **Virtual Desktop Session Start-up Details** test, administrators can receive deep visibility into the virtual desktop end of the Citrix logon process. This test takes an administrator into the virtual desktop, reveals the users who are currently logged on to the virtual desktop, and accurately reports the average time it took for the sessions of each user to start inside the virtual desktop. This way, administrators can rapidly identify which user's sessions are experiencing undue start-up delays.

In addition, the test also provides a break-up of the session start-up duration. This way, the test precisely pinpoints where the delay occurred - when user credentials were obtained? when credentials were validated? during profile loading? during login script execution? when mapping drives or creating printers?

For this purpose, the test categorizes its metrics into *client start-up metrics* and *server start-up metrics*.

The *client start-up metrics* are concerned with timing the operations that occur from the point when the user requests for access to a virtual desktop to the point at which a connection to the virtual desktop is established. While connection-brokering mechanisms involve components that are not on the physical client device, the tasks these systems perform have a direct impact on the performance of the connection start-up and are recorded as part of the client-side process.

The *server start-up metrics* are concerned with timing the operations that occur when creating a new session on the virtual desktop. This includes user authentication, client device mapping, profile loading, login scripts execution, and finally, starting the user's desktop.

Note:

This test will report metrics for only those users who are accessing virtual desktops via a XenDesktop broker.

Target of the test :A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every *user_on_VM*.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current

Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the

Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.2.1**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.
16. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.
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	Description	Measurement Unit	Interpretation
User sessions:	Indicates the number of sessions currently open for this user on this virtual desktop.	Number	Use the detailed diagnosis of this measure to view the complete details of this user's session. Such details includes the name and IP address of the client from which the session was launched, when session creation started, and when it ended. With the help of this information, administrators can quickly understand if the session took too long to get created.
Session start- up duration:	Indicates the time taken by this user to complete session start- up inside this virtual desktop.	Secs	Compare the value of this measure across users to know which user's sessions took the longest to start on the virtual desktop. To know what is causing this 'slowness', compare the values reported by all the other 'duration' measures of this test for that user on that virtual desktop. This will quickly lead you to where that user's session start-up is spending the maximum time.
Profile load duration:	Indicates the time taken to load this user's profile.	Secs	If the user's Session start- up

Measurement	Description	Measurement Unit	Interpretation
			duration is high, you may want to compare the value of this measure with that of the other 'duration' measures reported for this user to figure out if a delay in profile loading is what is really ailing that user's logon experience with this virtual desktop. One of the common reasons for high profile load time is the large size of the user profile.
Group policy processing duration:	Indicates the time taken by this user's session to process group policies.	Secs	If a user's Session start-up duration is high, you may want to compare the value of this measure with that of the other 'duration' measures reported for this user to figure out if a delay in group policy processing is what is really ailing that user's logon experience with this virtual desktop. In such a case, you can also use the detailed diagnosis of this measure to figure out the names of the group policy client-side extensions (CSE), the time each CSE took to run, the status of every CSE, and errors (if any) encountered by each CSE. Using these in- depth metrics, Citrix administrators can accurately pinpoint which CSE is impeding speedy group policy processing. Note: Detailed diagnostics will be

Measurement	Description	Measurement Unit	Interpretation
			available for this measure only if the eG VM Agent is deployed on the virtual desktops and the inside view using parameter of this test is set to eG VM Agent. Logon performance improves when fewer Group Policies are applied. Merge GPOs when possible instead of having multiple GPOs.
Login script execution duration:	Indicates the time taken for the login script to execute for this user.	Secs	If a user complains of slowness, then, you can compare the value of this measure with that of the other 'duration' measures of that user to figure out what could have really caused the slowness.
Start- up client duration:	This is the high- level client- side connection start-up metric. It starts at the time of the request (mouse click) and ends when the connection between this user's client device and the virtual desktop has been established.	Secs	When any user complains of slowness when trying to logon to a virtual desktop, you may want to compare the value of this measure with that of the Session start- up server duration measure of that user to know whether a client-side issue or a server- side issue is responsible for the slowness he/she is experiencing with that virtual desktop. If this comparison reveals that the Start-up client duration of the user is high, it indicates a client- side issue that is causing long start times. In this case therefore, compare the value of the client

Measurement	Description	Measurement Unit	Interpretation
			start-up metrics such as the Application enumeration client duration, Configuration file download client duration, Credentials obtention client duration, ICA file download client duration, Launch page web server duration, Name resolution client duration, Name resolution web server duration, Session look-up client duration, Session creation client duration, and Ticket response web server duration to know what client-side issue is causing the Start-up client duration to be high.
Back-up URL client count:	**This measure is relevant when the Citrix Receiver is the session launch mechanism**. It records the number of back-up URL retries before a successful launch. Note that this is the only start-up metric that is a measure of attempts, rather than time duration.	Number	If this metric has a value higher than 1, it indicates that the Web Interface server is unavailable and the Citrix Receiver is attempting to connect to back-up Web Interface servers to launch the virtual desktop. A value of 2 means that the main Web Interface server was unavailable, but the Citrix Receiver managed to launch the virtual desktop successfully using the first back-up server that it tried. A value higher than 2 means that multiple Web Interface servers are unavailable. Probable reasons for the non-availability of the Web Interface servers include (in order

Measurement	Description	Measurement Unit	Interpretation
			of likelihood): • Network issues between the client and the server. So the administrator should make sure that the Web Interface server is on the network and accessible to the clients. • An overloaded Web Interface server that is not responding (or has crashed for another reason). Try to log on to the server and check the Windows Performance Monitor/Task Manager to see how much memory is in use and so on. Also, review the Event Logs to see if Windows logged any serious errors.
Application enumeration client duration:	**This measure is relevant when the Citrix Receiver is the session launch mechanism** . It measures the time needed by this user's session to retrieve the list of applications from the Web Interface service.	Secs	If the Start- up client duration measure reports a high value for a user, then compare the value of this measure with that of the other client- side metrics such as Configuration file download client duration, Credentials obtention client duration, ICA file download client duration, Launch page web server duration, Name resolution client duration, Name resolution web server duration, Session look-up client duration, Session creation client duration, and Ticket response web server duration to know whether/not slowness in

Measurement	Description	Measurement Unit	Interpretation
			application enumeration is the precise reason why it took the user a long time to establish a session with the virtual desktop.
Configuration file download client duration:	**This measure is relevant when the Citrix Receiver is the session launch mechanism** . It measures the time this user's session took to retrieve the configuration file from the XML broker.	Secs	If the *Start- up client duration* measure reports a high value for a user, then compare the value of this measure with that of the other client- side metrics such as *Application enumeration client duration, Credentials obtention client duration, ICA file download client duration, Launch page web server duration, Name resolution client duration, Name resolution web server duration, Session look-up client duration, Session creation client duration* , and *Ticket response web server duration* to know whether/not slowness in retrieving the configuration file from the XML server is the precise reason why it took the user a long time an ICA session with the XenApp server.
Credentials obtention client duration:	**This measure is relevant when the Citrix Receiver is the session launch mechanism** . It measures the time required by this user's session to obtain the user credentials.		Note that COCD is only measured when the credentials are entered manually by the user. Because this metric may be artificially inflated if a user fails to provide credentials in a timely manner, it is subtracted from the Start-up client duration. However, in the event that the user manually inputs the credentials,

Measurement	Description	Measurement Unit	Interpretation
			and the value of this measure is higher than that of all the other client start-up metrics that this test reports, it is a clear indicator that any connection delay that the user may have experienced is owing to slowness in obtaining user credentials.
ICA file download duration:	**This measure is relevant when the Citrix Receiver is the session launch mechanism**. This is the time it takes for this user's client to download the ICA file from the web server.	Secs	The overall process here is: a. The user clicks on application icon. b. The user's browser requests the Web Interface launch page. c. The Web Interface launch page receives the request and starts to process the launch, communicating with the virtual desktop and potentially other components such as Secure Ticket Authority (STA). d. The Web Interface generates ICA file data. e. The Web Interface sends the ICA file data back to the user's browser. f. The browser passes ICA file data to the client. This measure represents the time it takes for the complete process (step 1 to 6). The measure stops counting time when the client receives the ICA file data.

Measurement	Description	Measurement Unit	Interpretation
			The Launch page web server duration measure on the other hand, covers the Web server portion of the process (that is, steps 3 and 4). If the ICA file download duration is high, but the Launch page web server duration is normal, it implies that the server-side processing of the launch was successful, but there were communication issues between the client device and the Web server. Often, this results from network trouble between the two machines, so investigate potential network issues first.
Launch page web server duration:	**This measure is relevant when the Web Interface is the session launch mechanism** . It measures the time needed by this user's session to process the launch page (launch. aspx) on the Web Interface server.	Secs	If the value of this measure is high, it indicates at a bottleneck on the Web Interface server. Possible causes include: • High load on the Web Interface server. Try to identify the cause of the slow down by checking the Internet Information Services (IIS) logs and monitoring tools, Task Manager, Performance Monitor and so on. • Web Interface is having issues communicating with the other components. Check to see if the network connection between Web Interface and virtual desktop is slow. If the Web

Measurement	Description	Measurement Unit	Interpretation
			server seems okay, consider reviewing the virtual desktop for problems.
Name resolution client duration:	This is the time it takes the XML service to resolve the name of a published application to an IP address.	Secs	This metric is collected when a client device directly queries the XML Broker to retrieve published application information stored in IMA. This measure is only gathered for new sessions since session sharing occurs during startup if a session already exists. When this metric is high, it indicates the XML Broker is taking a lot of time to resolve the name of a published application to an IP address. Possible causes include a problem on the client, issues with the XML Broker, such as the XML Broker being overloaded, a problem with the network link between the two, or a problem in IMA. Begin by evaluating traffic on the network and the XML Broker.
Name resolution web server duration:	**This measure is relevant when the Citrix Receiver is the session launch mechanism**. It is the time it takes the XML service to resolve the name of this virtual desktop to its IP address.	Secs	When this metric is high, there could be an issue with the Web Interface server or the Citrix Receiver, the XML Service, the network link between the two, or a problem in IMA. Like the *Name resolution client duration* measure, this metric indicates how long it takes the XML service to resolve the name of a

Measurement	Description	Measurement Unit	Interpretation
			virtual desktop to its IP address. However, this metric is collected when a Web Interface site is performing this process on behalf of a launch request it has received from either the Citrix Receiver or from a user clicking a Web Interface page icon.
Session look- up client duration:	Indicates the time this user's session takes to query every ICA session to host the requested published application.	MSecs	The check is performed on the client to determine whether the application launch request can be handled by an existing session. A different method is used depending on whether the session is new or shared.
Session creation client duration:	Indicates the new session creation time.	Secs	In the event of slowness, if the *Start-up client duration* of a user session is found to be higher than the *Session start- up server duration*, you may want to compare the value of this measure with all other client start-up measures to determine whether/not session creation is the process that is slowing down the application launch.
Ticket response web server duration:	**This measure is relevant when the Citrix Receiver or Web Interface is the desktop launch mechanism**. This is the time this user's sessions take to get a ticket (if required) from the STA	Secs	When this metric is high, it can indicate that the Secure Ticket Authority (STA) server or the XML Broker are overloaded.

