Monitoring Quality Virtual Desktop

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Quality Virtual Desktop is a powerful, open-source virtual desktop infrastructure (VDI) that makes it easy to deploy highly scalable and low-cost solutions to provision any number of users with local and remote access to their Linux desktop environments. QVD provides the perfect way to manage Linux users within large organizations, allowing systems administrators to effectively implement security policies, manage application installation and provision remote desktop access with ease.

QVD virtualizes Linux desktops by using one of two virtualization technologies. Most commonly the Linux Kernel Virtual Machine (KVM) is used as a complete bare-metal hypervisor, however as of QVD 3.1, it is also possible to take advantage of Linux Containers (LXC) to achieve operating-system level virtualization. This virtualization helps to keep each user's environment as its own discrete entity, to improve security and stability.

Regardless of the virtualization technology employed, QVD uses a number of core client-side and server-side components to create a complete QVD solution. In the client-side is the QVD GUI Client. The client software can be installed on any host and is capable of connecting to a VM running on a QVD Server Node.

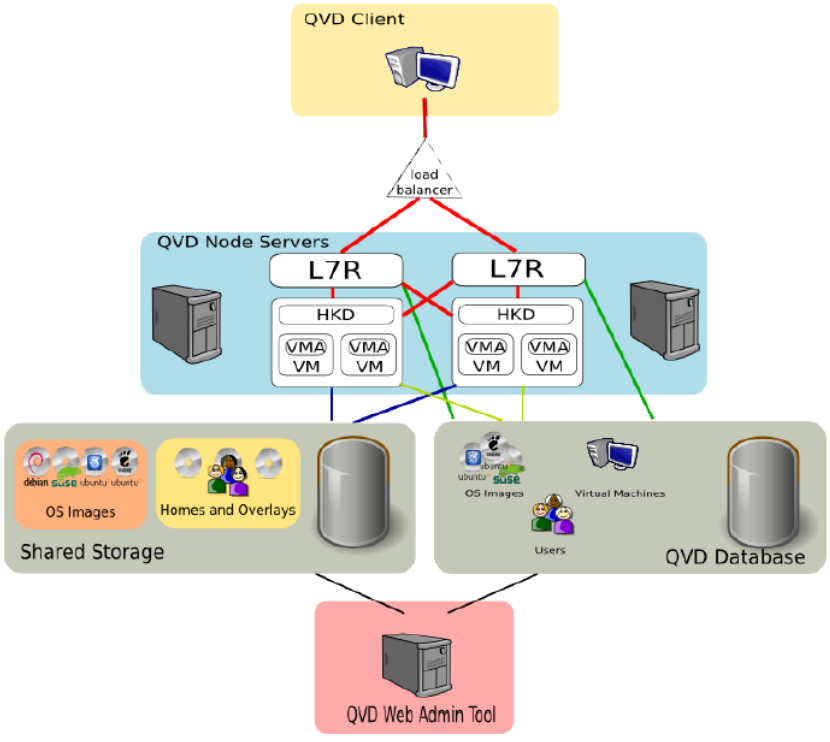

Figure 1.1: The QVD architecture overview

The QVD Server Node is a server-side component. It is a host that runs the QVD Server Node components, including the QVD Node daemon, the L7R daemon and the HKD. A QVD Server Node is responsible for accepting requests from the QVD Client and for loading a VM to serve the client request. QVD is designed to work with clusters of Server Nodes, each running the virtual machines to service different sets of users. The L7R daemon on a Server Node is nothing but the Layer-7 Router, which is responsible for authenticating users and routing client requests to the appropriate Server Node in the cluster that is running the VM for an authenticated user. HKD is the House Keeping Daemon, which is responsible for starting and stopping virtual machines and for performing virtual machine health checking.

Besides the QVD Server Nodes, the following components are also available in the server-side:

- Administration Server: The Administration Server or the QVD Web Admin Tool is a web-based GUI that allows an Administrator to configure and monitor the running of the QVD environment.
- PostgreSQL DBMS: In order to facilitate authentication requests, and to determine which image to load within the Virtual Machine, QVD Server makes use of a PostgreSQL database which is generally referred to as QVD-DB.

Since most QVD deployments comprise of a cluster of Server Nodes, the following components are also becoming common-place in many QVD environments:

- Load Balancer
- Shared Storage Facility (e.g. NFS etc)

Figure 2 depicts how all these components work together.

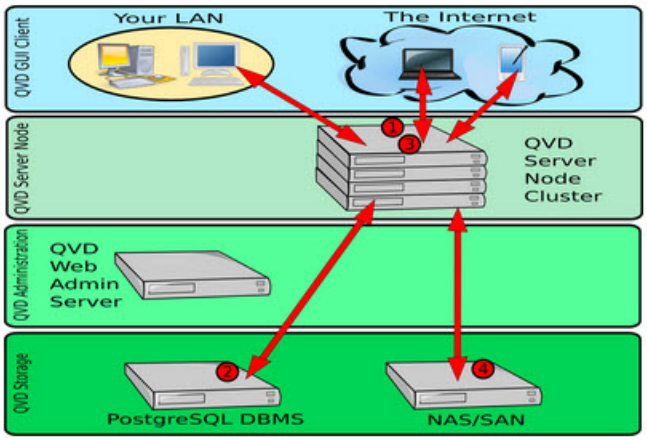

Figure 1.2: How QVD delivers virtual desktops to users?

When a user logs in via a QVD GUI Client and requests for a virtual desktop, the load-balancer routes the request to that Server Node that is least-loaded and has the most resources. The L7R

component within that Server Node connects to the PostgreSQL database to check configuration settings and to authenticate the user. This configuration information is typically entered by an Administrator via the QVD Web Admin Tool.

Once authenticated, the server and client renegotiate an NX protocol connection secured using SSL. The client is then able to connect to a desktop loaded within the allocated virtual machine running on the Server Node. To prepare the desktop for provisioning to a user, prior to any connection from the client, the Server Node will load a disk image from the Shared Storage into VM. Also, when a disk image is available within the Shared Storage, the QVD Web Admin Tool can be used to convert it to an OSF (Operating System Flavor). When the VM is started for a particular user, a qcow image is created for the user's home directory. This is also stored on the Shared Storage. Shared Storage is usually accessed on a mounted network filesystem such as NFS.

As you can see, these client and server-side components closely co-ordinate with each other to deliver desktops to users. This implies that a problem in any one of these components can ripple and affect the performance of the dependent components, thereby slowing down or suspending desktop delivery! Typically, users to the QVD service expect their virtual desktops running on Server Nodes to operate as well (if not better than!) as the physical desktops. Slowdowns in desktop delivery can hence leave users disappointed with the quality of the virtual desktop service, forcing them to either reconsider or worse, shelve, QVD rollout plans! If this is to be avoided, administrators should be able to quickly locate the source of a slowdown in the QVD service – is it the network? the web client? the load balancer? the Server Node? the Virtual Desktop? the PostgreSQL server? Or the Shared Storage? Rapid and accurate root-cause identification can hasten problem resolution, thus ensuring high uptime of the QVD service and an excellent user experience! To achieve this, administrators need visibility into the performance and status of every layer of every tier of the QVD service. This is exactly what eG Enterprise offers!

eG Enterprise offers dedicated monitoring models for each of the component silos engaged in delivering the QVD service. Specialized monitors are available out-of-the-box for the web server hosting the web client, the PostgreSQL database server, the NAS/SAN device hosting the shared storage, and even the routers/switches providing network connectivity to the components. In addition, eG Enterprise also offers extensive monitoring support to the QVD Server Nodes and the virtual desktops running on them. Performance metrics collected from each of these applications are automatically correlated by eG using its patented correlation algorithm – this algorithm analyzes the real-time performance results gathered from the service components in the light of the inter-component dependencies that the eG agent auto-discovers. Based on this analysis, eG Enterprise accurately pinpoints the root-cause of the slowdown!

This document delves deep into how eG Enterprise monitors QVD Server Nodes and their desktops and what performance statistics are obtained from them.

Chapter 2: How does eG Enterprise Monitor the QVD Server Node?

The Quality Virtual Desktop model adopts a **patented In-N-Out** approach to monitoring the QVD Server Node. This approach involves a single eG agent deployed on a remote Windows host in the environment, which remotely connects to the monitored QVD Server Node via SSH, monitors the overall health of the QVD host, and also reports the count and status of desktops configured on that host, from 'outside' the desktops. This is termed as the 'outside view'.

In addition, the eG remote agent connects to each Linux VM on the Server Node via SSH, captures which user logged into which desktop when, closely tracks the activities of a user on a desktop, and reports the impact of these activities on the physical resources of the QVD Server Node. Since this view reveals what happens 'inside' a virtual desktop, it is called the 'inside view'.

2.1 Pre-requisites for monitoring the QVD Server Node

To enable the eG agent to perform In-N-Out monitoring, the following pre-requisites should be fulfilled:

2.1.1 General Prerequisites

- Ensure that the remote agent is able to communicate with the eG manager port (default: 7077).

