Monitoring VMware Horizon Connection Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

VMware Horizon View is a commercial desktop-virtualization product developed by VMware, Inc., which provides remote desktop capabilities to users using VMware's virtualization technology.

Virtual desktops provide several advantages over traditional full workstations including easier management and simpler provisioning. Desktop virtualization takes a user's desktop workstation and stores it on a central server as a virtual machine. The user can then access it from anywhere using a small remote client application, which is referred to as a thin client. Thin clients can be either low-cost dedicated hardware devices that are basically just a monitor, keyboard and mouse, or an application installed on any type of PC. Because the desktop is hosted on a powerful server that handles all the processing for the desktop, the thin client has very small resource requirements and does not need to be that powerful. The only data that is sent back and forth between the thin client and the hosted server are video, keyboard/mouse inputs and peripheral connections (USB drives/printers).

VMware Horizon View leverages vSphere as the virtual desktop host platform; in other words, user desktops are virtual machines running on ESX/ESXi hosts. They can take full advantage of all the features built into vSphere like VMotion, snapshots, Distributed Resource Scheduler (DRS) and more.

View uses a special protocol to send data back and forth between the thin client and the hosted virtual machine. The Microsoft Remote Desktop Protocol (RDP) has been the protocol that has been used by View, but a new higher-performing protocol called PC over IP (PCoIP) was recently introduced with View version 4. PCoIP is intended to overcome some of the limitations that RDP experienced with high-resolution desktops and complex graphics situations. PCoIP enables View to deliver a much smoother experience to end users and is able to handle streaming video, high-definition audio and high resolution graphics. The RDP protocol is still available in View and can be used for lower-demand situations and lower-bandwidth connections between the thin client and the hosted virtual machines.

To recap, VMware Horizon View virtual desktops run on a thin client that uses either a RDP or PCoIP protocol to connect to a virtual machine (View Desktop) running on an ESX/ESXi host. There, are, however, additional components used to manage the connection, provisioning, authentication and applications.

The below image depicts the components of VMware Horizon View:

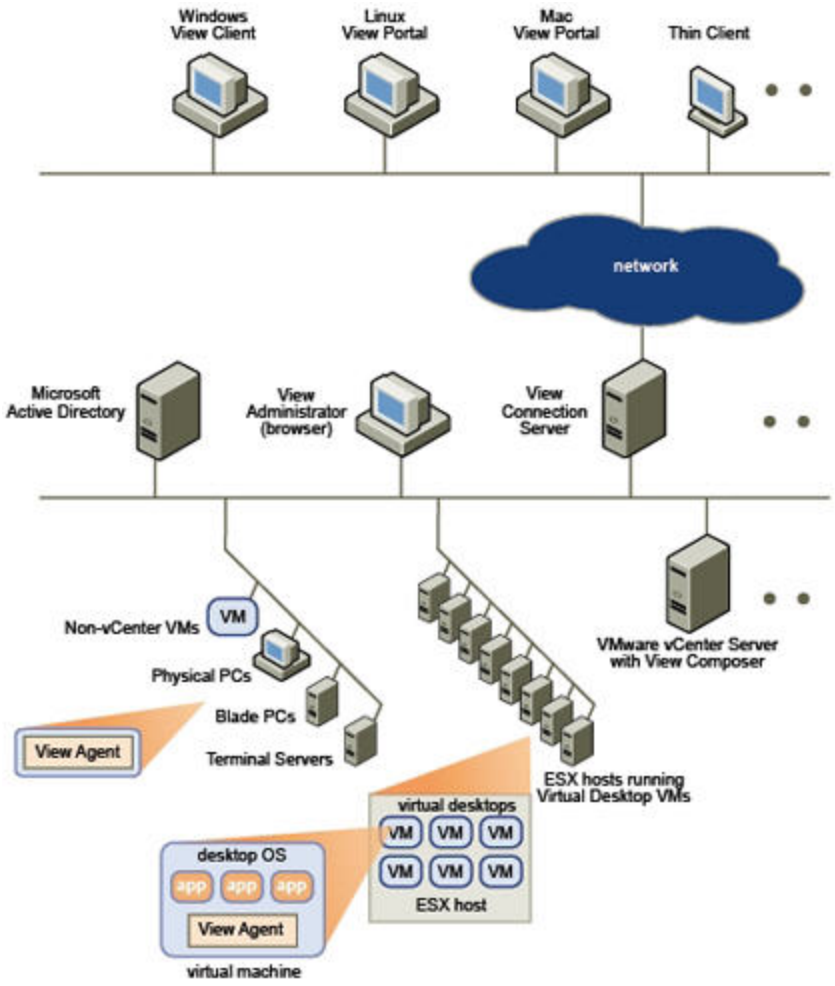

Figure 1.1: The core components of VMware Horizon View

a. **View Client** - This can be a dedicated thin client terminal or a desktop/laptop with a client application running on it. Optionally a View Portal is also available for connections made through a web browser.

b. **Display Protocol** - Used for the communication between the View Client and View desktop. Can be either Microsoft RDP, VMware PCoIP or Hewlett-Packard's (HP's) RDS used on HP blade servers.

c. **View Connection Server** - This is the broker for all View Client connections to View Desktops. Before a client can connect to a desktop it may stop at the broker where it is first authenticated via Active Directory/Lightweight Directory Access Protocol and then securely connect to a desktop. The broker can also apply policies, check entitlements and manage the desktop sessions. This is also known as VMware Horizon View Manager.

d. **View Desktop** - This is usually a virtual machine stored on an ESX/ESXi host, but can also be a physical desktop or Terminal Server. A View agent is installed on any of these devices and communicates with the View Client to monitor the connection and provide printing and USB features.

e. **View Composer** - This is an optional application that can help to reduce the amount of disk space that View Desktops take up on host server data stores. It does this by using a base disk image for many View Desktops and using linked clones of the image to store any data changes from the standard image for each desktop. If you're familiar with snapshots in VMware, it is pretty much the same concept.

f. **ThinApp** - Another optional application that encapsulates user applications (i.e. Microsoft Office) so they are not tied into the operating system, which greatly simplifies application deployment. Applications are packaged into a virtual OS as a single executable file, so there is no need to install it on a user's desktop - it can simply be executed. This separation from the OS makes View desktops much easier to manage and deploy.