Measurement	Description	Measurement Unit	Interpretation
	server or XML service.		
Reconnect enumeration client duration:	**This measure is relevant when the Citrix Receiver or Web Interface is the desktop launch mechanism**. This is the time it takes this user's client to get a list of reconnections.	Secs	Compare the value of this measure with that of other client start-up metrics for a user to know what is the actual cause for the client start-up delay.
Reconnect enumeration web server duration:	**This measure is relevant when the Citrix Receiver or Web Interface is the desktop launch mechanism**. This is the time it takes the Web Interface to get the list of reconnections for this user from the XML service.	Secs	Compare the value of this measure with that of other client start-up metrics for a user to know what is the actual cause for the client start-up delay.
Session start-up server duration:	This is the high-level server-side connection start-up metric. It includes the time spent on this virtual desktop to perform the entire start-up operation.	Secs	When this metric is high, it indicates that there is a server-side issue increasing session start times. To zero-in on this issue, compare the values of the server start-up metrics such as Session creation server duration, *Credentials obtention server duration, Program neighbourhood credentials obtention server duration, Credentials obtention network server duration, Credentials authentication server duration, Profile load server duration, Login*

Measurement	Description	Measurement Unit	Interpretation
			script execution server duration, Drive mapping server duration, Drive mapping server duration, and *Printer creation server duration.*
Session creation server duration:	Indicates the time spent by this virtual desktop in creating the session for this user.	Secs	This duration starts when the ICA client connection has been opened and ends when authentication begins. This should not be confused with '*Session start- up server duration*'.
Credentials obtention server duration:	Indicates the time taken by this virtual desktop to obtain the credentials of this user.	Secs	This time is only likely to be a significant if manual login is being used and the server- side credentials dialog is displayed (or if a legal notice is displayed before login commences). Because this metric may be artificially inflated if a user fails to provide credentials in a timely manner, it is not included in the *Session start- up server duration*. However, in the event that the user manually inputs the credentials, and the value of this measure is higher than that of all the other client start-up metrics that this test reports, it is a clear indicator that any connection delay that the user may have experienced is owing to slowness in obtaining user credentials.
Credentials obtentions network server duration:	Indicates the time spent by this virtual desktop performing network	Secs	This only applies to a Security Support Provider Interface login (a form of pass- through

Measurement	Description	Measurement Unit	Interpretation
	operations to obtain credentials for this user.		authentication where the client device is a member of the same domain as the server and Kerberos tickets are passed in place of manually entered credentials).
Program neighbourhood credentials obtention server duration:	Indicates the time needed for this virtual desktop to cause the Program Neighborhood instance running on the client ("Program Neighborhood Classic") to obtain this user's credentials.	Secs	As in the case of the Credentials obtention server duration metric, because this metric may be artificially inflated if a user fails to provide credentials in a timely manner, it is not included in the Session start-up server duration.
Credentials authentication server duration:	Indicates the time spent by this virtual desktop when authenticating the user's credentials against the authentication provider, which may be Kerberos, Active Directory® or a Security Support Provider Interface (SSPI).	Secs	Where server- side issues are causing user experience to deteriorate, you can compare the value of this measure with that of all the other server start- up metrics that this test reports – i.e., Session creation server duration, Credentials obtention server duration, Program neighbourhood credentials obtention server duration, Credentials obtention network server duration, Profile load server duration, Login script execution server duration, Drive mapping server duration, Drive mapping server duration, and Printer creation server duration – to know what is the root- cause of delays in server start-up.
Profile load server duration:	Indicates the time required by this virtual	Secs	If this metric is high, consider your

Measurement	Description	Measurement Unit	Interpretation
	desktop to load this user's profile.		Terminal Services profile configuration. Citrix Consulting has found that when customers have logon times greater than 20 seconds, in most cases, this can be attributed to poor profile and policy design. Roaming profile size and location contribute to slow session starts. When a user logs onto a session where Terminal Services roaming profiles and home folders are enabled, the roaming profile contents and access to that folder are mapped during logon, which takes additional resources. In some cases, this can consume significant amounts of the CPU usage. Consider using the Terminal Services home folders with redirected personal folders to mitigate this problem. In general, consider using Citrix Profile management to manage user profiles in Citrix environments. This tool also provides logging capabilities to help isolate profile issues. If you are using Citrix profile management and have slow logon times, check to see if your antivirus software is blocking the Citrix profile management tool.
Login script execution server	Indicates the time needed by this virtual	Secs	If the value of this measure is abnormally high for any user,

Measurement	Description	Measurement Unit	Interpretation
duration:	desktop to run this user's login script(s).		consider if you can streamline this user or group's login scripts. Also, consider if you can optimize any application compatibility scripts or use environment variables instead.
Drive mapping server duration:	Indicates the time needed for this virtual desktop to map this user's client drives, devices and ports.	Secs	Make sure that, when possible, your base policies include settings to disable unused virtual channels, such as audio or COM port mapping, to optimize the ICA protocol and improve overall session performance.
Printer creation server duration:	Indicates the time required for this virtual desktop to synchronously map this user's client printers.	Secs	If the configuration is set such that printer creation is performed asynchronously, no value is recorded for this measure as it is does not impact completion of the session start-up. On the other hand, if excessive time is spent mapping printers, it is often the result of the printer autocreation policy settings. The number of printers added locally on the users' client devices and your printing configuration can directly affect your session start times. When a session starts, the virtual desktop has to create every locally mapped printer on the client device. Consider reconfiguring your printing policies to reduce the number of printers that get created - especially if users have a lot of local printers.

As stated earlier, by default, clicking on the **Inside View of Virtual Desktops** layer, leads you to a page displaying the current status of the individual desktops that have been configured on the Nutanix Acropolis server. If you want to override this default setting - i.e., if you prefer to view the tests mapped to the **Inside View of Virtual Desktops** layer first, and then proceed to focus on individual desktop performance, follow the steps given below:

- Edit the **eg_ui.ini** file in the **<EG_INSTALL_DIR>\manager\config** directory
- Set the **LAYERMODEL_LINK_TO_VIRTUAL** flag in the file to **false**; this is set to **true** by default.
- Save the **eg_ui.ini** file.

Doing so ensures that as soon as the **Inside View of Virtual Desktops** layer is clicked, the list of tests mapped to that layer appears. If you now want the **Desktop view** of Figure 1, simply click on **Back** button in the layer model page.

From the desktop view, you can further drill-down to focus on the health of a particular desktop, by clicking on the icon representing the desktop in Figure 1. Figure 5.8 then appears displaying all the performance metrics extracted from that virtual desktop in real-time. You are thus enabled to cross-correlate across the various metrics, and quickly detect the root- cause of current/probable disturbances to the internal health of a desktop. To view the time-of-day variations in a measure, you can view its graph by clicking on that measure in Figure 5.8.

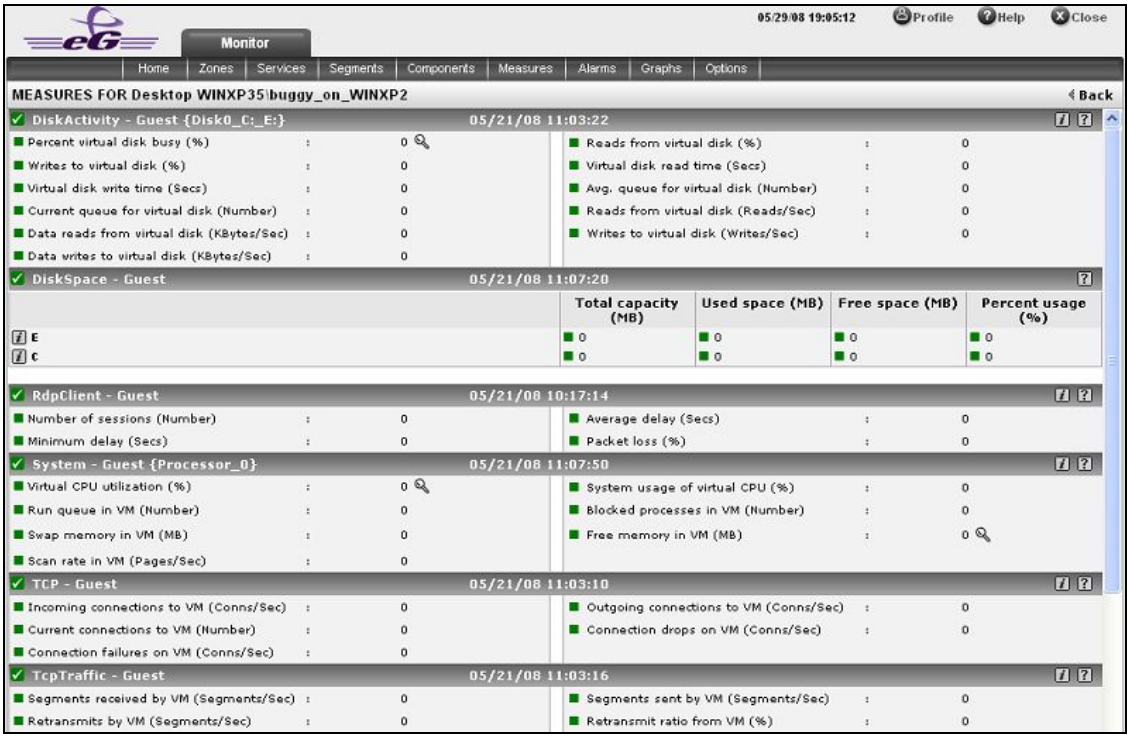


Figure 5.8: The measures pertaining to a particular desktop

You can also view live graphs of pre-configured measures pertaining to an Acropolis server and the virtual desktops configured on it, by clicking on the **LIVE GRAPHS** link in Figure 1. Alternatively, you can click on the icon that appears in the **Tests** panel of the layer model page when the **Virtual Desktop** layer (see Figure 2) is clicked to view the live graph. The resulting graph display (see Figure 5.9) has been organized in such a way that next to every host-pertinent measure graph, the closely related guest-specific measure graph appears. This way, you can easily compare and correlate how well the physical CPU resources are being utilized by both the host and the guests. On the basis of this analysis, you can proactively isolate potential performance issues, and also determine the root-cause of the issue - is it the Acropolis hypervisor? or is it the virtual guest? If you access this page from the **LIVE GRAPH** link in Figure 1, then, by default, you will view live graphs pertaining to the VDI server. However, you can select a different virtualized component-type and a different virtualized component using the **type** and **Component** lists (respectively) in Figure 5.9.