2.1.2 Pre-requisites for obtaining the 'outside-view' of the virtual desktops

- Ensure that the remote agent has IP connectivity to the QVD Server Node.
- Make sure that the SSH port (default: 22) is enabled for communication between the eG agent and the QVD Server Node.
- Ensure that all the tests executed by the eG agent are configured with the credentials of a user with root permissions.

2.1.3 Pre-requisites for obtaining the 'inside-view' of the virtual desktops

- Ensure that the SSH port (default: 22) is enabled for communication between the eG agent and each of the Linux desktops.
- All the 'inside-view' tests executed by the eG agent on Linux VMs, should be configured with the credentials of a user with *local administrator* privileges. Before doing so, you should make sure

that the same *local administrator* is available on every Linux VM to be monitored or configure multiple users – one for every Linux VM to be monitored.

2.2 Managing the Quality Virtual Desktop

The eG Enterprise cannot automatically discover the Quality Virtual Desktop node so that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a QVD node component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select Quality Virtual Desktop as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

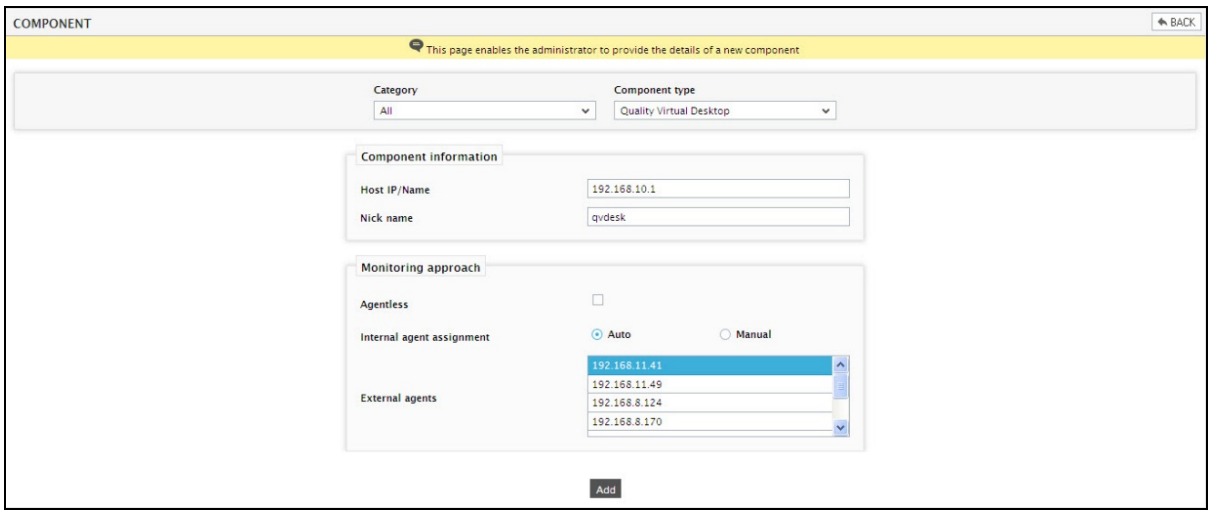

Figure 2.1: Adding a Quality Virtual Desktop server

4. Specify the **Host IP** and the **Nick name** of the Quality Virtual Desktop server in Figure 2.1. Also set the **Agentless** flag to **Yes**, select **Other** as the **OS** and **SNMP** as the **Mode**. Then click the **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

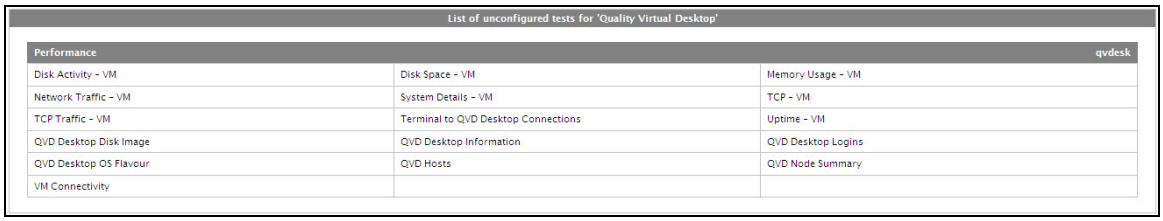

Figure 2.2: List of Unconfigured tests to be configured for the Quality Virtual Desktop server

6. Click on any test in the list of unconfigured tests to configure. For information on configuring these tests, refer to **Monitoring the Quality Virtual Desktop Server Node** chapter.
7. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Quality Virtual Desktop Server Node

The QVD Server Node and the virtual desktops operating on it are key components of a QVD infrastructure. Performance degradations experienced by a QVD Server Node and/or its virtual desktops, if not detected and addressed promptly, can significantly deteriorate the quality of the QVD service. If this is to be avoided, the QVD Server Node and virtual desktops should be monitored 24 x 7 and performance deviations brought to the attention of administrators, well before they become obvious to end-users!

eG Enterprise is capable of deep diving into the performance of a QVD Server Node and the virtual desktops running on it, promptly detecting current/potential deviations in performance, and proactively alerting administrators to them, so that remedial measures can be initiated before users complain. For this purpose, eG Enterprise provides a specialized Quality Virtual Desktop monitoring model.

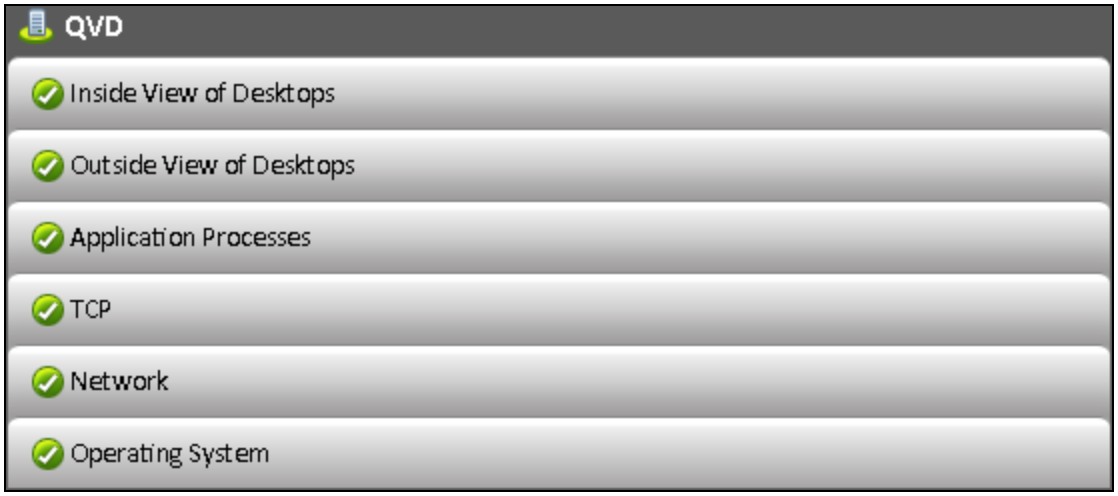

Figure 3.1: The layer model of the Quality Virtual Desktop

Each layer of this model periodically checks the health of host on which the target Server Node is operating, the status of Server Nodes in a cluster, the operational state of the virtual desktops configured on the Server Node, user logins to the virtual desktops, and how a login user uses the desktop, thus pointing to problematic Server Nodes, resource-hungry virtual desktops, and resource-intensive processing that a user may have initiated on the desktop.

Using the metrics collected by the remote agent, administrators can ascertain the following:

- What is the current state of the monitored Server Node? Is the Node blocked?
- Is the Web Client able to successfully negotiate NX connections with the Server Node? Have too many connection attempts failed?
- Is the Server Node able to authenticate user logins properly, or are too many authentication failures occurring?
- Have any Server Nodes in the cluster lost communication with the Web Client? Which Server Nodes are these?
- Which Server Nodes in the cluster are in a Blocked state currently?
- How many Disk Images are available in the shared storage of the monitored QVD Server Node? What are their IDs?
- Which Operating System Flavors (OSFs) have been configured and what is their RAM size?
- How many virtual desktops are assigned to the monitored Server Node? Which desktops are currently powered-off? Are there any blocked desktops on this Server Node? How many desktops on this node have no users logged in currently, and which ones are these?
- Which user has logged into which desktop? How long was he/she logged in?
- Are too many user sessions to desktops, logging out?
- Is any desktop user performing resource-intensive processing on a desktop? If so, which user is this and which virtual desktop is he/she logged in to?

The sections that follow will take you on a layer-by-layer tour of the Quality Virtual Desktop monitoring model. However, since the tests associated with the **Network**, **TCP** and **Application Processes** layers have been already dealt with in detail in the *Monitoring Windows and Unix Servers* document, this chapter will focus on the other layers only.

3.1 The Operating System Layer

Using the tests mapped to this layer, administrators can determine the percentage of physical CPU/disk/memory resources that are used by a QVD Server Node, and thus understand whether/not the node is right-sized. In addition, the tests associated with this layer also monitor the current state of and the load on the target Server Node, and in the process, alert administrators to the abnormal state of the node or a potential overload condition.

Most of the tests of this layer have been dealt with in the *Monitoring Unix and Generic Servers* document, let us now focus on the new tests that have been included in this layer for the QVD Server Node.