If any of these components fail or exhibit unhealthy performance patterns, it may delay or even deny users access to desktops, thus severely impacting the user experience with the desktop service. To avoid such adversities, the operations and all-round health of each component of the VMware Horizon View Connection server should be continuously monitored. The eG Enterprise helps administrators in continuous monitoring of VMware Horizon Connection Server.

Chapter 2: Managing VMware Horizon View Connection Server

eG Enterprise can automatically discover the VMware Horizon View Connection Server, and also lets you to manually add the component for monitoring. To manage a VMware Horizon View Connection Server, do the following:

1. Log into the eG admin interface.
2. If the VMware Horizon View Connection Server is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page.
3. However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **COMPONENTS** page. Remember that components manually added are managed automatically.
4. In the **COMPONENT** page that appears next, select *VMware Horizon View Connection Server* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

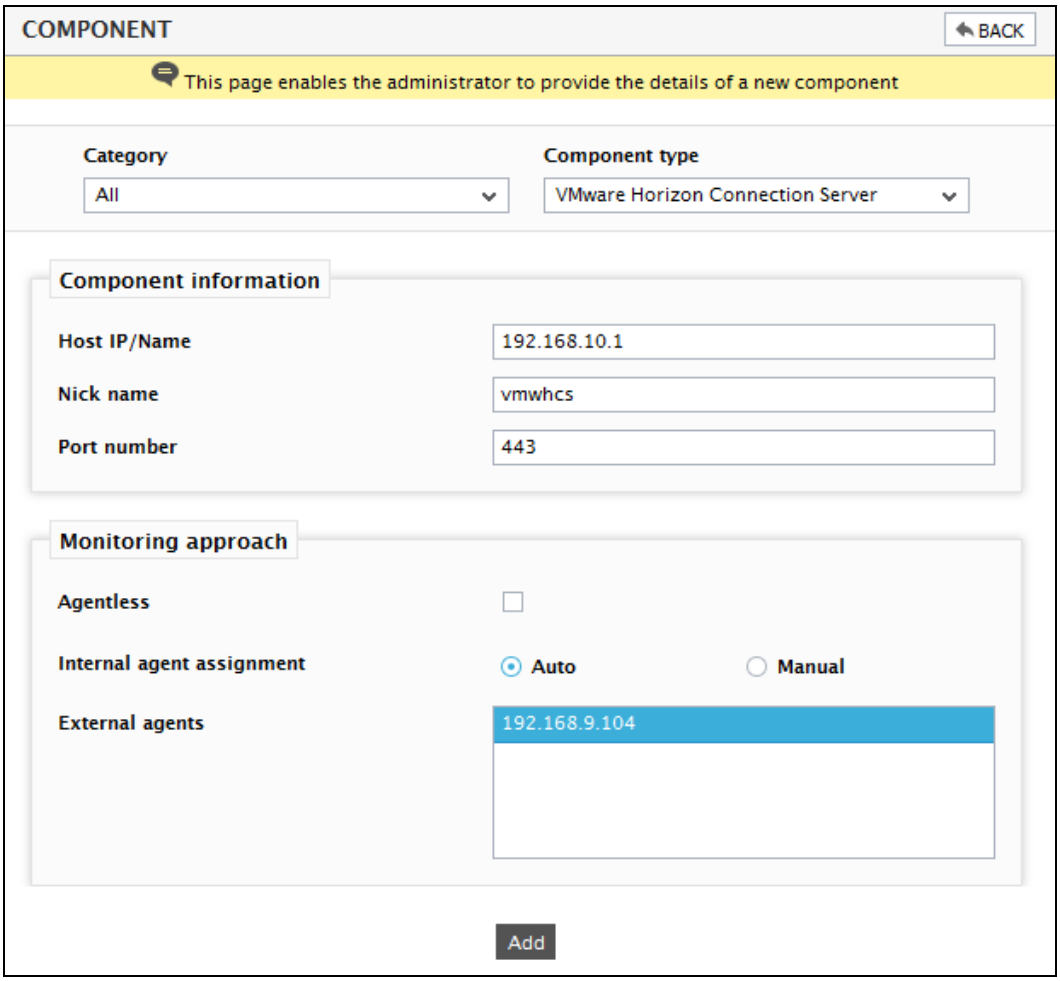

Figure 2.1: Adding a VMware Horizon Connection Server

5. Specify the **Host IP/Name** and the **Nick name** for the VMware Horizon Connection Server component.

6. The **Port number** will be set as 443 by default. If the Connection Server is listening on a different port in your environment, then override this default setting.

7. Then, click the **Add** button to add the Connection Server for monitoring.

8. Next, try to sign out of the admin interface. Doing so, will bring up the following page as shown in Figure 2.2, which prompts you to configure a list of unconfigured tests for the VMware Horizon Connection Server.

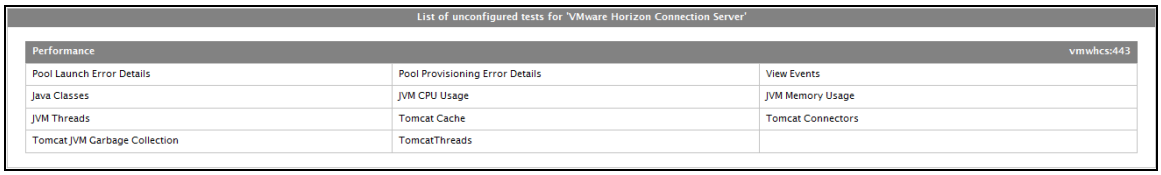

Figure 2.2: The list of unconfigured tests for VMware Horizon Connection Server

9. Click on any test in the list of unconfigured tests. For instance, click on the **Pool Launch Error Details** test to configure it. To know how to configure the tests, refer to **Monitoring the VMware Horizon Connection Server**.
10. After configuring all the tests, signout of the eG admin interface.

Chapter 3: Monitoring the VMware Horizon Connection Server

eG Enterprise offers a specialized *VMware Horizon Connection Server model*, which periodically evaluates the service levels achieved by each component of the VMware Horizon View solution, and proactively alerts administrators to potential performance troubles.