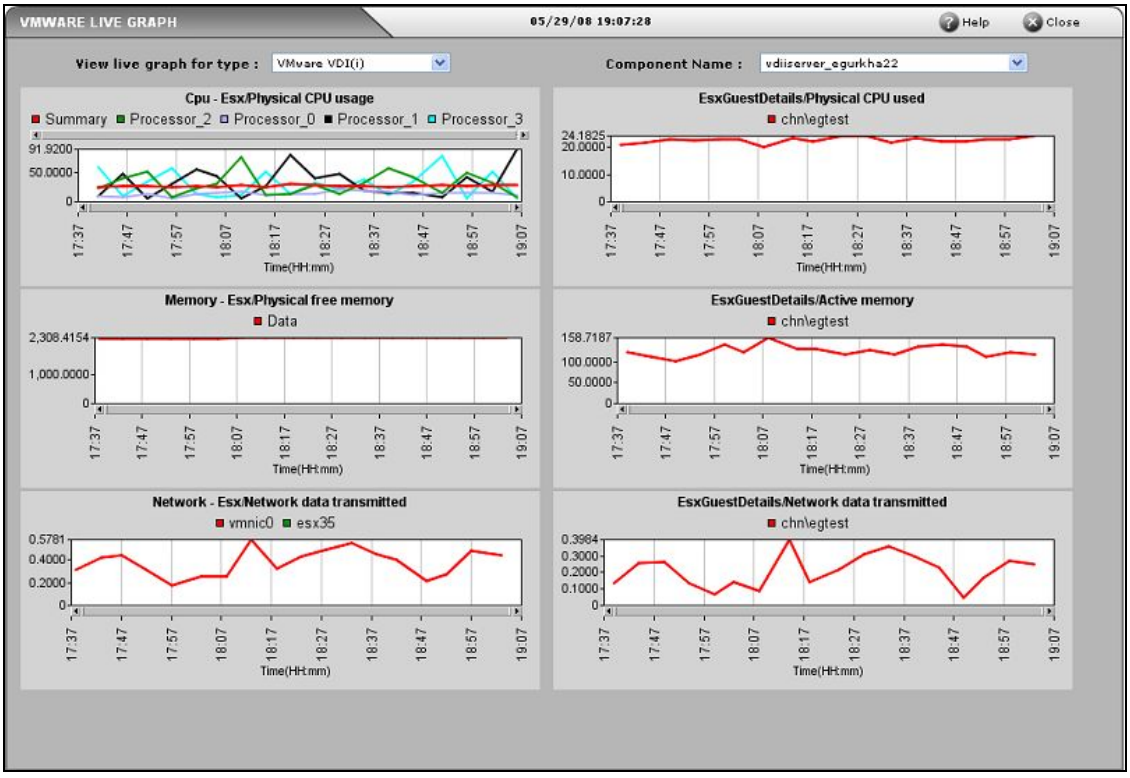


Figure 5.9: Live graph for VMware vSphere VDI server

5.2.2 Virtual Desktop Sessions Details Test

Every user who is logged into a virtual desktop, may not actively use that desktop. In a VDI infrastructure, it is common for users to just log into desktops, and leave them unused for long time periods. Such desktops are a huge resource drain, as they continue to consume resources,

regardless of the level of activity on them. Moreover, with many organizations these days providing the work-from-home option to their employees, identification of idle users is paramount, as such users themselves are deemed unproductive resource consumers. Also, this is a good indicator to whether/not the work-from-home facility is effectively used by employees or is abused! Besides, since idle users unnecessarily hold on to desktops, users with genuine needs may not have any desktops to work with. If administrators can quickly identify these idle users and the desktops they are logged into, they can rapidly pull the desktops from such users and assign them to users who can use them effectively. The **Virtual Desktop Sessions Details** test turns the spotlight on these idle users. For each user session on a virtual desktop, this test reports the total duration of the session and the percentage of time for which the session was active. The test also reports the total idle time during the session. From these statistics, administrators can accurately identify those users who are wasting the desktops assigned and resources allocated to them.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every user who is currently logged into a virtual desktop

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the

list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to

eG VM Agent (Windows). Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.2.2**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.
16. **IDLE TIME** - Specify the time duration (in minutes) of inactivity beyond which a session is considered to be "idle" by this test. By default, this parameter is set to 30 (minutes). This implies that by default, the test counts all sessions that have been inactive for over 30 minutes as idle sessions.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total time in session:	Indicates the time that has elapsed since this user logged into this desktop.	Mins	
Active time in last measure period:	Indicates the percentage of time in the last measurement period during which this user actively used this desktop.	Percent	Ideally, the value of this measure should be 100%. A low value for this measure denotes a high level of inactivity recently.
Time since last activity:	Indicates the time that has elapsed since this user performed an action on this desktop.	Mins	A high value for this measure indicates that the user has been idle for a long time. Compare the value of this measure across users to know which user has been idle for the longest time.
Is session idle in long time?	Indicates whether/not the session has been idle beyond the time duration specified against the **IDLE TIME** parameter.		The values that this measure can report and their corresponding numeric values are discussed in the table above: **Measure Value** / **Numeric Value** No – 0 Yes – 1 **Note:** By default, this measure reports the **Measure Value**s listed in the table above. In the graph of this measure however, the value of this measure is represented using their numeric equivalents only.

Measurement	Description	Measurement Unit	Interpretation
Total idle time in session:	Indicates the total time for which this user was idle during the session.	Mins	If the value of this measure is the same as the value of the *Total time in session* measure for a user, it means that the user has been idle throughout the session. If the value of this measure is close to the value of the *Total time in session* measure for a user, it implies that the user has been idle for a long time. If the value of this measure is much lesser than the value of the *Total time in session* measure for a user, it means that the user has been active for most part of the session.

5.2.3 Browser Activity – VM Test

When a user complains of a virtual desktop slowdown, administrators will have to instantly figure out if that VM is experiencing a resource crunch, and if so, which process/application on the desktop is contributing to it. One of the common reasons for CPU/memory contentions and handle leaks on a virtual desktop is web browsing! If a user to a virtual desktop browses resource-intensive web sites, it is bound to result in over-usage of the resources allocated to that VM, which in turn degrades the performance of not just that VM but even the other VMs on that host. While the **System Details – VM** test can lead administrators to the exact browser application that is consuming the CPU/memory resources of the VM excessively, it does not provide visibility into the precise websites that were been browsed when the resource contention occurred. This is where the **Browser Activity – VM** test helps. For each web browser that is being accessed by a user per virtual desktop, this test reports how every browser uses the allocated CPU, memory, and disk resources and reveals the number and URLs of the web sites that are being accessed using each browser. This way, the test not only points administrators to resource-hungry browsers, but also indicates which web sites were being accessed using that browser.

Note:

- This test will report metrics only if the Windows VM being monitored uses the .Net framework v3.0 (or above).
- This test will not be able to monitor the Microsoft Edge browser on Windows 10 VMs.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every user to each Windows virtual desktop on the Nutanix Acropolis 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that vCenter server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to theSection **Chapter 3** topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes

will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.2.3**.

- **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*.

14. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

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	Description	Measurement Unit	Interpretation
Running browser instances:	Indicates the number of instances of this browser currently running on this virtual desktop.	Number	Use the detailed diagnosis of this measure to know how much resources were utilized by each instance of a browser, so that the resource-hungry instance can be isolated.
Recent web sites:	Indicates the number of websites that were accessed using this browser on this virtual desktop during the last measurement period.	Number	Use the detailed diagnosis of this measure to know which web sites are being accessed using a browser.
CPU utilization:	Indicates the percentage CPU usage of this browser on this virtual desktop.	Percent	Compare the value of this measure across browsers to know which browser consumed the maximum CPU on a desktop. If the value of this measure is close to 100% on that desktop, it indicates excessive CPU usage by the browser. You may then want to use the detailed diagnosis of the Recent web sites measure to know which web sites are being accessed using that browser, which caused CPU usage to soar.
Memory used:	Indicates the percent usage of memory by this browser on this virtual desktop.	Percent	Compare the value of this measure across browsers to know which browser consumed the maximum memory on a desktop. If the value of this measure is close to 100% on that desktop, it indicates excessive memory usage by the browser. You may

Measurement	Description	Measurement Unit	Interpretation
			then want to use the detailed diagnosis of the Recent web sites measure to know which web sites are being accessed using that browser, which caused CPU usage to soar.
Handles used:	Indicates the number of handles opened by this browser on this virtual desktop.	Number	Compare the value of this measure across browsers to know which browser opened the maximum number of handles on a desktop. If the value of this measure consistently increases on that desktop, it indicates that the corresponding browser is leaking memory. You may then want to use the detailed diagnosis of the Recent web sites measure to know which web sites are being accessed using that browser, which caused the memory leak.
Disk reads:	Indicates the rate at which this browser read from the disks supported by this virtual desktop.	KB/Sec	A high value for these measures indicates that the browser is generating high disk I/O. You may then want to use the detailed diagnosis of the Recent web sites measure of this browser to know which web sites on the browser are responsible for the high disk I/O.
Disk writes:	Indicates the rate at which this browser read from the disks of this virtual desktop.	KB/Sec	
Disk IOPS:	Indicates the rate of read and write operations performed by this browser on the disks of this virtual	Operations/Sec	A high value for this measure indicates that the browser is generating high disk I/O. You may then want to use the detailed diagnosis of the Recent web sites

Measurement	Description	Measurement Unit	Interpretation
	desktop.		measure of this browser to know which web sites on the browser are responsible for the high disk I/O.
Page faults:	Indicates the rate at which page faults by the threads executing in this browser are occurring on this virtual desktop.	Faults/Sec	Ideally, the value of this measure should be low. A high value for a browser is a cause for concern. You may then want to use the detailed diagnosis of the Recent web sites measure of this browser to know which web sites on the browser are responsible for page faults.