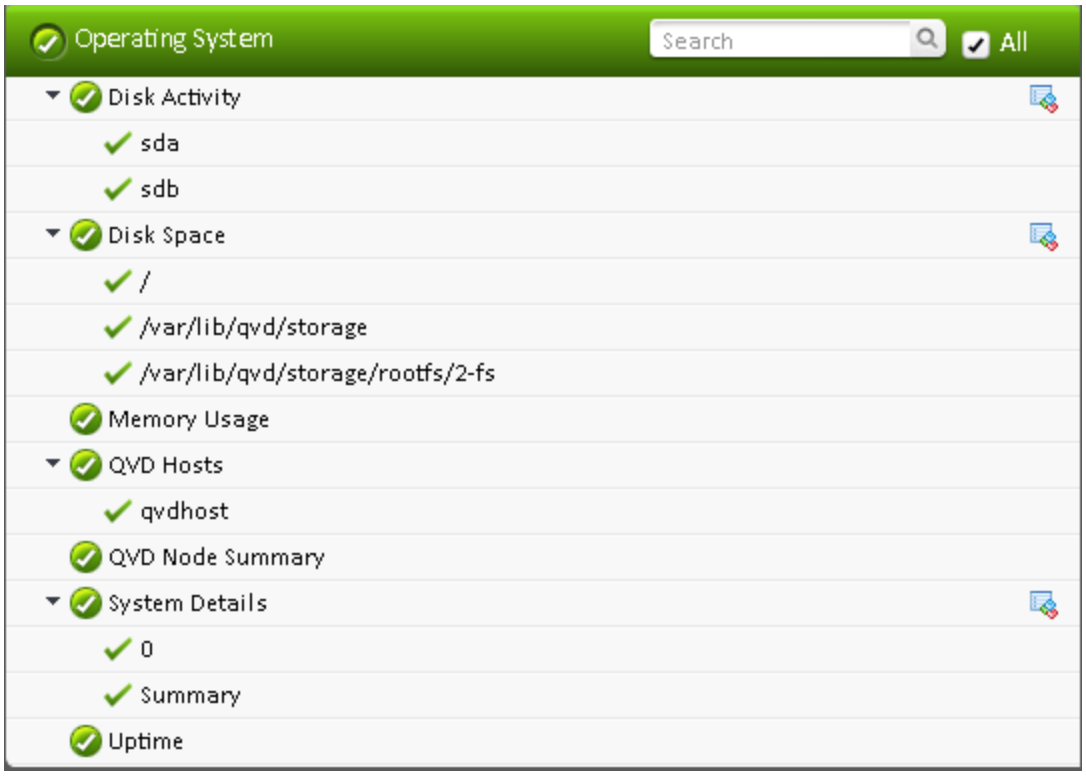

Figure 3.2: The tests mapped to the Operating System layer

3.1.1 QVD Hosts Test

If users complain that their desktop is inaccessible or that it takes too long to connect to their desktop, the powered-on state of the virtual desktop or the network connection to the virtual desktop may not always be the cause of the inaccessibility! Problems with the Server Node – such as the Server Node being stopped, the blocking of the Server Node, the inability of the client to connect to the Server Node, login authentication failures, or a Node overload – can also contribute to such accessibility issues. By keeping an eye on the status and operations of the Server Node, administrators can accurately figure out where the performance of the Server Node is bottlenecked, and quickly initiate measures to clear it, so as to augment the user experience with the QVD service. This is where the **QVD Hosts** test helps! This test continuously tracks the status of, client connections to, the HTTP load on, and the operations of the target Server Node, and proactively alerts administrators to real/potential abnormalities in the overall health, operational efficiency, and processing ability of that Server Node.

Target of the test : A Quality Virtual Desktop Node

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target Server Node being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
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
Node state	Indicates the current state of this Server Node.		The table below displays the States that can be reported by this measure, and their numeric equivalents: State: Starting = 0; Running = 1; Stopping = 2; Stopped = 3; Lost = 4 **Note:**

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure reports one of the **State**s listed in the table above. The graph of this measure however will represent the current state of the Server Node using the numeric equivalents - '0' to '4'. The detailed diagnosis of this measure if enabled, lists the details of each Server Node such as the Time, the ID of the node, IP address of the node and the House Keeping Deamon (HKD) of the node.
Is host blocked?	Indicates whether/not this Server Node is blocked.		Administrators can Block access to a Server Node. This will disable the Server Node from any behavior within the QVD infrastructure. This is effectively the same as shutting down the Server Node, in the sense that to the rest of the environment the Server Node will be unavailable. If the Server Node is currently hosting any number of virtual machines, and a client attempts to connect the client will not be able to access that Virtual Machine and will receive an error notifying it that the server is currently under maintenance. Clients that are already connected to virtual machines running on a Node that has been blocked will remain connected until they are either forced to disconnect by an Administrator or they disconnect of their own accord. This measure reports a value *Yes* if the host is blocked and a value *No* if otherwise. The numeric values that correspond to the measure values discussed above are listed 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>Numeric Value</th><th>Measure Value</th></tr>
<tr><td>1</td><td>Yes</td></tr>
<tr><td>0</td><td>No</td></tr>
</table>
Note:
By default, this measure reports the values Yes or No only to indicate whether the node is blocked or not. In the graph of this measure however, the same is represented using the numeric equivalents - 0 or 1.
</td></tr>
<tr><td>Desktops assigned to node</td><td>Indicates the number of virtual desktops that were assigned to this Server Node.</td><td>Number</td><td>The detailed diagnosis of this measure if enabled, lists the Desktop ID, Name of the Desktop, the user who has been assigned the desktop, IP address of the desktop, the OSF of the desktop, the Disk Image tag of the desktop, the Disk Image of the desktop, the current status of the desktop and whether/not the Server Node is in the Blocked state currently.</td></tr>
<tr><td>HTTP requests</td><td>Indicates the number of HTTP requests handled by this Server Node.</td><td>Number</td><td>This is a good indicator of the workload on the Server Node. A consistent increase in this value over time signals a potential overload condition.</td></tr>
<tr><td>Authentication attempts</td><td>Indicates the number of authentication attempts made by this Server Node.</td><td>Number</td><td>The L7R component within the Server Node connects to the backend PostgreSQL database to determine how authentication should take place (i.e. locally or using an external LDAP directory) and take the appropriate steps to perform the authentication process. The L7R will return an HTTP OK response if the authentication was successful, or will return a 401 Unauthorized if authentication fails.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			If authentication fails, users will not be able to gain access to their virtual desktops. Frequent failures therefore can adversely impact user experience with the desktop delivery service. This is why, the Percentage of successful authentications should be high and the number of Failed authentications should be low. Authentication failures can occur owing to improper configuration of the authentication process, invalid login credentials provided by user at login, and even due to the unavailability/inaccessibility of the PostgreSQL server that stores the configuration.
Successful authentications	Indicates the number of authentication attempts made by this host that were successful.	Number	
Percentage of successful authentications	Indicates the percentage of authentication attempts that were successful.	Percent	
Failed authentications	Indicates the number of authentication attempts that failed.	Number	
NX protocol attempts	Indicates the number of NX protocol attempts made by this Server Node.	Number	The NX protocol is used to handle remote X Windows connections and provides superior compression to allow for high performance even when accessing the desktop over a low-bandwidth connection. Furthermore, the QVD is able to encapsulate the NX protocol with SSL to secure connectivity so that users can work in a safe and secure manner, even if accessing their desktops from remote locations. Failure of NX connections between the client and Server Node causes users to be denied access to their virtual desktops. A high value for the Failed NX protocol attempts measure and a low value for the Percentage of successful attempts measure is hence a cause for concern.
Successful NX protocol attempts	Indicates the number of NX protocol attempts that were successful.	Number	
Percentage of successful attempts	Indicates the percentage of successful NX protocol attempts made by this host.	Percent	
Failed NX protocol attempts	Indicates the number of NX protocol attempts that failed for this host.	Number	

Measurement	Description	Measurement Unit	Interpretation
Short sessions	Indicates the number of sessions that were of short duration on this host.	Number	A high value of this measure could indicate that too many sessions logged out as soon as they logged into the Server Node. This could be owing to a low timeout setting on the node.

The detailed diagnosis of the *Node state* measure (see Figure 3.3) lists the details of each Server Node such as the Time, the ID of the node, IP address of the node and the House Keeping Deamon (HKD) of the host.