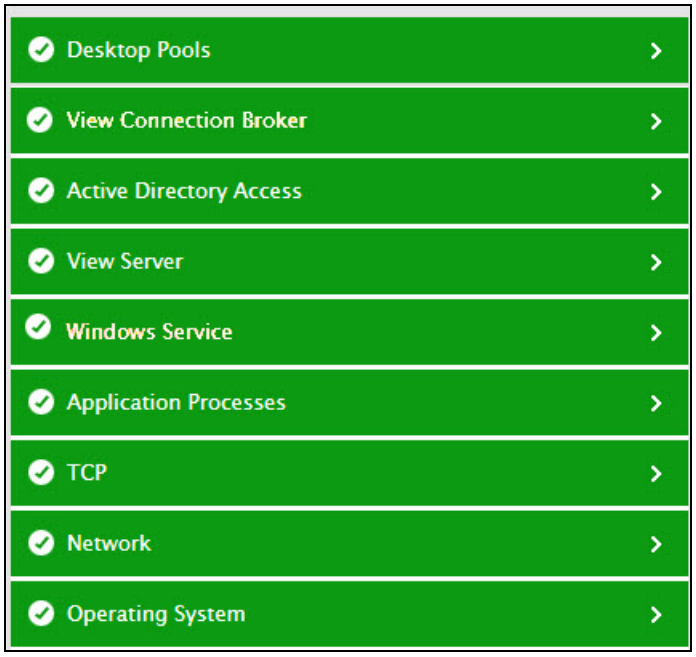

Figure 3.1: Layer model of VMware Horizon Connection Server

Each layer of the Figure 3.1 is mapped to a variety of tests that provide valuable insights into the overall health and performance of **VMware Horizon View** and its components. With the help of the metrics reported by these tests, you can find quick and accurate answers for the following queries:

- Is the VMware Horizon Connection Server available over the network? If so, how quickly is it responding to requests?
- Is the View Manager able to connect to the vCenter server?
- Is the Active Directory server accessible?
- Were any admin, transfer, agent, connection broker events captured recently?
- Is the connection broker enabled?
- Is the VMware Horizon Connection Server able to connect to the events database?

- Will the VMware Horizon View license expire soon?
- Is the local mode license enabled?
- Is the View Composer license enabled?
- How many desktops exist in each desktop pool?
- Which desktop pools are currently disabled?
- Is any desktop idle in a pool? If so, which desktop pool is it?
- Are there too many inactive desktops in a pool? If so, which pool is it?
- Are all virtual desktops accessible over the network? Which desktop is not?

The sections that follow will focus on the top 4 layers of Figure 3.1. The remaining layers have already been dealt with in the *Monitoring Unix and Windows Servers* document.

3.1 The View Server Layer

The View Manager - i.e., the View Connection Server - integrates with VMware vCenter Server, allowing administrators to create desktops from virtual machines running on VMware ESX server and then deploy them to end users.

If the View Manager is unable to connect to the vCenter server, then users may be unable to access the VMs running on vCenter.

The test mapped to this layer reports whether/not the View Manager is able to connect to the vCenter server.

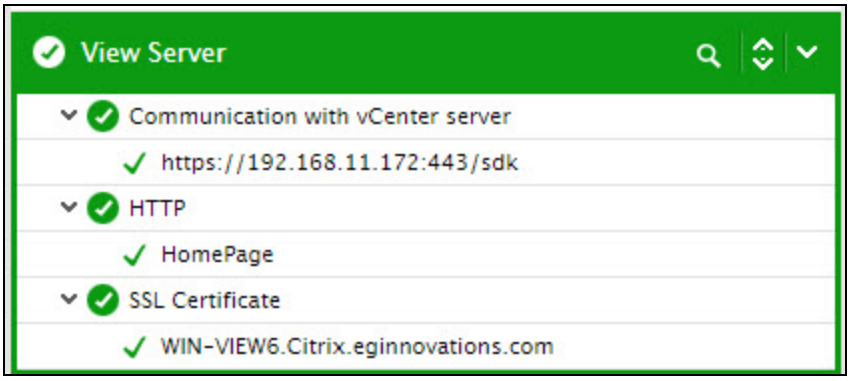

Figure 3.2: The test mapped to the View Server layer

3.1.1 Horizon Logins Test

This test monitors the user logins and logouts of the VMware Horizon Connection Server. By continuously tracking the logins and logouts, administrators can figure out the users who have logged in/logged out and the time of login/logout. This way, administrators can identify users who were unusually logged in for a longer duration as well as proactively identify connection issues as well as the session load on the server.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection Server being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by VMware Horizon Connection server. The default port number is *NULL*.
Logfile Path	In the Logfile Path text box, specify the full path to the *debug-<current date>* file where the details of the current logins/logouts are stored. By default, the file will be available in the *C:\Program files\VMware\VDM* directory. If the file indeed resides in its default location, set the Logfile Path to *none*. On the other hand, if the file has been installed in a different location, provide the full path to that location against the Logfile Path.
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.

Parameters	Description
	The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
New logins	Indicates the number of user logins to the server.	Number	This measure is a good indicator of the load on the VMware Horizon Connection Server. A consistent zero value could indicate a connection issue. The detailed diagnosis of this measure if enabled, lists the Session ID, the name of the user, the logged in time, User SID and the Client IP address.
New logouts	Indicates the number of user logouts from the server.	Seconds	If all the current sessions suddenly log out, it indicates a problem condition that requires investigation. The detailed diagnosis of this measure if enabled, lists the Session ID, the name of the user, the logout time, the time duration for which the user was logged in, the User SID and the Client IP address.

3.1.2 Communication with vCenter Server Test

This test, by proactively alerting administrators to potential connectivity issues between the View Manager and the vCenter server, helps these administrators initiate prompt action to plug the connection holes, so that the virtual desktop service can be delivered without a glitch.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to

Parameter	Description
	collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* 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	None	Measurement Unit	Interpretation
vCenter connectivity	Indicates whether the vCenter connectivity is available to the View Manager or not.		This measure reports either *Ok* or *Not available* as the status of the vCenter connectivity. The numeric values that correspond to the above-mentioned states are as follows:

Measurement	None	Measurement Unit	Interpretation
			<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>OK</td><td>1</td></tr><tr><td>Not Available</td><td>0</td></tr></table> **Note:** By default, this measure reports the above-mentioned states while indicating the status of the vCenter connectivity. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.

3.2 The Active Directory Access Layer

Using the tests mapped to this layer, you can quickly capture the non-availability of the Active Directory server and measure the health of interactions between the View server and the Active Directory server.