The detailed diagnosis of the *Running browser instances* measure reveals the process ID of each browser instance that is currently running on the virtual desktop and the resource usage of each instance. This way, you can easily and accurately identify the instance that is consuming resources excessively.

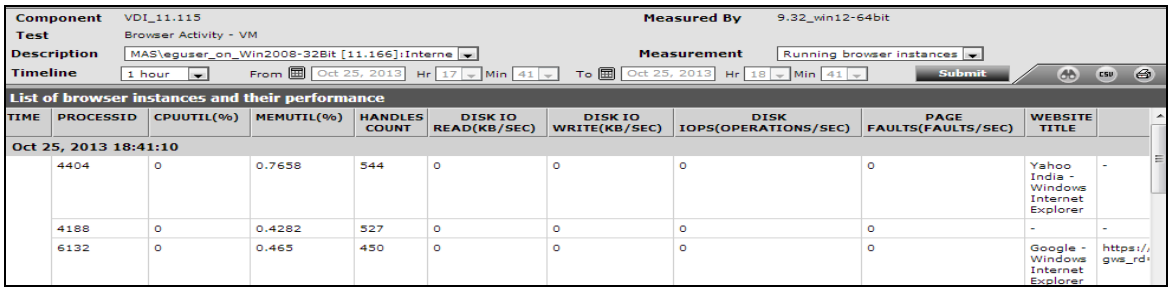


Figure 5.10: The detailed diagnosis of the Running browser instances measure

The detailed diagnosis of the *Recent web sites* measure reveals the names and URLs of the web sites that are being accessed using a browser.

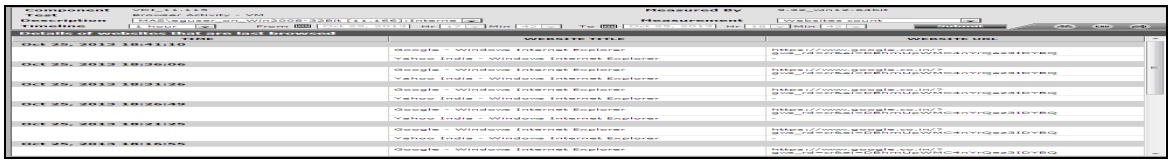


Figure 5.11: The detailed diagnosis of the Recent web sites measure

5.2.4 PCoIP Session - VM Test

PCoIP - PC over IP - is a proprietary protocol for remote workstation and desktop resolution. VMware View supports PCoIP to deliver virtual desktops to users connecting to the VDI. Since PCoIP recognizes different types of content and then uses different compression algorithms based on the content type, it is often considered ideal to deliver on the VDI promise of a rich user experience.

The key factors influencing user experience in such cases are the latencies experienced by the user while connecting to the desktop via PCoIP and the bandwidth used when a user interacts with a virtual desktop. High latency and excessive bandwidth consumption can often slowdown access to desktops, thereby significantly delaying subsequent user operations. Hence, monitoring the latency and bandwidth usage of the PCoIP communication channel between the user terminal and the virtual desktops is essential.

The **PCoIP Session - VM** test auto-discovers the virtual desktops on the Nutanix Acropolis host and the users who are currently connected to each desktop via PCoIP. For each such user, the test monitors the communication between a user and the virtual desktop, and reports the following:

- The latency experienced by each user session;
- The bandwidth used by the incoming and outgoing data/audio/multimedia traffic transacted by the PCoIP communication channel between each user and virtual desktop;

Using this test, an administrator can identify user sessions that are being impacted by high latency and abnormal bandwidth usage. In addition, the test also reveals the type of traffic that is causing excessive bandwidth usage, thereby providing pointers to how the client configuration can be fine-tuned in order to reduce bandwidth consumption and improve performance.

This test is relevant only where VMware View is used to broker connections between the user and the desktops. Hence, this test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence: Agents -> Tests -> Enable/Disable, pick *Nutanix Acropolis VDI* as the **Component type**, set *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.

Target of the test :A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every user who is connected to a virtual desktop via PCoIP.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.2.4**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Round trip time:	Indicates the round trip latency between the virtual desktop and this user terminal.	Secs	Comparing the value of this measure across users will enable administrators to quickly and accurately identify users who are experiencing higher latency when connecting to a virtual desktop.
Data received rate:	Indicates the rate at which data was received by this user from the virtual desktop.	Kbit/Sec	Comparing the value of each of these measures across users will enable administrators to quickly and accurately identify users who are consuming the maximum bandwidth. Once you zero-in on the user, you can compare the Data received rate of that user with the Data sent rate to know when the user consumed more bandwidth - when receiving data or while sending data?
Data sent rate:	Indicates the rate at which data was sent by this user to the virtual desktop.	Kbit/Sec	
Audio data received rate:	Indicates the bandwidth used while transmitting sound/audio to this user.	Kbit/Sec	Comparing these values across users will reveal which user is sending/receiving bandwidth-intensive sound/audio files over PCoIP.
Audio data sent rate:	Indicates the bandwidth used while receiving sound/audio from this user.	Kbit/Sec	

Measurement	Description	Measurement Unit	Interpretation
Imaging data received rate:	Indicates the bandwidth used when sending imaging data to this user.	Kbit/Sec	Comparing these values across users will reveal which user is sending/receiving bandwidth-intensive images over PCoIP.
Imaging data sent rate:	Indicates the bandwidth used when receiving imaging data from this user.	Kbit/Sec	
Imaging decoder capability rate:	Indicates the currrent estimate of the decoder processing capability.	Kbit/Sec	
Incoming bandwidth rate:	Indicates the overall bandwidth used by incoming PCoIP packets.	Kbit/Sec	Comparing the values of these measures across users will reveal which user is performing bandwidth- intensive operations over the PCoIP channel.
Outgoing bandwidth rate:	Indicates the overall bandwidth used by outgoing PCoIP packets.	Kbit/Sec	
USB data received:	Indicates the bandwidth used when this user received USB data over the PCoIP channel.	Kbit/Sec	Comparing the values of these measures across users will reveal which user is sending/receiving bandwidth-intensive USB data over the PCoIP channel.
USB data sent:	Indicates the bandwidth used when this user sent USB data over the PCoIP channel.	Kbit/Sec	
Received packets lost:	Indicates the percentage of packets received by this user that were lost.	Percent	A high value for these measures is indicative of a bad network connection between the user terminal and the virtual desktop.

Measurement	Description	Measurement Unit	Interpretation
Transmitted packets lost:	Indicates the percentage of packets transmitted by this user that were lost.	Percent	
Imaging encoded frames:	Indicates the number of imaging frames that were encoded per second.	Frames/Sec	

5.2.5 Personal vDisk – VM Test

The personal vDisk retains the single image management of pooled and streamed desktops while allowing people to install applications and change their desktop settings.

Unlike traditional Virtual Desktop Infrastructure (VDI) deployments involving pooled desktops, where users lose their customizations and personal applications when the administrator alters the base virtual machine (VM), deployments using personal vDisks retain those changes. This means administrators can easily and centrally manage their base VMs while providing users with a customized and personalized desktop experience.

Personal vDisks provide this separation by redirecting all changes made on the user's VM to a separate disk (the personal vDisk) attached to the user's VM. The content of the personal vDisk is blended at runtime with the content from the base VM to provide a unified experience. In this way, users can still access applications provisioned by their administrator in the base VM.

But, what happens if a personal vDisk runs out of space? Simple! Users will no longer be able to hold on to their customizations, allowing them access to only the base VM and the applications installed therein! This outcome beats the entire purpose of having personal vDisks! If this is to be avoided, then administrators should continuously monitor the usage of the personal vDisks, proactively detect a potential space crunch, determine what is causing the rapid erosion of space on the personal vDisk, and fix the root-cause, before desktop users complain. This is where the **Personal vDisk – VM** test helps.

For each VM on a Nutanix Acropolis server, this test tracks the status and space usage of its personal vDisk and promptly reports errors / abnormal space usage. This way, administrators can accurately identify personal

vDisks with very limited space, which VM such personal vDisks are associated with, and what is consuming too much disk space – user profiles? Or user applications?

Target of the test : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every *user_on_VM*.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that vCenter server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.2.5**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Personal vDisk service status:</td><td>Indicates whether Citrix Personal vDisk service is running or not on this VM.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been 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>Not installed</td><td>2</td></tr></table>Note:
By default, this test reports the Measures Values listed in the table above to indicate the status of the Personal vDisk service. In the graph of this measure however, the same will be represented using the numeric equivalents.</td></tr>
<tr><td>Recompose status:</td><td>Indicates the status of the initially provisioned disk or the updated image.</td><td>Number</td><td>Use the detailed diagnosis of this measure to know for which VM the initial personal vDisk provisioning or image update were unsuccessful and why. The VM can be in one of the following states:
• OK – The initial provisioning or last image update was successful.
• Disk Init – This is the first time that the personal vDisk has started or been resized. It is being initialized and partitioned by the service.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			• **Disk Format** – The personal vDisk is being formatted. • **Updating** – The initial provisioning or an image update is in progress. • **Error (Disk Discovery)** – An error state. An error occurred while discovering the personal vDisk. • **Error (Disk Init)** – An error state. An error occurred while partitioning or formatting the personal vDisk. • **Error (Sys Init)** – An error state. An error occurred while starting the Personal vDisk Service or configuring the personal vDisk. • **Error (Update)** – An error state. An error occurred during the initial provisioning or the last image update. • **Unknown** – An error state. An error occurred but the cause is unknown.
Space used by user applications:	Indicates the amount of space used by applications installed on the personal vDisk attached to this VM.	MB	Personal vDisks have two parts, which use different drive letters and are by default equally sized. One part comprises a Virtual Hard Disk file (a .vhd file). This contains items such as applications installed in C:\Program Files. By default, this part uses drive V: but is hidden from

Measurement	Description	Measurement Unit	Interpretation
			users. These measures indicate how much space has been allocated to this .vhd file and how much of the allocated space has been utilized by user applications contained in this file. A high value for the *Space used by user applications* and *Space utilized by user applications* measures is indicative of excessive space used by user applications. You can compare the value of these measures across VMs to know which user to which VM has utilized too much space reserved for user applications on the personal vDisk. If the value of the Space utilized by user applications measure grows close to 100% for any VM, it implies that potentially, the user to that VM will not be able to install any applications on the personal vDisk; nor access any applications.
Space allocated for user applications:	Indicates the amount of space allocation for storing user applications on the personal vDisk attached to this VM.	MB	
Space utilized by user applications:	Indicates the percentage of allocated space used by applications installed on the personal vDisk attached to this VM.	Percent	
Space used by user profiles:	Indicates the amount of space used for storing user profiles on the personal vDisk attached to this VM.	MB	Personal vDisks have two parts, which use different drive letters and are by default equally sized. One part comprises C:\Users (in Windows 7) or C:\Documents and Settings (in Windows XP). This contains user data, documents, and the user profile. By default this uses drive P:.