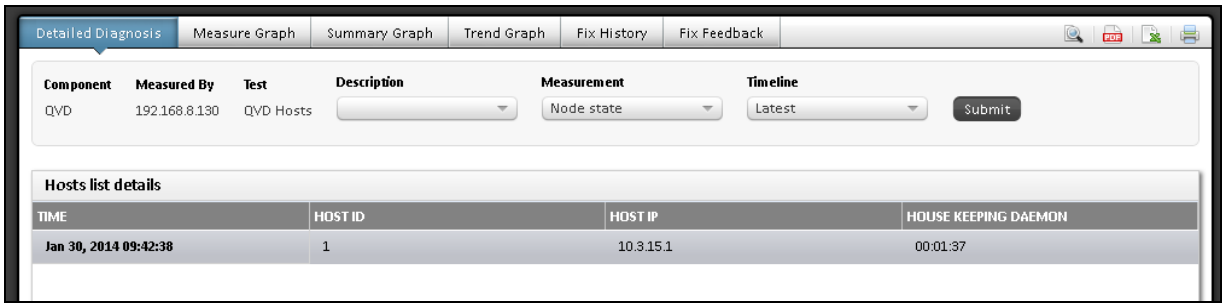

Figure 3.3: The detailed diagnosis of the Node state measure

The detailed diagnosis of the *Desktops assigned to node* measure lists the Desktop ID, Name of the Desktop, the user who has been assigned the desktop, IP address of the desktop, the OSF of the desktop, the Disk Image tag of the desktop, the Disk Image of the desktop, the current status of the desktop and an indicator as to whether the node is blocked or not.

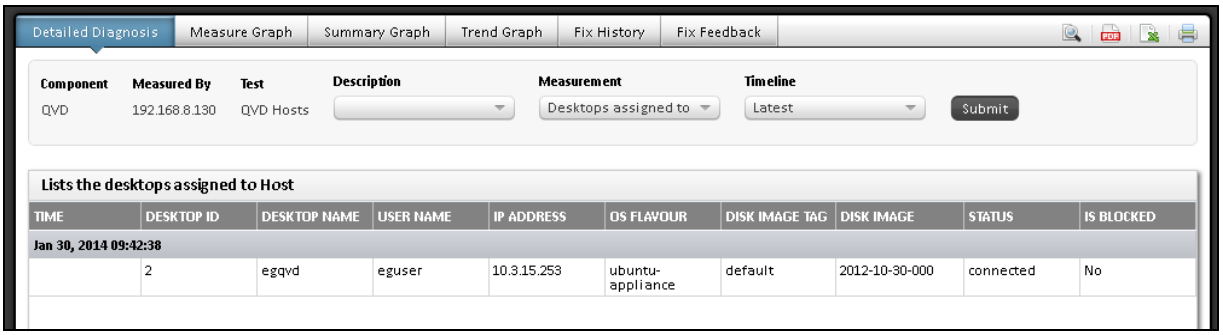

Figure 3.4: The detailed diagnosis of the Desktops assigned to node measure

3.1.2 QVD Node Summary Test

QVD is designed to work with clusters of Server Nodes, each running the virtual machines to service different sets of users. To know which Server Nodes in a cluster are up, running, and ready for use, and which ones are not and why, use the QVD **Node Summary** test. This test monitors the node cluster, reports the status of the nodes in the cluster, and reveals which node is in which state currently.

Target of the test : A Quality Virtual Desktop Node

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the Quality Virtual Desktop being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
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
Total hosts	Indicates the total number of nodes in this Server Node cluster.	Number	The detailed diagnosis of this measure if enabled, lists the ID, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node and whether/not the node is in the Blocked state.
Powered on hosts	Indicates the number of nodes in this Server Node cluster that are powered on currently.	Number	The detailed diagnosis of this measure if enabled, provides the details of the powered-on nodes such as the ID, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node and whether/not the node is in the Blocked state.
Powered off hosts	Indicates the number of nodes in this Server Node cluster that are powered off currently.	Number	The detailed diagnosis of this measure if enabled, provides the details of the powered-off nodes such as the ID, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node and whether/not the node is in the Blocked state.
Starting hosts	Indicates the number of nodes in this cluster that are starting currently.	Number	The detailed diagnosis of this measure if enabled, provides the details of the nodes that are starting; these details include the ID of the node, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node and whether/not the node is in the Blocked state.

Measurement	Description	Measurement Unit	Interpretation
Stopping hosts	Indicates the number of nodes in this cluster that are stopping currently.	Number	The detailed diagnosis of this measure if enabled, provides the details of the nodes that are stopping; these details include the ID of the node, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node and whether/not the node is in the Blocked state.
Lost hosts	Indicates the number of nodes for which connection was lost.	Number	The detailed diagnosis of this measure if enabled, provides the details of the nodes to which connection was lost; these details include the ID of the node, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node and whether/not the node is in the Blocked state.
Blocked hosts	Indicates the number of hosts that are currently blocked.	Number	The detailed diagnosis of this measure if enabled, lists the details of the hosts that are blocked; these details include the ID of the node, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node.

The detailed diagnosis of the *Total hosts* measure (see Figure 3.5) if enabled, lists the ID, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node and whether/not the node is in the.

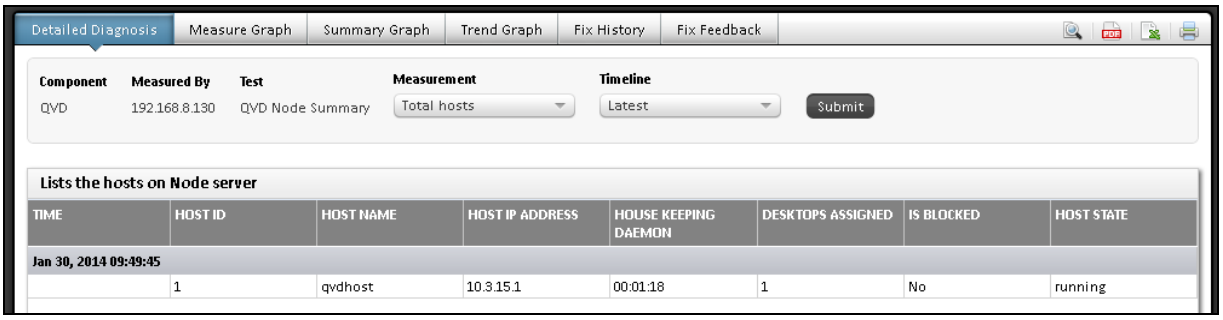

Figure 3.5: The detailed diagnosis of the Total hosts measure

The detailed diagnosis of the *Powered on hosts* measure (see Figure 3.6), provides the details of the powered-on nodes such as the ID, the name of the node, the IP address of the node, the House keeping Daemon of the node, the number of desktops assigned to the node, the current state of the node and whether/not the node is in the Blocked state.

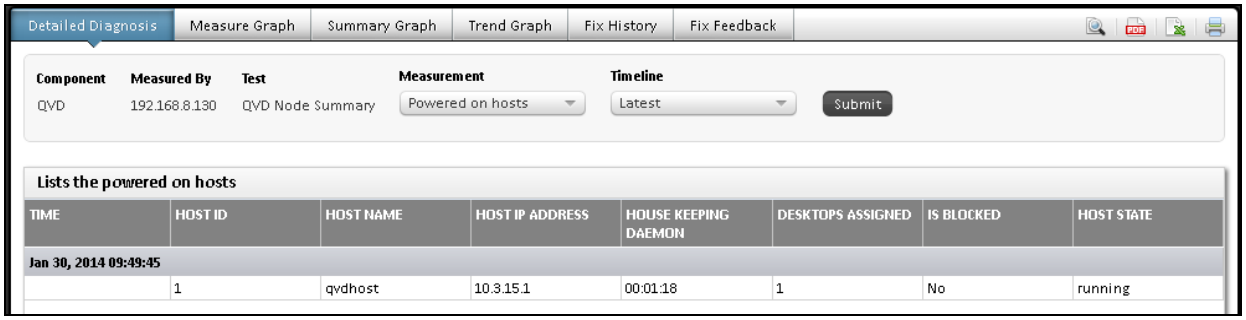

Figure 3.6: The detailed diagnosis of the Powered on hosts measure

3.2 The Outside View of Desktops Layer

This layer provides the host operating system's view of the status of the VMs operating on a Server Node. Using the information reported by this test, administrators can:

- Know which virtual desktops are operating on the target Server Node;
- Track the overall status of the virtual desktops;
- Detect issues in the network connectivity to the virtual desktops;
- Identify the disk images that are stored in the shared storage;
- Figure out the names and memory configurations of the OSFs (Operating System Flavor)

Figure 3.7: The tests mapped to the Outside View of Desktops layer

3.2.1 QVD Desktop Disk Image Test

A Disk Image (DI) is a qcow2 image that has been created as a virtual disk containing an installed operating system.

QVD uses DIs to serve groups of users that make use of a common set of applications. By using a single image to cater to a number of users, it becomes easier to administer desktop environments for all of your users. It also improves overall security, since a policy can be applied to each group of users.

In this way, if a group of users require a particular application, you can install it once and the change will apply to all of the users that share the same DI. Equally, you can remove an application from an entire group's desktop environment.

DIs can easily be duplicated, so that you can quickly create additional environments for different subsets of users. By copying a base image, you can edit the copy and provide additional applications or other customizations to a second set of users without having to repeat a full operating system installation.

This test reports the number of disk images that are available in the Shared Storage of the QVD Server Node.

Target of the test : A Quality Virtual Desktop Node

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the QVD that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
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
Disk images	Indicates the number of disk images that are available in the QVD Server Node.	Number	The detailed diagnosis of this measure if enabled, lists the DISK IMAGE ID, VERSION, PATH and DI TAGS.

The detailed diagnosis of the Disk images measure (see Figure 3.8), lists the DISK IMAGE ID, VERSION, PATH and the DI TAGS.