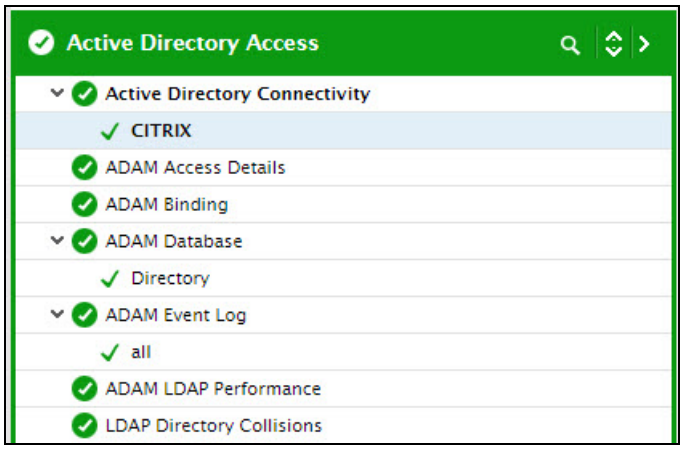

Figure 3.3: The tests mapped to the Active Directory Access layer

3.2.1 Active Directory Connectivity Test

View uses your existing Microsoft Active Directory infrastructure for user authentication and management. In the absence of a connection to the AD server, VMware Horizon View Connection

server will not be able to authenticate user logins, thereby denying even valid users access to their critical desktops.

With the help of this test, you can continuously monitor the VMware Horizon View Connection server - AD server connection, and promptly detect problems in it, so that the connection can be restored before users begin to complaint.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management

Parameter	Description
	Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* here.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active directory connection state	Indicates whether the VMware Horizon Connection server is able to connect to the Active Directory server or not.		This measure reports either *Ok* or *Not available* as the status of the active directory connection. The numeric values that correspond to the above-mentioned states are as follows: State: Ok — Numeric Value: 1 State: Not available — Numeric Value: 0 **Note:** By default, this measure reports the above-mentioned states while indicating the status of the active directory connection. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.

3.2.2 ADAM Access Details Test

This test measures the load on the AD server in terms of the level of read-write activity on the server and the count of search operations performed by the server. In the process, the test reveals the following:

- Which AD services initiated the read-write operations? Which of these services generated the maximum I/O load on the server - is it the LSA? the NSPI? the NTDS? SAM? or the replication service? - this information is useful when administrators are faced with an AD overload, as it accurately points them to the probable sources of the load;
- Which AD service performed the maximum searches on the server? - in the event of an overload, this metric will help you identify that service which could be contributing to the overload;
- Is the server sized with adequate threads to handle the I/O load?

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Schema cache hit ratio	Indicates the percentage of object name lookups serviced by the Schema Cache.	Percent	All changes made to Active Directory are validated first against the schema. For performance reasons, this validation takes place against a version of the schema that is held in memory on the domain controllers. This "in-memory version," called the

Measurement	Description	Measurement Unit	Interpretation
			schema cache, is updated automatically after the on- disk version has been updated. The schema cache provides mapping between attribute identifiers such as a database column identifier or a MAPI identifier and the in-memory structures that describe those attributes. The schema cache also provides lookups for class identifiers to get in- memory structures describing those classes. A low value of this measure indicates that the Directory Service needs high disk read/write activity to perform its job. This results in poor response time of the components available in the Active Directory.
Notify queue size	Indicates the number of pending update notification requests that have been queued and not transmitted.	Number	When any change in the Active Directory occurs, the originating domain controller sends an update notification requests to the other domain controllers. A high value of this measure indicates that the Active Directory is changing frequently but the update notification requests have not been transmitted to the other domain controllers. This results in a loss of data integrity in the directory store. This problem can be corrected by forcing the replication.

Measurement	Description	Measurement Unit	Interpretation
Current threads in use	Indicates the current number of threads in use by the directory service (which is different from the number of threads in the directory service process).	Number	This is the number of threads currently servicing client API calls; it can be used to indicate whether additional processors should be used. A fluctuating value for this measure indicates a change in the load. A low value could point to network problems that are preventing client requests from succeeding.
Server binds	Indicates the number of domain controller– to–domain controller binds per second that are serviced by this domain controller.	Binds/Sec	
Directory reads	Indicates the rate of directory reads.	Reads/Sec	These measures serve as effective indicators of the ability of the AD server to process read, write, and search requests.
Directory writes	Indicates the rate of directory writes.	Writes/Sec	
Directory searches	Indicates the number of directory searches per second.	Searches/Sec	
DS reads from DRA	Indicates the percentage of reads on the directory by replication.	Percent	If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the *DS reads from KCC, DS reads from LSA, DS reads from NSPI, DS reads from NTDS*, and *DS reads from SAM* measures to know which AD service is performing the maximum reads on

Measurement	Description	Measurement Unit	Interpretation
			the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS reads from KCC	Indicates the percentage of reads performed by the Knowledge Consistency Checker on the directory.	Percent	The **Knowledge Consistency Checker (KCC)** generates the replication topology by specifying what domain controllers will replicate to which other domain controllers in the site. The KCC maintains a list of connections, called a replication topology, to other domain controllers in the site. The KCC ensures that changes to any object are replicated to all site domain controllers and updates go through no more than three connections. If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the *DS reads from DRA, DS reads from LSA, DS reads from NSPI, DS reads from NTDS*, and *DS reads from SAM* measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS reads from LSA	Indicates the percentage of reads performed by the Local Security Authority on the	Percent	The **Local Security Authority (LSA)** is the security subsystem responsible for all interactive user authentication and authorization

Measurement	Description	Measurement Unit	Interpretation
	directory.		services on a local computer. The LSA is also used to process authentication requests made through the Kerberos V5 protocol or NTLM protocol in Active Directory. If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the *DS reads from DRA, DS reads from KCC, DS reads from NSPI, DS reads from NTDS*, and *DS reads from SAM* measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS?
DS reads from NSPI	Indicates the percentage of reads performed by the Name Service Provider Interface (NSPI) on the directory.	Percent	The **Name Service Provider Interface (NSPI)** is the protocol by which Messaging API (MAPI) clients access the AD DS. Exchange Address Book clients use the client MAPI provider Emsabp32.dll to look up e- mail addresses in the global catalog. The client- side MAPI provider communicates with the server through the proprietary Name Service Provider Interface (NSPI) RPC interface. If the AD server is experiencing