Measurement	Description	Measurement Unit	Interpretation
			These measures indicate how much space has been allocated to user profiles and how much of the allocated space has been utilized by user profiles. A high value for the *Space used by user profiles* and *Space utilized by user profiles* measures is indicative of excessive space used by user profiles. You can compare the value of these measures across VMs to know which VM's user profiles are consuming the maximum space on the personal vDisk. If the value of the Space utilized by user profiles measure grows close to 100% for any VM, it implies that potentially, the user to that VM will not be able to store/access any more documents or user data on the personal vDisk .
Space allocated for user profiles:	Indicates the amount of space allocated for storing user profiles on the personal vDisk attached to this VM.	MB	
Space utilized by user profiles:	Indicates the percentage of allocated space that has been used up by user profiles on the personal vDisk attached to this VM.	Percent	
Free space:	Indicates the amount of unused space on the personal vDisk attached to this VM.	MB	Ideally, the value of this measure should be high. You can compare the value of this measure across VMs to know which VM's personal vDisk has the least free space. You may then want to resize that personal vDisk to accommodate more data.
Total size:	Indicates the total size of the personal vDisk attached to this VM.	MB	The minimum size of a Personal vDisk is 3 GB, however a size of 10 GB is recommended.
Space utilized:	Indicates the percentage of space in	Percent	A consistent increase in the value of this measure is a cause for concern,

Measurement	Description	Measurement Unit	Interpretation
	the personal vDisk attached to this VM that is currently used.		as it indicates a gradual erosion of free space in the personal vDisk of a VM. By comparing the value of this measure across VMs, you can identify which VM's personal vDisk is running out of space! Once the VM with the space-hungry vDisk is isolated, you may want to compare the value of the *Space utilized by user applications* and *Space utilized by user profiles* measures of that VM, to clearly understand what is occupying too much space in the personal vDisk – is it the user profiles? Or is it the user applications? Based on this inference, you can figure out which drive partition of the personal vDisk has limited free space, and can decide between freeing up space in that partition or allocating more space to the personal vDisk itself.

5.2.6 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 5.12 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.

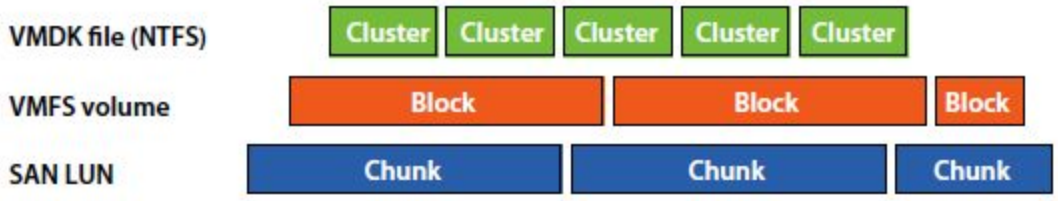


Figure 5.12: The SAN, VMFS, and NTFS blocks

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:

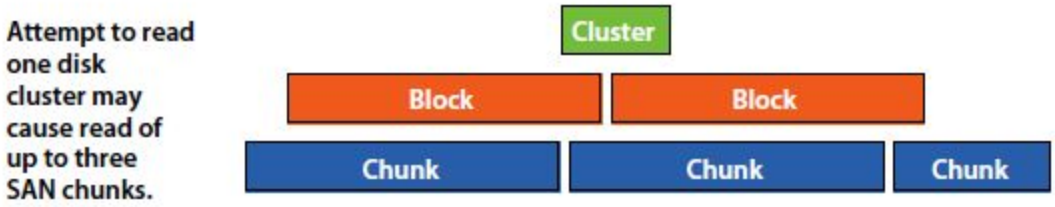


Figure 5.13: Unaligned partitions

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 5.13 above to be aligned so that a single NTFS block requires only one SAN block to be read as illustrated below:

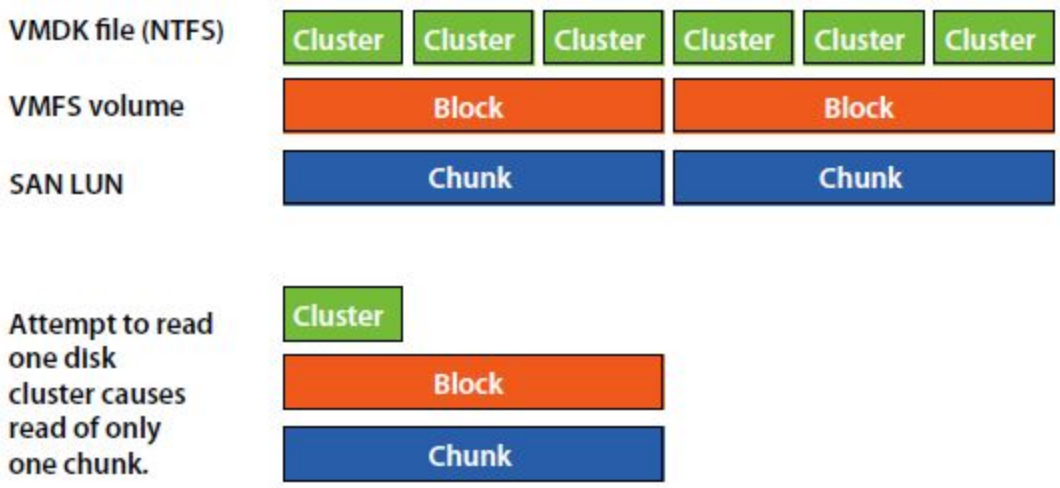


Figure 5.14: Aligned partitions

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.

Note:

This test reports metrics for Windows VMs only.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Nutanix Acropolis* as the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each disk partition on every Windows VM on a Nutanix Acropolis 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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option

from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.2.6**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

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	Description	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:

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Partition is aligned</td><td>100</td></tr><tr><td>Partition is not aligned</td><td>0</td></tr></table> **Note:** By default, this measure reports one of the **Measure Value**s 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.

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.

Details of physical disk partition

Time	Caption	Device id	Logical partition name	Block size
May 31, 2011 17:38:37	VMware Virtual disk SCSI Disk Device	\\.\PHYSICALDRIVE0	C:	512

Figure 5.15: The detailed diagnosis of the Disk partition alignment status measure

5.2.7 User Profile Management - VM

User logon is a complex and resource intensive process in a VDI environment, and is a key determinant of the quality of a user's experience with the VDI service. This process is initiated when a desktop broker's load balancing algorithm selects the virtual desktop where a published application or desktop, which a user has selected, will be started and ends when the application or desktop is running and the user is able to interact with it.

Delays in the user logon process can therefore serve as key spoilers of a user's experience with the desktop service, causing significant loss of revenue and reputation in mission- critical VDI environments.

One of the common causes for delays in user logons is a delay in the loading of user profiles. To reduce the time taken to load profiles and thus minimize the user logon time, VDI environments where user connections are brokered through the Citrix XenDesktop Broker, use the Citrix Profile Management solution. Citrix Profile Management is a profile type that supersedes all other profiles for the user.

During logon, the Profile management service manages the user settings in a user profile. This service helps minimize the user logon time by enabling administrators to exclude (and include) certain files and folders in order to prevent extraneous settings from needlessly being copied with the profile. For example, some applications may create folders and files that account for tens or hundreds of megabytes - data that is really not required. By excluding these items, the profile is thus smaller, and smaller profiles load faster. Alternatively, you could elect to only include specific files and folders, thus keeping to a minimum the amount of profile data being managed within the user's profile.

Also, upon logoff, the Profile management service merges back only changed user settings to the centrally stored user settings (user's store).

In environments where the Citrix Profile Management service is utilized therefore, the user experience with the VDI service greatly depends upon how efficient the service is.

Note:

This test is relevant only where the Citrix XenDesktop Broker is used to broker connections between the user and the desktops.

To ascertain the efficiency of the Citrix Profile Management service, VDI administrators may have to periodically track the logon/logoff duration and profile size of each user to the virtual desktops operating on a target virtual host. Doing so will enable these administrators to determine whether/not the Profile management service has succeeded in minimizing both user logon times and profile sizes. The **User Profile Management - VM** test helps administrators perform this check at pre-configured intervals. The 'per-user' performance results reported by this test will not only enable administrators to judge the effectiveness of the Profile management service in its entirety, but will also shed light on those user logons/logoffs that are still experiencing delays; this provides insights into how the service can be fine-tuned to enhance the VDI experience of such users.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence: Agents -> Tests -> Enable/Disable, pick *Nutanix Acropolis* or *Nutanix Acropolis VDI* as the **Component type**, set *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.

Target of the test : A Nutanix Acropolis server

Agent deploying the test : An internal/remote agent

Outputs of the test : One set of results for every user who is connected to a virtual desktop via ICA.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed

against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to

Section **5.2.7**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Logon Duration:	Indicates the duration of logon processing for this user.	Secs	This value helps to measure the reduction in logon times when the Profile Management service 'streams' the profile. Ideally therefore, this value should be low. A high value or a consistent increase in the value of this measure could indicate that profile loading still takes a lot of time at logon - this could be owing to a large profile size. You can then check the value reported by the Logon Bytes measure to know the

Measurement	Description	Measurement Unit	Interpretation
			profile size at logon. If profile sizes continue to grow at logon despite the use of Profile management, it is indicative of the ineffectiveness of profile management. You may then have to fine-tune the feature to further reduce the profile size by excluding more unnecessary files from the profile, or you may have to explore other options such as roaming profiles, mandatory profiles, etc.
Logon Bytes:	Indicates the size of this user's profile when it is retrieved from the user's store at logon.	MB	Ideally, the value of this measure should be low. A low profile size could result in faster profile loading at logon, lesser time to login, and consequently, a richer user experience with the VDI service. If profile sizes continue to grow despite the use of Profile management, it is indicative of the ineffectiveness of profile management. You may then have to fine-tune the feature to further reduce the profile size by excluding more unnecessary files from the profile.
Logoff Duration:	Indicates the duration of logoff processing for this user.	Secs	A low value is desired for this measure. A high value could indicate that the profile management service takes too long to update the user's store with changes in the user settings. This could be because of a bad network