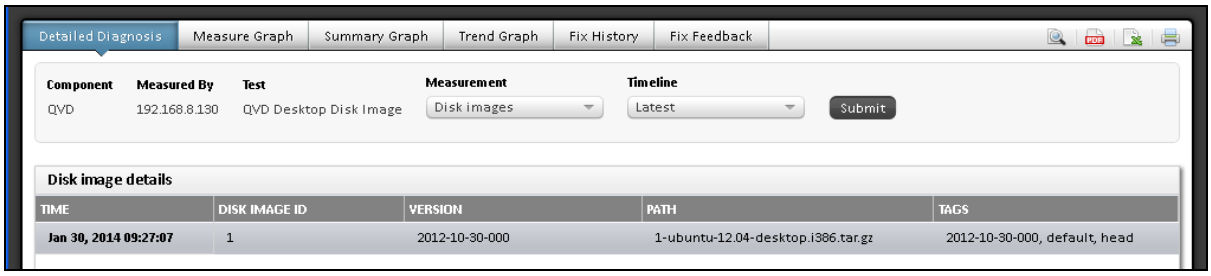

Figure 3.8: The detailed diagnosis of the Disk images measure

3.2.2 QVD Desktop Information Test

When users complain that they are unable to access their virtual desktops, administrators would want to know the reason for the anomaly - is it because the virtual desktop is powered-off? Is it because the virtual desktop is blocked? or is it because the desktop is in a zombie state? Besides desktop status, time and again, administrators may also want to know which desktops are powered-on, but are not effectively used by users – such desktops can be marked for deletion or can at least be powered-off, so as to prevent unnecessary resource consumption. In the same manner, administrators may also want to isolate unregistered desktops, so that they can be registered with the Server Node soon. The **QVD Desktop Information** test provides the inputs administrators require to take these critical decisions! This test reports the number and names of registered desktops on a Server Node, thus indirectly pointing administrators to those desktops that are yet to be registered! In addition, the test indicates the current status of the desktops, so that administrators know which desktops are usable and which are not. Moreover, the test leads administrators to powered-on desktops that have no users logged in, thus revealing idle desktops that can be removed.

Target of the test : A Quality Virtual Desktop Node

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every QVD being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD	Provide the credentials of a user possessing *root user* privileges in the QVD User and

Parameter	Description
Password	QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
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
Registered desktops	Indicates the number of virtual desktops that are registered with the QVD Server Node.	Number	The detailed diagnosis of this measure if enabled, provides the details of each registered desktop – these details include the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.
Powered on desktops	Indicates the number of virtual desktops that are currently powered on.	Number	The detailed diagnosis of this measure if enabled, provides the details of each powered-on desktop – these details include the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.
Powered off desktops	Indicates the number of virtual desktops that are currently powered off.	Number	The detailed diagnosis of this measure if enabled, provides the details of each

Measurement	Description	Measurement Unit	Interpretation
			powered-off desktop – these details include the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.
Starting desktops	Indicates the number of virtual desktops that are currently in the Starting state.	Number	If a desktop is in the Starting state, it could mean either of the following: • That the HKD (House Keeping Daemon) has received the start command but is waiting until it has the resources available to move to the next machine state • That the VM has been started but the boot process has not yet completed The detailed diagnosis of this measure if enabled, provides the details of each desktop in the Starting state – these details include the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.
Stopping desktops	Indicates the number of virtual desktops that are currently in the Stopping state.	Number	If a desktop is said to be in the Stopping state, it could mean either of the following: • That the HKD (House Keeping Daemon) received the stop command but is waiting for the VMA (Virtual Machine Agent) within the VM to respond to the request

Measurement	Description	Measurement Unit	Interpretation
			• That the VMA has responded to the stop request and the VM is in the process of shutting down The detailed diagnosis of this measure if enabled, provides the details of each desktop in the Stopping state – these details include the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.
Desktops in zombie state	Indicates the number of virtual desktops that are currently in the zombie state.	Number	If a desktop is said to be in the Zombie state, it could mean either of the following: • That the VM is running but is not responding, and a TERM signal has been sent to the process • That the VM is running but is not responding, and a KILL signal has been sent to the process The detailed diagnosis of this measure if enabled, provides the details of each desktop in the Zombie state – these details include the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.
Desktops in debugging state	Indicates the number of virtual desktops that are currently in debugging state.	Number	The detailed diagnosis of this measure if enabled, provides the details of each desktop in the debugging state – these details include the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI

Measurement	Description	Measurement Unit	Interpretation
			tag of the desktop and the disk image using which the desktop was created.
Blocked desktops	Indicates the number of virtual desktops that have been blocked by the administrator.	Number	Virtual machines can enter a Blocked state automatically if they fail to start correctly or if there is some problem with their network configuration or with the QVD-VMA that should be running on each virtual machine. However, it is also possible to force the Blocked state using the QVD-WAT. This is usually done if an administrative task needs to be performed on the Virtual Machine, and the administrator does not want anybody to be accessing the virtual machine at the same time. The detailed diagnosis of this measure if enabled, provides details of each blocked desktop – these details include the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.
Desktops with users	Indicates the number of powered on virtual desktops with users logged in.	Number	The detailed diagnosis of this measure if enabled, provides the details of each desktop with a user – these details include, the desktop ID, name of the desktop, the user who is logged into the desktop, IP address, the OSF associated with the desktop, the DI tag of the desktop, the disk image using which the desktop was created and the connection status of the desktop.
Desktops without users	Indicates the number of powered on virtual desktops without any	Number	The detailed diagnosis of this measure if enabled, provides the details of

Measurement	Description	Measurement Unit	Interpretation
	users logged in.		desktops to which no user is currently logged in – such details include, the desktop ID, name of the desktop, the user who is registered with the desktop during desktop creation, IP address, the OSF associated with the desktop, the DI tag of the desktop, the disk image using which the desktop was created and the connection status of the desktop.

The detailed diagnosis of the *Registered desktops* measure (see Figure 3.9), lists the details of each registered desktop such as the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.

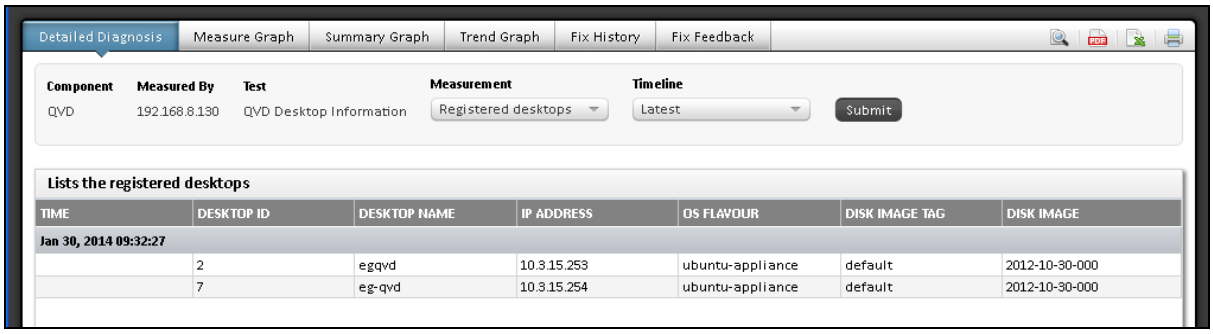

Figure 3.9: The detailed diagnosis of the Registered desktops measure

The detailed diagnosis of the *Powered on desktops* measure (see Figure 3.10) lists the details of each powered on desktop such as the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.

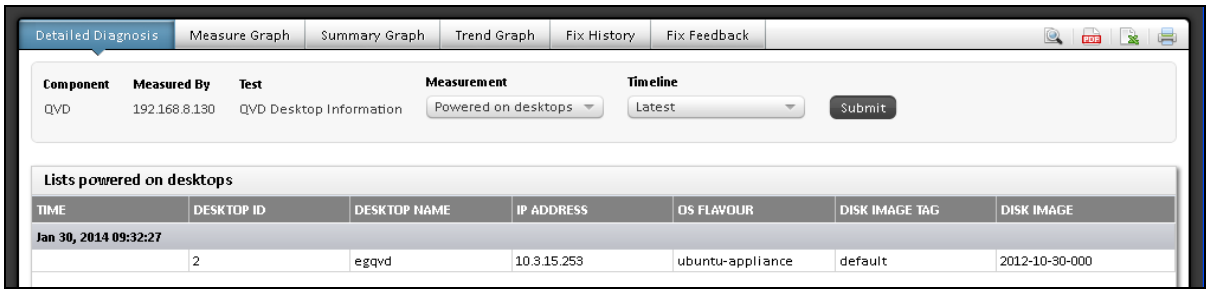

Figure 3.10: The detailed diagnosis of the Powered on desktops measure

The detailed diagnosis of the *Powered off desktops* measure (see Figure 3.11) lists the details of each powered off desktop such as the desktop ID, name of the desktop, the IP address, the OSF associated with the desktop, the DI tag of the desktop and the disk image using which the desktop was created.