Measurement	Description	Measurement Unit	Interpretation
			abnormally high read activity, then, you can compare the value of this measure with the values reported by the *DS reads from KCC, DS reads from LSA, DS reads from DRA, DS reads from NTDS*, and *DS reads from SAM* measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? or the NSPI?
DS reads from NTDS	Indicates the percentage of reads performed by the name service directory APIs on the directory.	Percent	If the AD server is experiencing abnormally high read activity, then, you can compare the value of this measure with the values reported by the *DS reads from KCC, DS reads from LSA*, and *DS reads from DRA, DS reads from NSPI*, and *DS reads from SAM* measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? or the SAM?
DS reads from SAM	Indicates the percentage of reads performed by the Security Account Manager (SAM) on the directory.	Percent	The **Security Accounts Manager (SAM)** is used for verifying passwords and for checking passwords against any existing password policies that are in effect on a domain controller. If the AD server is experiencing abnormally high read activity, then, you can compare the value of this

Measurement	Description	Measurement Unit	Interpretation
			measure with the values reported by the *DS reads from KCC, DS reads from LSA*, and *DS reads from DRA, DS reads from NSPI*, and *DS reads from NTDS* measures to know which AD service is performing the maximum reads on the AD server - is it the replication service? the LSA? the KCC? the NSPI? or the NTDS?
DS writes from DRA	Indicates the percentage of writes on the AD server by replication.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the *DS writes from KCC, DS writes from LSA, DS writes from NSPI, DS writes from NTDS*, and *DS writes from SAM* measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS writes from KCC	Indicates the percentage of writes performed by the Knowledge Consistency Checker on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the *DS writes from DRA, DS writes from LSA, DS writes from NSPI, DS writes from NTDS*, and *DS writes from SAM* measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the KCC? the LSA? the

Measurement	Description	Measurement Unit	Interpretation
			NSPI? the NTDS? or the SAM?
DS writes from LSA	Indicates the percentage of writes performed by the Local Security Authority on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the *DS writes from DRA, DS writes from KCC, DS writes from NSPI, DS writes from NTDS*, and *DS writes from SAM* measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS writes from NSPI	Indicates the percentage of writes performed by the Name Service Provider Interface (NSPI) on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the *DS writes from DRA, DS writes from KCC, DS writes from LSA, DS writes from NTDS,* and *DS writes from SAM* measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS writes from NTDS	Indicates the percentage of writes performed by the name service directory APIs on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the *DS writes from DRA, DS writes from KCC, DS writes from LSA, DS writes from NSPI*, and *DS writes from SAM* measures to

Measurement	Description	Measurement Unit	Interpretation
			know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS writes from SAM	Indicates the percentage of writes performed by the Security Accounts Manager (SAM) on the directory.	Percent	If the AD server is experiencing abnormally high write activity, then, you can compare the value of this measure with the values reported by the *DS writes from DRA, DS writes from KCC, DS writes from LSA, DS writes from NSPI*, and *DS writes from NTDS* measures to know which AD service is performing the maximum writes on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from DRA	Indicates the percentage of searches performed by the replication service on the AD server.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the *DS searches from KCC, DS searches from LSA, DS searches from NSPI, DS searches from NTDS,* and *DS searches from SAM* measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from KCC	Indicates the percentage of searches	Percent	If the AD server is processing an

Measurement	Description	Measurement Unit	Interpretation
	performed by the Knowledge Consistency Checker on the directory.		abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the *DS searches from DRA, DS searches from LSA, DS searches from NSPI, DS searches from NTDS,* and *DS searches from SAM* measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from LSA	Indicates the percentage of searches performed by the Local Security Authority on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the *DS searches from DRA, DS searches from KCC, DS searches from NSPI, DS searches from NTDS,* and *DS searches from SAM* measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from NSPI	Indicates the percentage of searches performed by the Name Service Provider Interface (NSPI) on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the *DS searches from DRA, DS searches*

Measurement	Description	Measurement Unit	Interpretation
			from KCC, DS searches from LSA, DS searches from NTDS, and *DS searches from SAM* measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from NTDS	Indicates the percentage of searches performed by the name service directory APIs on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the *DS searches from DRA, DS searches from KCC, DS searches from LSA, DS searches from NSPI,* and *DS searches from SAM* measures to know which AD service is performing the maximum number of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?
DS searches from SAM	Indicates the percentage of searches performed by the Security Accounts Manager (SAM) on the directory.	Percent	If the AD server is processing an abnormally large number of search requests, then, you can compare the value of this measure with the values reported by the *DS searches from DSA, DS searches from KCC, DS searches from LSA, DS searches from NSPI*, and *DS searches from NTDS* measures to know which AD service is performing the maximum number

Measurement	Description	Measurement Unit	Interpretation
			of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?

3.2.3 ADAM Binding Test

In Active Directory Domain Services, the act of associating a programmatic object with a specific Active Directory Domain Services object is known as binding. When a programmatic object, such as an IADs or DirectoryEntry object, is associated with a specific directory object, the programmatic object is considered to be bound to the directory object.

This test reports the type of binds that exist in an AD environment, and for each bind type, reports how fast the AD server bound the programmatic objects to the directory object.

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Ntlm binds	Indicates the rate at which programmatic and directory objects were bound to one another using NTLM binds.	Binds/Sec	
Simple binds	Indicates the rate at which programmatic and directory objects were bound to one another using Simple binds.	Binds/Sec	In a simple bind, the client either binds anonymously, that is, with an empty bind Distinguished Name, or by providing a Distinguished Name and a password.
External binds	Indicates the rate at which programmatic and directory objects were bound to one another using External binds.	Binds/Sec	
Fast binds	Indicates the rate at which programmatic and directory objects were bound to one another using Fast binds.	Binds/Sec	Fast bind mode allows a client to use the LDAP bind request to simply validate credentials and authenticate the client without the overhead of establishing the authorization information.
Negotiated binds	Indicates the rate at which programmatic and directory objects were bound to one another using Negotiated binds.	Binds/Sec	

3.2.4 ADAM Database Test

This test reports critical statistics pertaining to the usage of the database caches, and the overall health of the AD database.