Measurement	Description	Measurement Unit	Interpretation
			connection between the virtual desktop and the user's store, or because too many changes are waiting to be written to the user store.
Logoff Bytes:	Indicates the size of this user's profile when it is copied to the user store at logoff.	MB	This measure provides a fair idea of the volume of changes that were copied to the user's store at logoff.
Local Profile Setup Duration:	Indicates the time taken to create or prepare this user's profile on the local computer.	Secs	A low value is desired for these measures. If a user complaints of delays during logon, you can use the value of these measures to determine where the VDI service is spending too much time - is it when setting up the local profile? or is it when deleting the local profile?
Delete Local Profile Duration:	Indicates the time spent deleting this user's local profiles during the initial migration.	Secs	
Processed Logon Files - Under 1KB:	Indicates the number of locally copied files for this user's profile that are synchronized during logon and categorized by the file size of 1KB.	Number	All the *Processed Logon Files* measures help VDI administrators to understand whether/not 'profile streaming' (performed by the Profile Management service) has helped in reducing the number of locally copied files during logon. All the *Processed Logoff Files* measures help VDI administrators to understand how many files changed when the user session was in progress.
Processed Logoff Files - Under 1KB:	Indicates the number of locally copied file for this user's profile that are synchronized during logoff and categorized by the file size of 1KB.	Number	
Processed Logon Files from 1KB to 10KB:	Indicates the number of locally copied files for this user's profile that	Number	

Measurement	Description	Measurement Unit	Interpretation
	are synchronized during logon and categorized by the file size ranging from 1KB to 10KB.		
Processed Logoff Files from 1KB to 10KB:	Indicates the number of locally copied files for this user's profile that are synchronized during logoff and categorized by the file size ranging from 1KB to 10KB.	Number	
Processed Logon Files from 10KB to 100KB:	Indicates the number of locally copied files for this user's profile that are synchronized during logon and categorized by the file size ranging from 10KB to 100KB.	Number	
Processed Logoff Files from 10KB to 100KB:	Indicates the number of locally copied files for this user's profile that are synchronized during logoff and categorized by the file size ranging from 1KB to 10KB.	Number	All the *Processed Logon Files* measures help VDI administrators to understand whether/not 'profile streaming' (performed by the Profile Management service) has helped in reducing the number of locally copied files during logon. All the *Processed Logoff Files* measures help VDI administrators to understand how many files changed when the user session was in progress.
Processed Logon Files from 100KB to 1MB:	Indicates the number of locally copied files for this user's profile that are synchronized during logon and categorized by the file size ranging from 100KB to 1MB.	Number	
Processed Logoff Files from 100KB	Indicates the number of locally copied files for	Number	

Measurement	Description	Measurement Unit	Interpretation
to 1MB:	this user's profile that are synchronized during logoff and categorized by the file size ranging from 100KB to 1MB.		
Processed Logon Files from 1MB to 5MB:	Indicates the number of locally copied files for this user's profile that are synchronized during logon and categorized by the file size ranging from 1MB to 5MB.	Number	
Processed Logoff Files from 1MB to 5MB:	Indicates the number of locally copied files for this user's profile that are synchronized during logoff and categorized by the file size ranging from 1MB to 5MB.	Number	All the *Processed Logon Files* measures help VDI administrators to understand whether/not 'profile streaming' (performed by the Profile Management service) has helped in reducing the number of locally copied files during logon. All the *Processed Logoff Files* measures help VDI administrators to understand how many files changed when the user session was in progress.
Processed Logon Files Above 5MB:	Indicates the number of locally copied files for this user's profile that are synchronized during logon and categorized by the file size above 5MB.	Number	
Processed Logoff Files Above 5MB:	Indicates the number of locally copied files for this user's profile that are synchronized during logoff and categorized by the file size above 5MB.	Number	

5.2.8 User Logon - VM Test

The process of a user logging into a virtual server is fairly complex. First, the domain controller is discovered and the login credentials are authenticated. Then, the corresponding user profile is identified and loaded. Next, group policies are applied and logon scripts are processed to setup the user environment. In the meantime, additional processing may take place for a user – say, applying system profiles, creating new printers for the user, and so on. A slowdown in any of these steps can significantly delay the logon process for a user. Since logons on Windows happen sequentially, this may adversely impact the logins for other users who may be trying to access the virtual server at the same time. Hence, if a user complains that he/she is unable to access an application/desktop published on virtual server, administrators must be able to rapidly isolate exactly where the logon process is stalling and for which user. The typical process for monitoring and troubleshooting the login process on Windows is to use the user environment debugging mechanism. To enable this on Windows and to set the logging level associated with the userenv.log file, perform the following steps:

- Start a registry editor (e.g., regedit.exe).
- Navigate to the **HKEY_ LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon** registry subkey.
- From the Edit menu, select New, DWORD Value.
- Enter the name UserEnvDebugLevel, then press Enter.
- Double-click the new value, set it to 65538 (decimal) - which corresponds to the debugger output.

Once these changes are enabled, details about the Windows login process are logged into the file *%systemroot%\debug\usermode\userenv.log* . The log file is written to the *%Systemroot%\Debug\UserMode\Userenv.log* file. If the Userenv.log file is larger than 300 KB, the file is renamed *Userenv.bak*, and a new *Userenv.log* file is created. This action occurs when a user logs on locally or by using Terminal Services, and the Winlogon process starts. However, because the size check only occurs when a user logs on, the Userenv.log file may grow beyond the 300 KB limit. The 300 KB limit cannot be modified.

The **User Logon - VM** test periodically checks the userenv log file on Windows to monitor the user login and profile loading process and accurately identify where the process is bottlenecked. On Windows 2008 (or above), this test takes the help of the Windows event logs to capture anomalies in the user login and profile loading process and report where the process is bottlenecked - in the authentication process? during profile loading? during GPO processing and if so, which GPO?

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every user to the Nutanix Acropolis server to be monitored

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.
- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access

this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.2.8**.

- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.
16. **REPORT FOR EACH USER –** By default, this flag is set to **Yes**. This implies that, by default, the test will report metrics for each user to the virtual machine. If you set this flag to **No**, then metrics will be reported for VMs.
17. **REPORT BY DOMAIN NAME –** By default, this flag is set to **No**. This means that, by default, the test will report metrics for each username only. You can set this flag to **Yes**, to ensure that the test reports metrics for each domainname\username.
18. **REPORT UNKNOWN –** By default, this flag is set to **No**. Accordingly, the test, by default, disregards user sessions that have remained active on the server for a duration lesser than the **TEST PERIOD**. If you want the test to report metrics for such users as well, then set this flag to **Yes**. In this case, the test will additionally support an Unknown descriptor – the metrics reported by this descriptor will be aggregated across all such user sessions that have been active on the server only for a limited duration.
19. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a *Nutanix Acropolis* server, this is set to *1:1* by default. This indicates that, by

default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

20. **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	Description	Measurement Unit	Interpretation
Logon duration:	Indicates the average time taken by this user for logging in during the last measurement period.	Msecs	If this value is abnormally high for any user, then, you can compare the User account discovery time, LDAP bind time to Active Directory, Client side extension processed time, DC discovery time, Total group policy object file access time, Avg system policy processing time and User profile load time measures to know exactly where that user's login process experienced a bottleneck - is it when loading the profile? is it when processing system policies? is it when processing group policies? is it when interacting with AD for authenticating the user login?
User account discovery:	Indicates the amount of	Msecs	Compare the value of this measure across users to know which user's

Measurement	Description	Measurement Unit	Interpretation
	time taken by the system call to get account information for this user during the last measurement period.		logon process spent maximum time in retrieving account information.
LDAP bind time to Active Directory:	Indicates the amount of time taken by the LDAP call for this user to connect and bind to Active Directory during the last measurement period.	MSecs	Compare the value of this measure across users to know which user's logon process spent maximum time in connecting to Active Directory. Besides impacting authentication time, high LDAP bind time may also affect group policy processing.
Client side extension processed time:	Indicates the amount of time that client side extensions took for processing group policies for this user during the last measurement period.	MSecs	Compare the value of this measure across users to know which user's logon process spent maximum time in group policy processing. If this measure reports an unusually high value for any user, then, you may want to check the value of the LDAP bind time to Active Directory measure for that user to figure out if a delay in connecting to AD is affecting group policy processing. This is because, group policies are built on top of AD, and hence rely on the directory service's infrastructure for their operation. As a consequence, DNS and AD issues may affect Group Policies severely. One could say that if an AD issue does not interfere with authentication, at the very least it will hamper group policy processing.

Measurement	Description	Measurement Unit	Interpretation
			You can also use the detailed diagnosis of this measure to know which client side extension was used to process which group policy for a particular user.
DC discovery time:	Indicates the time taken to discover the domain controller to be used for processing group policies for this user during the last measurement period.	MSecs	Compare the value of this measure across users to know which user's logon process spent maximum time in domain controller discovery.
Total group policy object file accessed time:	Indicates the amount of time the logon process took to access group policy object files for this user during the last measurement period.	MSecs	Compare the value of this measure across users to know which user's logon process spent maximum time in accessing the group policy object file.
User profile load time:	Indicates the amount of time it took to load this user's profile successfully in the last measurement period.	MSecs	Compare the value of this measure across users to know which user's profile took the longest time to load. One of the common reasons for long profile load times is large profile size. In such circumstances, you can use the User Profile test to determine the current size of this user's profile. If the profile size is found to be large, you can conclude that it is indeed the size of the profile which is affecting the profile load time. Another reason would be the absence of a profile. If the user does not already have a profile a

Measurement	Description	Measurement Unit	Interpretation
			new one is created. This slows down the initial logon quite a bit compared to subsequent logons. The main reason is that Active Setup runs the IE/Mail/Theme initialization routines. Moreover, this measure reports the average time taken for loading a user's profile across all the sessions of that user. To know the profile load time per user session, use the detailed diagnosis of this measure. This will accurately pinpoint the session in which the profile took the longest to load.
Group policy starts:	Indicates the number of group policy applications started for this user in the last measurement period.	Number	Logon performance improves when fewer Group Policies are applied. Merge GPOs when possible instead of having multiple GPOs.
Group policy completes:	Indicates the number of group policy applications completed for this user in the last measurement period.	Number	
Client side extensions applied:	Indicates the number of client side extensions used for processing group policies for this user during the last measurement period.	Number	
Max group policy time:	Indicates the maximum time taken for applying group policies for this	Msecs	