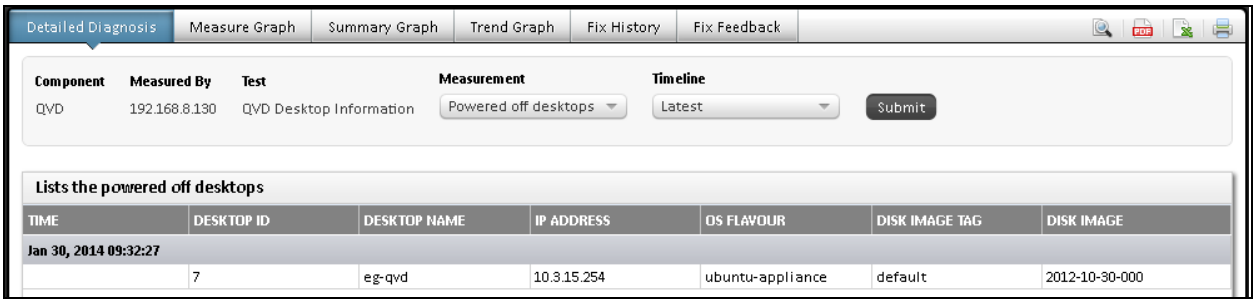

Figure 3.11: The detailed diagnosis of the Powered off desktops measure

3.2.3 QVD Desktop Logins Test

Administrators can track user logins to virtual desktops with the help of the **QVD Desktop Logins** test. This test monitors user sessions to the virtual desktops on a target Server Node and reports the total count of the logins and logouts. This way, administrators can determine the load on the desktops and identify sessions that abruptly logged out from desktops.

Target of the test : A Quality Virtual Desktop Node

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the QVD that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
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
Current sessions	Indicates the number of desktop user sessions that are currently active on the QVD Server Node.	Number	This measure is a good indicator of the load on the QVD Server Node.
New logins	Indicates the number of new desktop user logins to the QVD Server Node during the last measurement period.	Number	A consistent zero value could often indicate a connection issue. The detailed diagnosis of this measure if enabled, lists the name of the desktop, the name of the user logged into the desktop and the logged in time of the user.

Measurement	Description	Measurement Unit	Interpretation
Percentage of new logins	Indicates the percentage of new desktop users who logged in to the QVD Server Node during the last measurement period.	Percent	
Sessions logging out	Indicates the number of user sessions that logged out from the QVD Server Node.	Number	A sudden log out of all the sessions, indicates a problem situation which requires further investigation. The detailed diagnosis of this measure if enabled, lists the DESKTOP NAME, USER NAME, LOGIN TIME and the DURATION (MINS).

The detailed diagnosis of the *New logins* measure (see Figure 3.12), lists the name of the desktop, the name of the user logged into the desktop and the logged in time of the user.

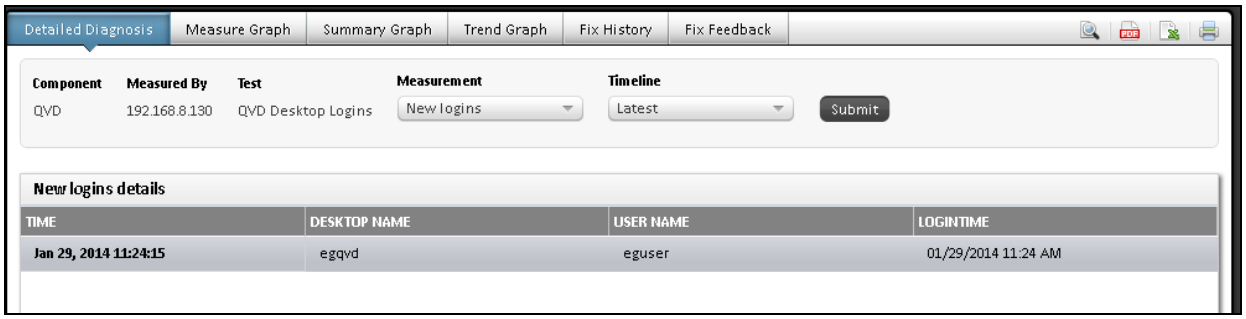

Figure 3.12: The detailed diagnosis of the New logins measure

3.2.4 QVD Desktop OS Flavour Test

An Operating System Flavour (OSF) is loaded into any number of virtual machines on a QVD Server Node in order to serve a virual desktop to a client. The OSF is usually installed into QVD along with particular runtime parameters such as the amount of system memory that should be available to it.

This test auto-discovers the Operating System Flavours configured on the QVD and reports the total memory size of each OSF. In addition, this test indicates if overlay is enabled on each OSF.

Target of the test : A Quality Virtual Desktop Node

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every OSF being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
RAM	Indicates the total memory size of this Operating System Flavour.	MB	
Overlay	Indicates whether/not overlay is enabled on this Operating System Flavour.		Virtual Machines make use of overlays in order to best utilize different elements of the Guest operating system, and in order to make particular elements persistent. For instance, while write activity is not persistent within the actual OSF that is loaded, it is important that data written to the user's home folder or desktop is stored for future connections to the virtual desktop. Overlays can also be used to make other data such as log and tmp files persistent from a user perspective. This measure reports a value *Yes* if the overlay is enabled and a value *No* if otherwise. The numeric values that correspond to the measure values discussed above

Measurement	Description	Measurement Unit	Interpretation
			are listed in the table below: Numeric Value: Measure Value 1: Yes 0: No **Note:** By default, this measure reports the values Yes or No only to indicate whether the overlay is enabled or not. The graph of this measure however, is represented using the numeric equivalents - 0 or 1.

3.2.5 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 Quality Virtual Desktop Node

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each VM configured on the QVD server host being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD	Provide the credentials of a user possessing *root user* privileges in the QVD User and

Parameter	Description
Password	QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
PacketSize	The size of packets used for the test (in bytes).
PacketCount	The number of packets to be transmitted during the test.
Timeout	How long after transmission should a packet be deemed lost (in seconds).
PacketInterval	Represents the interval (in milliseconds) between successive packet transmissions during the execution of the network test for a specific target.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted 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.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can

Parameter	Description
	hence be ignored.
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
Average 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.
Minimum 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	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.

3.3 The Inside View of Desktops Layer

The tests mapped to the **Inside View of Desktops** layer provide an "inside" view of the workings of each of the guests - these tests execute on a QVD server host, but send probes into each of the guest operating systems to analyze how well each virtual desktop 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 Desktops** layer, does not display the list of tests associated with that layer. Instead, Figure 3.13 appears. This figure provides you with a list of all the virtual desktops and their respective state (see Figure 3.13).

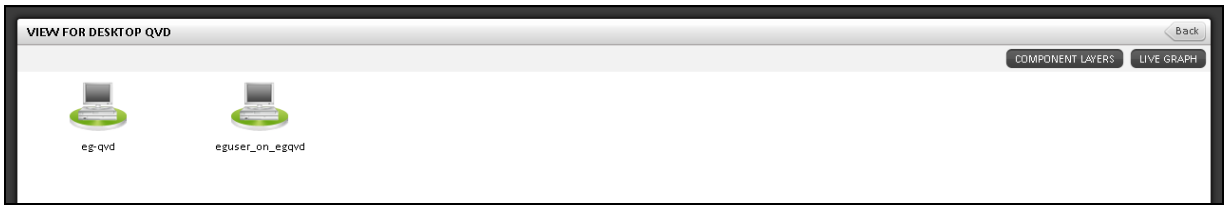

Figure 3.13: A list of guest operating systems on a QVD server host and their current state

To return to the layer model of the Quality Virtual Desktop and view the tests associated with the **Inside View of Desktops** layer, click on the component layers link in Figure 3.13. You can now view the list of tests mapped to the **Inside View of Desktops** layer, as depicted by Figure 3.14 below.

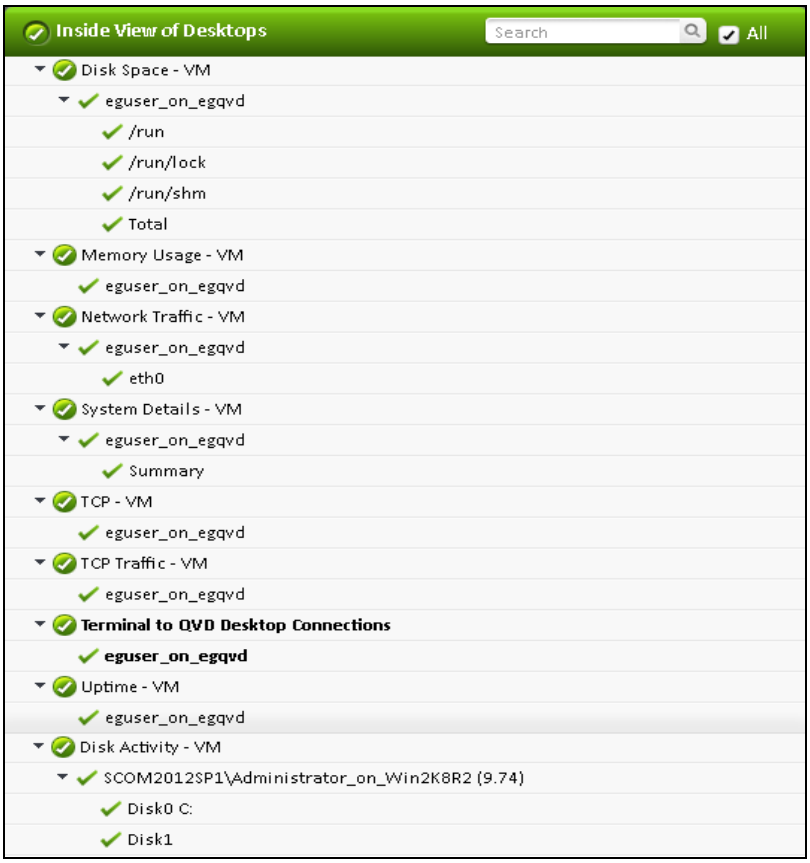

Figure 3.14: The tests mapped to the Inside View of Desktops layer

3.3.1 Disk Activity - VM Test

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

Target of the test : A Quality Virtual Desktop Server Host

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

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.