Target of the test : An Active Directory server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every AD Server being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Database cache hits	Indicates the percentage of page requests of the database file that were occupied in a cache before responding to the request.	Percent	Ideally, the value of this measure should be moderate. A high value of this measure indicates the high utilization of physical memory. In such a case, you can add the required memory to the database.
Database table cache hits	Indicates the percentage of database tables that were opened using cached schema information.	Percent	Ideally, the value of this measure should be high.
Log records waiting	Indicates the rate of log record stalls, per second.	Records/Sec	

Measurement	Description	Measurement Unit	Interpretation
Log threads waiting	Indicates the current number of threads waiting for data to be written to the log so that database updation will be executed.	Number	

3.2.5 ADAM Event Log Test

This test reports statistical information about Active Directory performance recorded in the event log.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *VMware Horizon Connection Server* as the **Component type**, *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the filter configured

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by VMware Horizon Connection Server. Here it is *NULL*.
Logtype	Refers to the type of event logs to be monitored. The default value is *application*.
Policy Filter	Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: • Manually specify the event sources, IDs, and descriptions in the Filter text area, or,

Parameters	Description
	• Select a specification from the predefined filter policies listed in the Filter box For explicit, manual specification of the filter conditions, select the **NO** option against the Policy Filter field. This is the default selection. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the **YES** option against the Policy Filter field.
Filter	If the Policy Filter flag is set to **NO**, then a Filter text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that the Filter text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here: • OS_events is the display name that will appear as a descriptor of the test in the monitor UI; • all indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify none. • Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, Browse and Print have been excluded from monitoring. Alternatively, you can use all to indicate that all the event sources have to be excluded from monitoring, or none to denote that none of the event sources need be excluded. • In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The all in our example represents that all the event IDs need to be considered while monitoring. • Similarly, the none (following all in our example) is indicative of the fact that none of the event IDs need to be excluded from monitoring. On the other hand, if you want to instruct the eG Enterprise system to ignore a few event IDs during monitoring, then provide the IDs as a comma-separated list. Likewise, specifying all makes sure that all the event IDs are excluded from monitoring.

Parameters	Description
	• The all which follows implies that all events, regardless of description, need to be included for monitoring. To exclude all events, use none. On the other hand, if you provide a comma-separated list of event descriptions, then the events with the specified descriptions will alone be monitored. Event descriptions can be of any of the following forms - desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. • In the same way, you can also provide a comma-separated list of event descriptions to be excluded from monitoring. Here again, the specification can be of any of the following forms: desc*, or desc, or *desc*,or desc*, or desc1*desc2, etc. desc here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. In our example however, none is specified, indicating that no event descriptions are to be excluded from monitoring. If you use all instead, it would mean that all event descriptions are to be excluded from monitoring. By default, the Filter parameter contains the value: *all:all:none:all:none:all:none*. Multiple filters are to be separated by semi-colons (;). **Note:** The event sources and event IDs specified here should be exactly the same as that which appears in the Event Viewer window. On the other hand, if the Policy Filter flag is set to **YES**, then a Filter list box will appear, displaying the filter policies that pre-exist in the eG Enterprise system. A filter policy typically comprises of a specific set of event sources, event IDs, and event descriptions to be monitored. This specification is built into the policy in the following format: *{Policyname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}* To monitor a specific combination of event sources, event IDs, and event descriptions, you can choose the corresponding filter policy from the Filter list box. Multiple filter policies can be so selected. Alternatively, you can modify any of the existing policies to suit your needs, or create a new filter policy. To facilitate this, a **Click here** link appears just above the test configuration section, once the **YES** option is chosen

Parameters	Description
	against Policy Filter. Clicking on the **Click here** link leads you to a page where you can modify the existing policies or create a new one. The changed policy or the new policy can then be associated with the test by selecting the policy name from the Filter list box in this page.
UseWMI	The eG agent can either use WMI to extract event log statistics or directly parse the event logs using event log APIs. If the UseWMI flag is **YES**, then WMI is used. If not, the event log APIs are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set this parameter value to **NO**.
DDForInformation	eG Enterprise also provides you with options to restrict the amount of storage required for event log tests. Towards this end, the DDForInformation and DDForWarning flags have been made available in this page. By default, both these flags are set to **Yes**, indicating that by default, the test generates detailed diagnostic measures for information events and warning events. If you do not want the test to generate and store detailed measures for information events, set the DDForInformation flag to **No**.
DDForWarning	To ensure that the test does not generate and store detailed measures for warning events, set the DDForWarning flag to No.
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
Errors	This refers to the number of AD error events that were generated.	Number	A very low value (zero) indicates that the AD server is in a healthy state without any potential problems. An increasing trend or high value indicates the existence of problems like loss of functionality or data. The detailed diagnosis capability, if enabled, lists the description of specific events. Please check the Application Logs in the Event Log Viewer for more details.
Information count	This refers to the number of information events generated when the test was last executed.	Number	A change in the value of this measure may indicate infrequent but successful operations performed by the AD server. The detailed diagnosis capability, if enabled, lists the description of specific events.
Warnings	This refers to the number of warnings that were generated when the test was last executed.	Number	A high value of this measure indicates problems that may not have an immediate impact, but may cause future problems in the Directory Service. The detailed diagnosis capability, if enabled, lists the description of specific events.
Critical errors	Indicates the number of critical events that were	Number	**This measure is applicable only for Windows 2008/Windows**

Measurement	Description	Measurement Unit	Interpretation
	generated when the test was last executed.		**Vista/Windows 7 systems**. A high value of this measure indicates that too many errors have occurred, which the Directory Service cannot automatically recover from. The detailed diagnosis capability, if enabled, provides the description of specific events.
Verbose count	Indicates the number of verbose events that were generated when the test was last executed.	Number	**This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems**. Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better. The detailed diagnosis of this measure describes all the verbose events that were generated during the last measurement period.

3.2.6 ADAM LDAP Performance Test

The Lightweight Directory Access Protocol (LDAP) is a directory service protocol that runs on a layer above the TCP/IP stack. It provides a mechanism used to connect to, search, and modify Internet directories. The LDAP directory service is based on a client-server model. The function of LDAP is to enable access to an existing directory. LDAP is one of the protocols used to query and modify items on the Active Directory server.

To monitor the interactions between clients and the AD server over LDAP, and to promptly capture slowdowns in LDAP searches and binds, use the LDAP Performance test.

Note:

This test applies only to Active Directory Servers installed on Windows 2008.