Measurement	Description	Measurement Unit	Interpretation
	user in the last measurement period.		
Profile load starts:	Indicates the number of profile loads started for this user in the last measurement period.	Number	Use the detailed diagnosis of this measure to know the details of the user sessions in which profile loads were started.
Profile load successes:	Indicates the number of successful profile loads for this user in the last measurement period.	Number	
Profile loading failures:	Indicates the number of profile load failures for this user in the last measurement period.	Number	An unusual increase in number of profile loading failures is a cause for concern. The userenv.log/event logs file will have details of what profile loads failed and why.
Profile load failures percent:	Indicates the percentage of profile loads that failed for this user in the last measurement period.	Percent	A low value is desired for this measure. Compare the value of this measure across users to know which user's profile failed to load most often.
Avg user profile load time:	Indicates the average time it took to load this user's profile successfully in the last measurement period.	Msecs	Ideally, profile load time should be low for any user. A high value or a consistent rise in this value is a cause for concern, as it indicates a delay in profile loading. This in turn will have a negative impact on user experience. One of the common reasons for long profile load times is large profile size. Compare the value of this measure across users to identify that user whose profile took the longest to load. Then, use the User Profile

Measurement	Description	Measurement Unit	Interpretation
			test to determine the current size of this user's profile. If the profile size is found to be large, you can conclude that it is indeed the size of the profile which is affecting the profile load time.
Max profile load time:	Indicates the maximum time it took to load a profile during the last measurement period.	Msecs	
Profile unload starts:	Indicates the number of profile unloads started for this user during the last measurement period.	Number	Use the detailed diagnosis of this measure to know when a user's session was initiated and how long each session remained active on the virtual server. From this, you can infer how many sessions were active for a user on the server and the duration of each session, and thus identify long-running sessions for the user.
Profile unload successes:	Indicates the number of successful profile unloads for this user during the last measurement period.	Number	
Profile unload failures:	Indicates the number of unsuccessful profile unloads during the last measurement period.	Number	
Profile unload failures percent:	Indicates the profile unload failures as a percentage of the total profile unloads.	Percent	
Avg user profile	Indicates the average	Msecs	

Measurement	Description	Measurement Unit	Interpretation
unload time:	time for unloading a profile during the last measurement period.		
Max profile unload time:	Indicates the maximum time for unloading a profile during the last measurement period.	Msecs	
System policy starts:	Indicates the number of system policy processes that were started for this user in the last measurement period.	Number	
System policy completes:	Indicates the number of system policy completions for this user in the last measurement period.	Number	Compare the total number of starts to completions. if there is a significant discrepancy, this denotes a bottleneck in system policy application. Check the userenv.log file for more details.
Avg system policy processing time:	Indicates the average time taken for applying system policies in the last measurement period for this user.	Msecs	If the system policy times are long, check the detailed diagnosis to view if the policy handling is taking time for all users. Analyze the userenv.log to determine the reason for any slowdown.
Max system policy time:	Indicates the maximum time for applying system policies for this user in the last measurement period.	Msecs	

5.3 Outlook Add-ins - VM Test

Outlook add-ins are integrations built by third parties into Microsoft Outlook using the new web technologies based platform. Microsoft Outlook add-ins have three key aspects:

- The same add-in and business logic works across desktop Microsoft Outlook for Windows and Mac, web (Office 365 and Outlook.com), and mobile.
- Outlook add-ins consist of a manifest, which describes how the add-in integrates into Outlook (for example, a button or a task pane), and JavaScript/HTML code, which makes up the UI and business logic of the add-in.
- Outlook add-ins can be acquired from the Office store or side-loaded by end-users or administrators.

The Outlook add-ins may be useful in connecting the business and social networks of the users. These add-ins when integrated with Microsoft Outlook simplifies the job of the users as they can stay up to date on the status and activities of their contacts by merely overlooking the Microsoft Outlook! When a user complains that it is taking too long to launch the add-ins of the Microsoft Outlook published on virtual desktops, administrators must be able to quickly identify the add-ins that were loaded while the Microsoft Outlook is opened by the user, know how much time each add-in took to load, and thus pinpoint the add-in that is the slowest in loading. The **Outlook Add-ins - VM** test provides these valuable insights to the administrators. This test auto-discovers all the add-ins integrated with the Microsoft Outlook published on the virtual desktops hosted by the virtual server, and for each discovered add-in, reports the number of times the add-in was loaded and the average and maximum time that add-in took to load. This way, the test points administrators to add-ins that are slow in loading.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis VDI host

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every outlook add-in integrated with the Microsoft Outlook published on the virtual desktops provisioned by the Nutanix Acropolis VDI being monitored

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis VDI server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for

discovering this Nutanix Acropolis VDI server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis VDI server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis VDI server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis VDI server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis VDI server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis VDI server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.3**.
- **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*.

14. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_*

virtualmachinename. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of times loaded in last measure period	Indicates the number of times this outlook add-in was loaded during the last measurement period.	Number	The detailed diagnosis of this measure lists the time and duration for which the outlook add-in was loaded. Compare the value of this measure across the add-ins to figure out the most/least popular add-in.
Average load time	Indicates the average time taken by this outlook add-in to load.	Secs	
Maximum load time	Indicates the maximum time taken by this outlook add-in to load.	Secs	Compare the value of this measure across the add-ins to figure out the add-in that is the slowest to load.

5.3.1 Virtual Desktop EDT Performance - VM Test

Adaptive Transport – a new transport mechanism for virtual servers is faster, reliable and more scalable, and improves application interactivity and quickly delivers HDX content to users on long-haul WAN and Internet over UDP or TCP. While TCP is a default choice for HDX content delivery, Adaptive Transport uses an enhanced version of UDP as the primary data transport protocol i.e., Enlightened Data Transport (EDT) protocol to overcome shortfalls of TCP. This mechanism has been built with the intelligence to automatically understand network conditions and react to changes dynamically. Based on dynamic determination of conditions where TCP would perform better, or should the network not support UDP, or in the event of an EDT failure, the ICA virtual channels intelligently switch from EDT to TCP automatically. Automatic fallback to TCP ensures that there is no connection timeout, faster and uninterrupted session connectivity for the users on WAN and increased session reliability. These benefits make the EDT a standard data transport protocol for

HDX content delivery in the virtual environments. With such great user impact, monitoring the performance of sessions that are established via EDT becomes inevitable for administrators. Before a user complains about a problem on an EDT session, administrators need to have the capability to continuously monitor EDT performance and connectivity, and isolate bottlenecks for proactive troubleshooting. This is where the **Virtual Desktop EDT Performance - VM** test helps!

This test auto-discovers the virtual desktop user sessions that use the EDT protocol, and reports the bandwidth usage, network traffic, and latency of each such session. Using these performance metrics, administrators can measure the experience of users connected over EDT, and accurately isolate bandwidth-hungry and latent user sessions.

Note:

This test will report metrics only if the following configuration is available in the environment:

- XenApp and XenDesktop 7.13 and above
- VDA for Desktop OS 7.13 and above
- VDA for Server OS 7.13 and above
- StoreFront 3.9 and above
- Citrix Receiver for Windows 4.7 and above
- Citrix Receiver for Mac 12.5 and above
- Citrix Receiver for iOS 7.2 and above
- IPv4 VDAs only. IPv6 and mixed IPv6 and IPv4 configurations are not supported.
- NetScaler 11.1-51.21

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every user who is currently connected to the Nutanix Acropilis server via the EDT protocol.

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 specified **HOST** listens. By default, this is NULL.
4. **CITRIX HOME** - By default, the **CITRIX HOME** parameter is set to none indicating that the eG agent would automatically discover the location at which the Virtual Delivery Agent VDA; is installed for collecting the metrics of this test. If the Virtual Delivery Agent is installed in a different location in your Citrix environment, then indicate that location in the **CITRIX HOME** text box.
5. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.
6. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Configuring eG Enterprise to Monitor Nutanix Acropolis topic for details on how to use this page.

7. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
8. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
9. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.
10. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.
11. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

12. **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.

13. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

14. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.3.1**.

- **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*.

15. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.
16. **REPORT POWERED OS** - **This flag becomes relevant only if the REPORT BY USER FLAG is set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.
17. **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	Description	Measurement Unit	Interpretation
Number of sessions	Indicates the number of sessions intiated by this user.	Number	The value 0 indicates that the user is not currently connected to the Citrix server.
Bandwidth	Indicates the bandwidth usage of all sessions of	Kbps	Compare the value of this measure across users to know

Measurement	Description	Measurement Unit	Interpretation
	this user.		which user is consuming the maximum bandwidth.
Round trip time	Indicates the round trip latency between the virtual machine and this user.	Seconds	Comparing the value of this measure across users will enable administrators to quickly and accurately identify users who are experiencing higher latency when connecting to a virtual machine via EDT protocol.
Flow window	Indicates the size of the flow window.	KB	The flow window and congestion window are used to control the congestion in the network. The smaller the value of both the windows, the data will be sent without any delay. The larger the value, the data will be added up in the sent queue and it will be sent with delay.
Congestion window	Indicates the size of the congestion window.	KB	
Sent packets	Indicates the number of EDT packets sent by this user.	Packets	
Received packets	Indicates the number of EDT packets received by this user.	Packets	
Retransmitted packets	Indicates the number of EDT packets that were retransmitted by the user.	Packets	
Lost sent packets	Indicates the number of packets lost by this user during transmission.	Packets	Ideally, the value of this measure should be zero. Comparing the value of these measures across users will enable administrators to quickly

Measurement	Description	Measurement Unit	Interpretation
			and accurately identify users who have extensively lost packets during transmission and reception of packets via EDT protocol.
Lost received packets	Indicates the number of packets lost by this user during reception.	Packets	
Sent acknowledgements	Indicates the number of acknowledgements that were received by this user for sending the EDT packets.		
Sent negative acknowledgements	Indicates the number of negative acknowledgements that were received by this user for sending the EDT packets.		
Received acknowledgements	Indicates the number of acknowledgements that were received by this user for reception of EDT packets.		
Received negative acknowledgements	Indicates the number of negative acknowledgements that were received by this user for reception of EDT packets.		

5.3.2 Windows Security Center Status - VM Test

Windows Security Center (WSC) is a comprehensive reporting tool that helps administrators establish and maintain a protective security layer around Windows VMs to monitor the VM's health state. The Windows Security Center also monitors third party security products such as firewall, antivirus, antimalware and antispyware, installed on the VM. In order for the security products to be

compliant with Windows and successfully report status to Action Center, these products should be registered with the security center. The security products communicate any subsequent status changes to the security center using private APIs. The security center, in turn, communicates these updates to Action Center, where they are finally displayed to the end user. With Windows Security Center, administrators can check whether any security product is installed and turned on, and if the definitions of the products are up to date and real-time protection is enabled. By continuously monitoring the Windows Security Center, administrators can instantly find out whether the security products are up-to-date or out dated, and the status of security products in real-time. This is what exactly the **Windows Security Center Status - VM** test does!