Parameter	Description
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted 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.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
Domain, Admin	By default, this test connects to each virtual guest remotely and attempts to collect

Parameter	Description
User, Admin Password, and Confirm Password	"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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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 Section **3.4**.
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default; which 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*.
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 virtual machine 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.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the

Parameter	Description
	detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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
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	Secs	

Measurement	Description	Measurement Unit	Interpretation
	data from the 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 local disk per second.	Writes/Sec	A dramatic increase in this value may be indicative of an I/O bottleneck on the guest.
Data writes to virtual disk	Indicates the rate at which bytes are transferred from the disk during write operations.	KB/Sec	A very high value indicates an I/O bottleneck on the guest.

3.3.2 Disk Space - VM Test

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

Target of the test : A Quality Virtual Desktop Server Host

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

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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.

Parameter	Description
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted 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.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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 Section **3.4**.
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default;

Parameter	Description
	which 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*.
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 virtual machine 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.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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
Total capacity	Indicates the total capacity of a disk partition; for the Total descriptor, this	MB	

Measurement	Description	Measurement Unit	Interpretation
	measure reports the sum of the total capacity of all disk partitions.		
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.

3.3.3 Memory Usage - VM Test

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

Target of the test : A Quality Virtual Desktop Server Host

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 Quality Virtual Desktop server monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted list of VMs/VM name patterns in the Exclude VMs text box, you can make sure the eG agent

Parameter	Description
	stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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 Section **3.4**.
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default; which 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*.
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 virtual machine 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

Parameter	Description
	currently.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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
Total physical memory	Indicates the total physical memory of this VM.	MB	
Used physical memory	Indicates the used physical memory of this VM.	MB	
Free physical memory	Indicates the free physical memory of the VM.	MB	This measure typically indicates the amount of memory available for use by applications running on the target VM. On Unix operating systems (AIX and Linux), the operating system tends to use parts of the available memory for caching files, objects, etc. When applications require additional

Measurement	Description	Measurement Unit	Interpretation
			memory, this is released from the operating system cache. Hence, to understand the true free memory that is available to applications, the eG agent reports the sum of the free physical memory and the operating system cache memory size as the value of the Free physical memory measure while monitoring AIX and Linux guest operating systems.
Physical memory utilized	Indicates the percent usage of physical memory by this VM.	Percent	Ideally, the value of this measure should be low. While sporadic spikes in memory usage could be caused by one/more rogue processes on the VM, a consistent increase in this value could be a cause for some serious concern, as it indicates a gradual, but steady erosion of valuable memory resources. If this unhealthy trend is not repaired soon, it could severely hamper VM performance, causing anything from a slowdown to a complete system meltdown. You can use the detailed diagnosis of this measure to figure out which processes on the VM are consuming memory excessively.

Note:

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

3.3.4 Network Traffic - VM Test

This is an internal test that monitors the incoming and outgoing traffic through each virtual desktop on a QVD server.

Target of the test : A Quality Virtual Desktop Server Host

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

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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

Parameter	Description
	default.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted 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.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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 Section **3.4**.

Parameter	Description
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default; which 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*.
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 virtual machine 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.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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
Incoming traffic	Indicates the rate of incoming traffic.	Pkts/Sec	An increase in traffic to the guest can indicate an increase in accesses to the

Measurement	Description	Measurement Unit	Interpretation
			guest (from users or from other applications) or that the guest is under an attack of some form.
Outgoing traffic	Indicates 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).

3.3.5 System Details - VM Test

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

Target of the test : A Quality Virtual Desktop Server Host

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

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. Here, the * (asterisk) is used to denote leading and trailing

Parameter	Description
	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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted 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.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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.

Parameter	Description
	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 Section **3.4**.
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default; which 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*.
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 virtual machine 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.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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:

Parameter	Description
	• 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

Measurement	Description	Measurement Unit	Interpretation
			consumption and look to tune their memory usages and allocations accordingly.
Free memory in VM	Indicates the free memory available.	MB	A very low value of free memory is also an indication of high memory utilization on a guest.
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 3.15). 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.

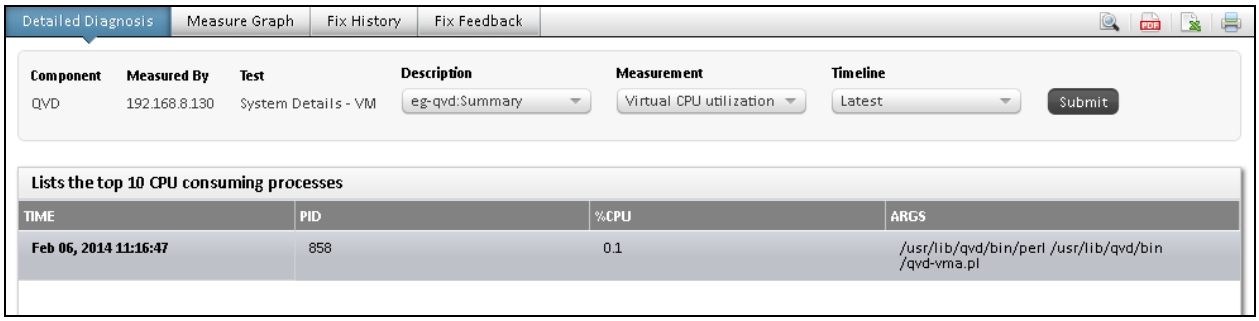

Figure 3.15: The top 10 CPU consuming processes

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.

3.3.6 Tcp - VM Test

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

Target of the test : A Quality Virtual Desktop Server Host

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 Quality Virtual Desktop server monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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

Parameter	Description
	default.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted 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.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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 Section **3.4**.

Parameter	Description
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default; which 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*.
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 virtual machine 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.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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
Incoming connections to VM	Indicates the connections per second received by the	Conns/Sec	A high value can indicate an increase in input load.

Measurement	Description	Measurement Unit	Interpretation
	guest.		
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 connections being dropped without completion.

3.3.7 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 Quality Virtual Desktop Server Host

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 Quality Virtual Desktop server monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their

Parameter	Description
	less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted 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.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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 Section **3.4**.
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default; which implies that in case of VDI servers, by default, the guests will be identified using

Parameter	Description
	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*.
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 virtual machine 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.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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
Segments received by VM	Indicates the rate at which segments are received by the guest.	Segments/Sec	
Segments sent by	Indicates the rate at which	Segments/Sec	

Measurement	Description	Measurement Unit	Interpretation
VM	segments are sent to clients or other guests.		
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 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.

3.3.8 Terminal to QVD Desktop Connections Test

The Terminal to QVD Desktop Connection test is executed by the eG agent on a QVD server host. This test auto-discovers the virtual desktops on the QVD Server Node, the users who are currently logged on to each of the virtual desktops, and the IP address from which they are connecting to the virtual desktops. For each user, the test monitors the quality of the link between the client and the virtual desktop.

Using this test, an administrator can identify user sessions that are being impacted by high latencies or by excessive packet drops. In some cases, a virtual desktop may regard a user session as active, even though the network link connecting the user terminal to the virtual desktop has failed. The Terminal to Desktop Connection test alerts administrators to such situations.

Target of the test : A Quality Virtual Desktop Server Host

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every QVD being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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

Parameter	Description
	views of all VMs on a virtual host by default. By providing a comma-separted 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.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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 Section **3.4**.
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default; which 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*.
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 virtual machine name and not by the username_

Parameter	Description
	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.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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 current number of sessions for a particular user.	Number	The value 0 indicates that the user is not currently connected to the virtual desktop.
Average delay	Indicates the average delay between transmission of a request by the agent on a virtual desktop and receipt of the response back from the 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.
Minimum delay	Indicates the minimum	Secs	A significant increase in the minimum round-trip time is often a sure sign of a

Measurement	Description	Measurement Unit	Interpretation
	delay between transmission of a request by the agent on a virtual desktop and receipt of the response back from the user terminal.		poor link between the desktop and a user's terminal.
Packet loss	Indicates the percentage of packets lost during data exchange between the virtual desktop and the user terminal.	Percent	Comparing the value of this measure across users will enable administrators to quickly and accurately identify users who are experiencing slowdowns because of poor performance on the network links between their terminals and the virtual desktop.