Target of the test : An Active Directory or Domain Controller on Windows 2008

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Active Directory being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Ldap searches	Indicates the rate at which LDAP clients perform search operations.	Searches/Sec	This counter should show activity over time. If it does not, network problems are probably hindering the processing of client requests.
Ldap writes	Indicates the rate at which clients perform write operations on the AD server.	Writes/Sec	
Ldap active threads	Indicates the current number of threads in use by the LDAP subsystem of the local directory service.	Number	A high number indicates a high level of LDAP activity on the directory service.
Ldap bind time	Indicates the time, in milliseconds, taken for the last successful LDAP	Secs	In Active Directory Domain Services, the act of associating a programmatic object with a specific Active Directory Domain Services object is known

Measurement	Description	Measurement Unit	Interpretation
	bind.		as binding. When a programmatic object, such as an IADs or DirectoryEntry object, is associated with a specific directory object, the programmatic object is considered to be bound to the directory object. This measure should be as low as possible. If it is not, hardware or network- related problems are indicated.
Ldap sessions	Indicates the number of currently connected LDAP client sessions.	Number	This measure is just an indicator of the number of Ldap clients connected to the Active Directory. A high or low value for this measure does not always denote an error situation.
Ldap closed connections	Indicates the LDAP connections that have been closed in the last second.	Connections/Sec	
Ldap new connections	Indicates the number of new LDAP connections that have arrived in the last second.	Connections/Sec	
Ldap new ssl connections	Indicates the number of new SSL or TLS connections that arrived in the last second.	Connections/Sec	
Ldap successful binds	Indicates the number of successful LDAP	Binds/Sec	In Active Directory Domain Services, the act of associating a programmatic object with a specific Active Directory

Measurement	Description	Measurement Unit	Interpretation
	binds per second.		Domain Services object is known as binding. When a programmatic object, such as an IADs or DirectoryEntry object, is associated with a specific directory object, the programmatic object is considered to be bound to the directory object. A high value is desired for this measure. A very low value could indicate network problems.

3.2.7 LDAP Directory Collisions Test

If duplicate LDAP entries are created on two or more View Connection Server instances, this can cause problems with the integrity of LDAP data in View. This test checks the ADAM database at pre-configured intervals for the existence of collision references and colliding entries, and reports the count of such entries (if any are found), so that they can be removed with immediate effect to ensure data integrity.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
View Install DIR	Indicate the full path to the install directory of the target VMware

Parameter	Description
	Horizon Connection Server. By default, this is *none*.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* here.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Collision entry references found	Indicates the number of collision references currently found in the ADAM database.	Number	Typically, the value 0 is desired for both these measures. A non-zero value indicates the existence of colliding entries. For example, this condition can happen during an

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>upgrade while LDAP replication is inoperative.</td></tr>
<tr><td>Collision entries found</td><td>Indicates the number of collision entries currently found in the ADAM database.</td><td>Number</td><td>When colliding entries exist in the LDAP directory (ADAM database), identify what those entries are and resolve the collision.</td></tr>
<tr><td>Deleted entry references found</td><td>Indicates the number of collision references currently deleted from the ADAM database.</td><td>Number</td><td></td></tr>
<tr><td>Local View LDAP Directory</td><td>Indicates whether any collision references were currently found in ADAM database or not.</td><td></td><td>If this measure reports the value clean, it indicates that no collision references were found in LDAP (ADAM database) directory.

The value Not Clean means there are collision references in LDAP (ADAM database) directory.

The numeric values that correspond to the measure values discussed above are as follows:

<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Clean</td><td>1</td></tr><tr><td>Not Clean</td><td>0</td></tr></table>
Note:

By default, this measure reports the above- mentioned Measure Value s while indicating whether/not collision references were found in the LDAP directory. However, in the graph of this measure, the same will be indicates</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			using the corresponding numeric equivalents of the states as mentioned in the table above.

3.2.8 Replication Details Test

To provide high availability and load balancing, you can install one or more additional instances of VMware Horizon Connection Server that replicate an existing Connection Server instance. After a replica installation, the existing and newly installed instances of Connection Server are identical. When a change is made on one instance, the updated information is copied to the replicated instances simultaneously. If any of the replicated instances fails, the other instances in the group continue to operate such that operations of the Horizon Connection server would be uninterrupted. If the replications fail due to authentication or configuration problems, then, high availability of the Connection Server will be uncertain. To avoid such eventualities, you should continuously monitor the replication processes within the target environment and take necessary actions swiftly if the replication process fails. The **Replication Details** test helps you in this regard!

This test tracks the replications processes and reports the number of replications that were successful and the number of replications that failed in the target environment.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
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

Parameter	Description
	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 success	Indicates the number of replications that were performed successfully during the last measurement period.	Number	A high value is desired for this measure. For complete details of the successful replication attempts, use the detailed diagnosis of this measure.
Number of failure	Indicates the number of replications that failed during the last measurement period.	Number	Ideally, the value of this measure should be zero. For complete details of the failed replication attempts, use the detailed diagnosis of this measure.

3.3 The View Connection Broker Layer

Using the tests mapped to this layer, you can determine the following:

- The status of the connection broker;
- The number and nature of admin, agent, connection broker, and transfer events that have been captured;
- Whether/not the events database is accessible;
- The number of days left for the View license to expire.
- The number and type of sessions that are currently active on the VMware Horizon View server

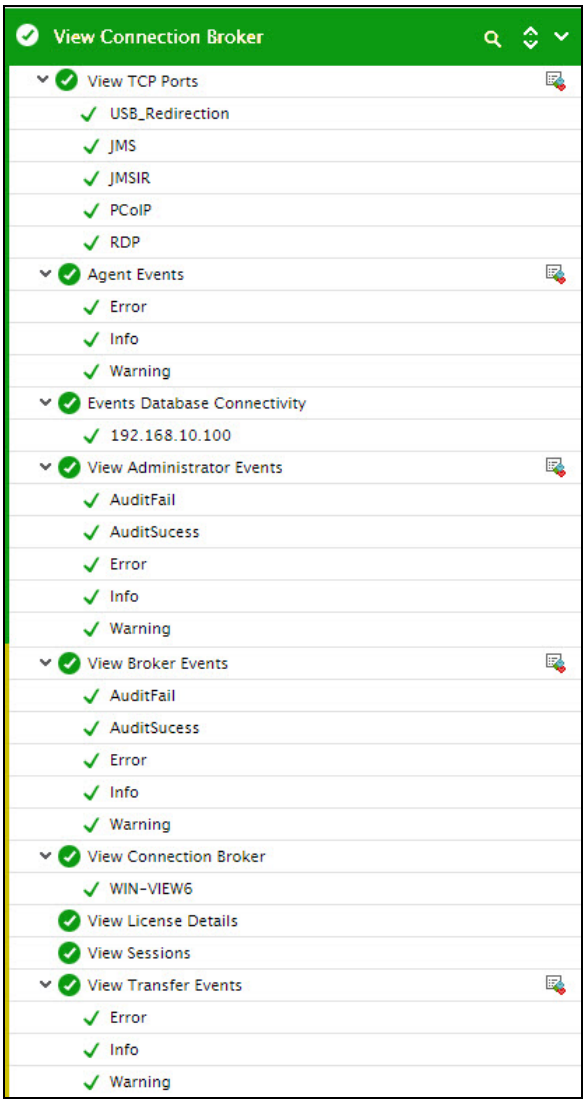

Figure 3.4: The tests mapped to the View Connection Broker layer

3.3.1 View TCP Ports Test

This test monitors configured ports on the VMware Horizon Connection Server and reports the availability and responsiveness of each port. This way, you can instantly identify unavailable and unresponsive ports on the server.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each target configured for monitoring