This test auto-discovers the security products installed on the Windsows VMs on the target host, and for each security product reports the current definition status and the current protection status. Using these details, administrators are alerted to the systems on which the automatic updates are outdated and virus protection turned off. By closely monitoring the status, administrators can take necessary actions before the end users become vulnerable to virus threats or malicious attacks.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Nutanix Acropolis/ Nutanix Acropolis-VDI* as the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis/ Nutanix Acropolis-VDI server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every *security product:provider combination* on each Windows VMs on the target server.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to theSection **Chapter 3** topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Section **Chapter 3** topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.
7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.
8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port

9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.3.2**.
- **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. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.

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	Description	Measurement Unit	Interpretation
Signature status	Indicates the current status of this security product.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Unknown – 25 Up to date – 15 Out of date – 10 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current state of this security product. The graph of this measure however, represents the status of a server using the numeric equivalents only. Use the detailed diagnosis of this

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>measure, to know about the name of Windows system on which the product is running, the file paths of product executables and the current status of the product.</td></tr>
<tr><td>Real-time protection status</td><td>Indicates the real-time protection status of this security product.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>25</td></tr><tr><td>Snoozed</td><td>20</td></tr><tr><td>On</td><td>15</td></tr><tr><td>Expired</td><td>10</td></tr><tr><td>Off</td><td>0</td></tr></table>Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current protection status of this security product. The graph of this measure however, represents the status of a server using the numeric equivalents only.</td></tr>
</table>

5.3.3 Windows Update Details - VM Test

Microsoft regularly releases various Windows updates to enhance and protect the Windows operating system. These updates are also applicable for the Windows virtual desktops on the VMs. The Windows updates fix newly discovered security holes and bugs, add malware definitions to Windows Defender and Security Essentials utilities, strengthen Office security and add new

features/enhancements to the Windows operating system. By installing these updates regularly, you can keep the operating system highly secure, reliable and stable, and can maintain the performance of the operating system at peak. If the operating system is not updated regularly, the critical bugs and security errors may increase vulnerabilities. These vulnerabilities can be exploited by the malware or hackers, thus exposing the operating system to malicious attacks and degrading the operating system's performance. To avoid such eventualities, you should regularly check whether the Windows operating system is up-to-date or not. This check can be easily done using the **Windows Update Details - VM** test.

This test continuously monitors the Windows operating system and reports the current status of the Windows updates on the operating system. Besides, this test indicates whether any update is pending for the operating system and whether the Windows system is rebooted or not. In the process, this test also reports the total number of updates to be installed for the operating system and the number of Windows updates of different types at regular intervals.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Microsoft Windows* as the desired **Component type**, set *Performance* as the **Test type**, choose the 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 : A Nutanix Acropolis/ Nutanix Acropolis-VDI server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every *security product:provider combination* on each Windows VMs on the target server.

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 specified **HOST** listens. By default, this is NULL.
4. **PRISM IP** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still

want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Nutanix Prism will be automatically displayed against the respective text boxes.

On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to theSection **Chapter 3** topic for details on how to use this page.

5. **PRISM USER** and **PRISM PASSWORD** - If the eG manager had discovered the target Nutanix Acropolis server by connecting to the Nutanix Prism, then the IP address of the Nutanix Prism server used for discovering this Nutanix Acropolis server would be automatically displayed against the **PRISM IP** parameter; similarly, the **PRISM USER** and **PRISM PASSWORD** text boxes will be automatically populated with the Prism user credentials, using which Nutanix Acropolis discovery was performed.

   If this Nutanix Acropolis server has not been discovered using the Nutanix Prism, but you still want to monitor the Nutanix Acropolis server via the Prism, then select the IP address of the Prism server that you wish to use for monitoring the Nutanix Acropolis server from the **PRISM IP** list. By default, this list is populated with the IP address of all Nutanix Prism hosts that were added to the eG Enterprise system at the time of discovery. Upon selection, the **PRISM USER** and **PRISM PASSWORD** that were pre-configured for that Prism server will be automatically displayed against the respective text boxes.

   On the other hand, if the IP address of the Prism server of interest to you is not available in the list, then, you can add the details of the Prism server on-the-fly, by selecting the **Other** option from the **PRISM IP** list. This will invoke the **MANAGER DISCOVERY - VIRTUAL PLATFORM SETTINGS** page. Refer to the Section **Chapter 3** topic for details on how to use this page.

6. **CONFIRM PASSWORD** - Confirm the password by retyping it here.

7. **SSL** - By default, the Nutanix Prism server is SSL-enabled. Accordingly, the SSL flag is set to **Yes** by default. This indicates that the eG agent will communicate with the Prism server via HTTPS by default.

8. **WEBPORT** - By default, the Nutanix Prism server listens on port 9440. This implies that while monitoring a Nutanix Acropolis server via the Prism server, the eG agent connects to port 9440.

9. **EXCLUDE VMS** - Administrators of some virtualized environments may not want to monitor some of their less-critical VMs 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.

10. **IGNORE VMS INSIDE VIEW** - Administrators of some high security Nutanixe 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 a Nutanix Acropolis 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.

11. **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.

12. **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.** Refer to Configuring the eG Agent to Collect Current Hardware Status Metrics for more details on the **eG VM Agent**. To ensure that the "inside view" of Windows VMs is obtained using the eG VM Agent, set the **INSIDE VIEW USING** flag to **eG VM Agent (Windows)**. Once this is done, you can set the **DOMAIN**, **ADMIN USER**, and **ADMIN PASSWORD** parameters to *none*.

13. **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 Troubleshooting the Failure of the eG Remote Agent to Connect to or Report Measures for Linux Guests.

- **If the guests belong to different domains** - In this case, you might want to provide multiple domain names. If this is done, then, to access the guests in every configured domain, the test should be configured with the required user privileges; this implies that along with multiple **DOMAIN** names, multiple **ADMIN USER** names and **ADMIN PASSWORDS** would also have to be provided. To help administrators provide these user details quickly and easily, the eG administrative interface embeds a special configuration page. To access this page, simply click on the Click here hyperlink that appears just above the parameters of this test in the test configuration page. To know how to use the special page, refer to Section **5.3.3**.
- **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*.

14. **REPORT BY USER** - While monitoring a Nutanix Acropolis server, the **REPORT BY USER** flag is set to **No** by default, indicating that by default, the guest operating systems on the Acropolis server are identified using the hostname specified in the operating system. On the other hand, while monitoring Acropolis desktop environments, this flag is set to **Yes** by default; this implies that in case of VDI servers, by default, the guests will be identified using the login of the user who is accessing the guest OS. In other words, in VDI environments, this test will, by default, report measures for every *username_on_virtualmachinename*.

15. **REPORT POWERED OS** - **This flag becomes relevant only if theREPORT BY USER FLAGis set to 'Yes'**.

    If the **REPORT POWERED OS** flag is set to **Yes** (which is the default setting), then this test will report measures for even those VMs that do not have any users logged in currently. Such guests will be identified by their *virtualmachine name* and not by the *username_ on_ virtualmachinename*. On the other hand, if the **REPORT POWERED OS** flag is set to **No**, then this test will not report measures for those VMs to which no users are logged in currently.

16. **DD FOR TOTAL UPDATES** – In large VDI environments where hundreds of Windows virtual desktops have been provisioned, the frequent collection of detailed diagnosis information related to the update details of the virtual desktops may increase the processing overheads of the eG agent, and may even choke the eG database. To avoid this, by default, the **DD FOR TOTAL UPDATES** flag is set to **No** indicating that this test will not report the detailed diagnostics for the *Total Updates Available* measure. However, you can set this flag to **Yes** if you want to

collect the detailed diagnostics of the *Total Updates Available* measure.

17. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. For a Nutanix Acropolis server, this is set to *1:1* by default. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem.
18. **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	Description	Measurement Unit	Interpretation
Are pending updates available?	Indicates whether/not the updates are pending.		The values that this measure can report and the numeric values they indicate have been listed in the table below: **Measure Value** / **Numeric Value** No – 0 Yes – 1 **Note:** By default, this measure can report the **Measure Value**s mentioned above while indicating whether/not the updates are available. However, the graph of this measure is indicated using the numeric equivalents.

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Is a system reboot pending?</td><td>Indicates whether the Windows system is rebooted or not.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>No</td><td>0</td></tr><tr><td>Yes</td><td>1</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating whether the system is rebooted or not. However, the graph of this measure is indicated using the numeric equivalents.</td></tr>
<tr><td>Windows update service status</td><td>Indicates the current status of the Windows update service.</td><td></td><td>The values that this measure can report and the numeric values they indicate have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Running</td><td>1</td></tr><tr><td>Start pending</td><td>2</td></tr><tr><td>Continue pending</td><td>3</td></tr><tr><td>Pause pending</td><td>4</td></tr><tr><td>Stop pending</td><td>5</td></tr><tr><td>Paused</td><td>6</td></tr><tr><td>Stopped</td><td>7</td></tr></table>
Note:
By default, this measure can report the Measure Values mentioned above while indicating the current status of</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Windows update service. However, the graph of this measure is indicated using the numeric equivalents.
Total updates available	Indicates the total number of Windows updates available for the Windows operating system.	Number	The detailed diagnosis of this measure, if enabled, lists the Windows updates available for the system and the categories of the available updates.
Critical updates available	Indicates the number of critical updates available for the Windows operating system.	Number	A critical update is a widely and frequently released update that deals with the specific, non-security related, critical bugs. If these bugs are not fixed quickly, they can cause serious performance degradation, interoperability malfunction or disturb application compatibility.
Important updates available	Indicates the number of important updates available for the Windows operating system.	Number	The important updates help fixing the vulnerabilities using which malware/hackers can exploit the system resources or steal data. This in tun may leave the confidentiality and integrity of the system defenseless and make the user data unavailable.
Moderate updates available	Indicates the number of moderate security updates available for the Windows operating system.	Number	The moderate updates fix a vulnerability whose exploitation can be mitigated to a significant degree by default configuration, auditing, or difficulty of exploitation.
Low updates available	Indicates the number of low security updates available for the Windows operating system.	Number	These updates fix the vulnerability whose exploitation is extremely difficult.
Optional updates available	Indicates the number of optional updates available for the Windows operating system.	Number	An optional update includes Feature Pack and standard Updates, and does not have a severity rating.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.