3.3.9 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 Quality Virtual Desktop server.

Target of the test : A Quality Virtual Desktop Server Host

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each guest discovered on the Quality Virtual Desktop server being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port number at which the specified host listens to. By default, this is *NULL*.
QVD User and QVD Password	Provide the credentials of a user possessing *root user* privileges in the QVD User and QVD Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Ignore VMs Inside View	Administrators of some high security 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: **ubuntu*,*lin*,rhel*,*suse**. 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 QVD host by default configured to **not obtain the 'inside view' of such 'inaccessible' VMs** using the Ignore VMs Inside View parameter. **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.
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.
Exclude VMs	Administrators of some virtualized environments may not want to monitor some of their less-critical VMs - for instance, VM templates - both from 'outside' and from 'inside'. The eG agent in this case can be configured to completely exclude such VMs from its monitoring purview. To achieve this, provide a comm-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: **ubuntu*,*lin*,rhel*,*suse**. 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-separted list of VMs/VM name patterns in the Exclude VMs text box, you can make sure the eG agent

Parameter	Description
	stops collecting 'inside' and 'outside' view metrics for a configured set of VMs.
Inside View Using	This parameter applies only to virtualized environments supporting Windows VMs. Since QVD supports only Linux VMs, this parameter is not relevant for QVD and can hence be ignored.
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. For this, you need to specify a domain name, an admin user name, and an admin password. Since QVD supports only Linux guests, specify "*none*" in the Domain field, and specify a local administrator account name in the Admin User text box. Prior to this, you need to ensure that the same local administrator account is available or is explicitly created on each of the virtual machines to be monitored. 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 Section **3.4**.
Report By User	While monitoring virtualized desktop environments, this flag is set to **Yes** by default; which 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*.
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 virtual machine 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

Parameter	Description
	currently.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
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
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	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

Measurement	Description	Measurement Unit	Interpretation
			less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the VM was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period - the smaller the measurement period, greater the accuracy.
Total uptime	Indicates the total time that the guest has been up since its last reboot.		This measure displays the number of years, months, days, hours, minutes and seconds since the last reboot. 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.

3.4 Troubleshooting

By default, the eG agent uses secure shell (SSH) to connect to Linux guests, and collect performance metrics from them. Password Authentication is the default method for SSH connections in eG Enterprise. If the eG agent fails to report measures for a Linux guest or is unable to connect to a guest, it could imply that the Linux guest does not support SSH or that password authentication is not supported by the SSH daemon running on the Linux guest. Under such circumstances, you can perform either of the following:

- Enable Password Authentication in the SSH daemon on the Linux guest; or,
- Implement Key-Based Authentication between eG agent and the SSH daemon of the Linux guest.

If you pick option (1), then follow the steps given below to enable password authentication:

- Login to the Linux guest to be monitored.
- Edit the **sshd_config** file in the **/etc/ssh** directory.

- Check whether the **Password Authentication** flag in the **sshd_config** file is set to **no**. If so, set it to **yes**.
- Then, save the file and restart/signal the SSH daemon (eg., using **kill -1 <sshd_config PID>**).

On the contrary, if you choose to enable key-based authentication [i.e, option (2)], then you will have to generate a public/private key pair. A public/private key pair is available in the <EG_INSTALL_DIR>\agent\sshkeys directory (on Windows; on Unix, this will be /opt/egurkha/agent/sshkeys) of the eG agent. While the private key is available in the file named **id_rsa**, the public key is contained within the file authorized_keys. You now have the option to proceed with the default keys or generate a different key pair. If you decide to go with the keys bundled with the eG agent, do the following:

- To enable key-based authentication, the private key should remain in the <EG_INSTALL_DIR>\agent\sshkeys directory (on Windows; on Unix, this will be /opt/egurkha/agent/sshkeys), and the public key should be copied to each of the Linux guests to be monitored. To achieve this, first login to the Linux guest to be monitored as the eG user.
- Create a directory named **.ssh** in the <USER_HOME_DIR> on the guest operating system, using the command: **mkdir ~/.ssh**.
- Next, copy the authorized_keys file from the <EG_INSTALL_DIR>\agent\sshkeys directory (on Windows; on Unix, this will be /opt/egurkha/agent/sshkeys) on the eG remote agent host to the <USER_HOME_DIR>/.ssh directory on the Linux guest.
- Make sure that the permission of the **.ssh** directory and the authorized_keys file is 700.
- Finally, on the eG manager host, edit the <EG_INSTALL_DIR>\manager\config\eg_tests.ini file. Against the **EgJavaSSHKeyFile** parameter, enter: **agent/sshkeys/id_rsa.pub**, and save the file.

On the other hand, if you want to generate a new key pair, then do the following:

- Login to any Linux host in your environment (even a Linux VM) as an eG user.
- From the <USER_HOME_DIR>, execute the command: **ssh-keygen -t rsa**. Upon executing the command, you will be requested to specify the full path to the file to which the key is to be saved. By default, a directory named **.ssh** will be created in the <USER_HOME_DIR>, to which the key pair will be saved. To go with the default location, simply press **Enter**.

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/egurkha/.ssh/id_rsa):
```

- Next, you will be prompted to provide a pass phrase. Provide any pass phrase of your choice.

```
Enter passphrase (empty for no passphrase): eginnovations
Enter same passphrase again: eginnovations
```

- If the key pair is created successfully, then the following messages will appear:

```
Your identification has been saved in /home/egurkha/.ssh/id_rsa.
Your public key has been saved in /home/egurkha/.ssh/id_rsa.pub.
The key fingerprint is:
09:f4:02:3f:7d:00:4a:b4:6d:b9:2f:c1:cb:cf:0e:e1 dclements@sde4.freshwater.com
```

- The messages indicate that the private key has been saved to a file named **id_rsa** in the <USER_HOME_DIR>/.ssh, and the public key has been saved to a file named **id_rsa.pub** in the same directory. Now, to enable key-based authentication, login to the Linux guest to be monitored as the eG user.
- Create a directory named **.ssh** in the <USER_HOME_DIR> on the guest operating system, using the command: **mkdir ~/.ssh**.
- Next, copy the **id_rsa.pub** file from the <USER_HOME_DIR>/.ssh directory on the Linux host to the <USER_HOME_DIR>/.ssh directory on the Linux guest.
- Ensure that the **id_rsa.pub** file on the Linux guest is renamed as **authorized_keys**.
- Repeat this procedure on every Linux guest to be monitored.
- Then, lock the file permissions down to prevent other users from being able to read the key pair data, using the following commands:

```
chmod go-w ~/chmod 700 ~/.sshchmod go-rwx ~/.ssh/*
```

- Finally, on the eG manager host, edit the <EG_INSTALL_DIR>\manager\config\eg_tests.ini file. Against the **EgJavaSSHKeyFile** parameter, enter: **agent/sshkeys/id_rsa.pub**, and save the file.

Instead of choosing between the authentication modes (Password or Key-based), you can also disable the usage of the Java SSH client, and use **plink** to connect to Linux guests. To achieve this, follow the steps given below:

- Edit the **eg_tests.ini** file in the /opt/egurkha/manager/config directory (on Unix; on Windows, this will be <EG_INSTALL_DIR>manager\config directory).
- Set the **JavaSSHForVm** flag in the **[AGENT_SETTINGS]** section of the file to **false**; by default, this is set to **true** indicating that the eG agent uses Java SSH by default. By setting the flag to **false**, you can ensure that the eG agent does not use Java SSH, and instead uses the **plink** command to connect to Linux guests.
- The **plink** command exists in the <EG_INSTALL_DIR>\lib\vmgfiles directory (on Windows; on

Unix, this will be /opt/egurkha/lib/vmgfiles) of the eG agent. To use the **plink** command, you need to explicitly configure the SSH keys, so that the eG agent is able to communicate with the Linux guests using SSH. To do this, follow the steps given below:

- Go to the command prompt and switch to the directory containing the **plink** command.
- Then, execute the **plink** command to connect to any of the Linux-based virtual machines on the vSphere host. The syntax for the **plink** command is as follows:

```
plink -ssh <user>@<IP_of_target_host> <command>
```

For example, assume that you want to connect to the virtual machine, **192.168.10.7**, as user **john** with password **john**, to know its hostname. The syntax of the **plink** command in this case will be:

plink -ssh john@192.168.10.7 hostname, where **hostname** is the command to be executed on the remote host for extracting its hostname.

- To ensure that you do not connect to an imposter host, **SSH2.x** presents you with a unique host key fingerprint for that host, and requests your confirmation to save the displayed host key to the cache.

```
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:<host key>

If you trust this host, enter "y" to add the key to PuTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, enter "n".

If you do not trust this host, press Return to abandon the connection.

Store key in cache? (y/n) y
```

Once you confirm the host key storage and provide the user's password to connect to the virtual guest, this message will not appear during your subsequent attempts to connect to any Linux-based virtual machine on the monitored vSphere/ESX host. In other words, the eG agent will be able to execute tests on all Linux guests on the target ESX host without any interruption. Therefore, press **y** to confirm key storage.

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.