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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Targets	Specify either a comma-separated list of port numbers that are to be tested (e.g., 80,7077,1521), or a comma-separated list of *port name:port number* pairs that are to be tested (eg., JMS:4001,JMSIR:4100). In the latter case, the port name will be displayed in the monitor interface.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Port Connectivity Status	Indicates whether this port is available or not.	Percent	This measure will report the value 100, if the port is identified by the View Agent, and will report the value 0 if the View Agent is not able to identify the port.
Response time	Indicates the time taken by this port to respond to a request.	Seconds	An increase in response time can be caused by several factors such as a server bottleneck, a configuration problem with the

Measurement	Description	Measurement Unit	Interpretation
			DNS server, a network problem, etc.

3.3.2 View Events Test

The events database stores information about View events as records in a database rather than in a log file. This database serves as a rich source of information on the status of and problems encountered by VMware Horizon Connection Server. Using the **View Events** test, administrators can periodically query the events database for the count of errors, warnings, general information, success and failure events stored in it, and also view the details of such events. With the help of these details, administrators can easily and effectively troubleshoot issues affecting the operations of VMware Horizon Connection Server.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
DatabaseType	Specify the type of the database in the DatabaseType text box. By default, the DatabaseType is Microsoft SQL.
DatabaseServer	Specify the IP address of the database server that holds the VMware Horizon Connection Server event database.
DatabasePort	Specify the port of the database server.
Instance	Specify the instance name of the VMware Horizon Connection Server event database. By default, this is set to *none*.

Parameter	Description
EventsDatabaseName	Specify the name of the database that holds the VMware Horizon Connection Server events.
EventsTableName	Specify the name of the table containing the VMware Horizon View events in the VMware Horizon Connection Server events database.
User name and Passsword	Provide the credentials of the user who has the authorization to execute queries on the Events Database.
Confirm Password	Confirm the password by retyping it here.
Domain	Specify the name of the domain in the Domain text box.
SSL	By default, the SSL flag is set to **No**. If the Microsoft SQL server that is hosting the Events Database is SSL-enabled, set this flag to **Yes**.
Show Info DD	By default, this flag is set to **No**, indicating that this test will not report detailed diagnostics for the **Information** measure. This means that, by default, eG will not capture and store the complete details of information messages in the eG database. This default setting is ideal, as in the real world, hundreds of information messages will be written to the events database, and by not writing the details of these messages in the eG database, considerable database space can be saved. However, if your eG database is well-sized and you prefer to view the description of all the information messages that are written to the events database, then set this flag to **Yes**.
Show Audit Success DD	By default, this flag is set to **No**, indicating that this test will not report detailed diagnostics for the **Audit success** measure. This means that, by default, eG will not capture and store the complete details of successful audit events in the eG database. This default setting is ideal, as in the real world, numerous audits will be successful, and by not writing the details of these successful events in the eG database, considerable database space can be saved. However, if your eG database is well-sized and you want to view the description of all the successful audit events that are written to the events database, then set this flag to **Yes**.
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.

Parameter	Description
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
Information	Indicates the total number of information events in the database.	Number	For complete details of the information events, use the detailed diagnosis of this measure.
Error	Indicates the total number of error events in the database.	Number	For complete details of the error events, use the detailed diagnosis of this measure.
Warning	Indicates the total number of warning event sin the database.	Number	For complete details of the warning events, use the detailed diagnosis of this measure.
Audit success	Indicates the total number of audit successes recorded in the events database.	Number	For complete details of the audit success events, use the detailed diagnosis of this measure.
Audit failure	Indicates the total number of audit failures recorded in the events database.	Number	For complete details of the audit failure events, use the detailed diagnosis of this measure.
Others	Indicates the total	Number	For complete details of the other

Measurement	Description	Measurement Unit	Interpretation
	number of other events in the database.		events, use the detailed diagnosis of this measure.

3.3.3 View Connection Broker Test

A connection broker is a server that allows connections between remote users and virtual desktops, and provides authentication and session management.

This test reports the current status of the connection broker.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server Name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User Name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management,

Parameter	Description
	configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* 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
Status	Indicates whether the connection broker is enabled or not.		This measure reports either *Enabled* or *Disabled* as the status of the connection broker. The numeric

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>values that correspond to the above- mentioned states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>0</td></tr></table>
Note:
By default, this measure reports the above- mentioned states while indicating the status of the connection broker. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.
The detailed diagnosis of this test shows the connection status of the connection broker.</td></tr>
</table>

3.3.4 Horizon View Licensing Usage Test

By tracking the number and type of sessions to the VMware Horizon Connection broker, administrators can not only understand the load on their VMware Horizon Connection Server, but can also determine how their VMware Horizon licenses are being utilized. Such useful insights on load and license usage are provided by the **Horizon View Licensing Usage** test. This test reports the total number of sessions on the VMware Horizon Connection Server, and also reveals the number of sessions of each type currently active on the server. In addition, the test also highlights the maximum number of concurrent sessions of each type that were launched on the server. Based on these inputs, administrators can understand current license usage and can also plan future license requirements. The test also promptly alerts administrators to the impending expiry of the View license.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* here.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
All sessions	The number of View sessions currently active.	Number	This is a good indicator of the current session load on View.
Checkedout VM sessions	Indicates the current number of sessions in which VMs are checked out for use as local desktops.	Number	This measure will not be available from VMware Horizon View 6.0 onwards, as the 'Local Mode' feature has been deprecated from this version. Compare the value of this measure with that of the Linked clone sessions measure to know what type of sessions are contributing to the current session load on the View server – full VM sessions? or linked-clone sessions?
Full VM sessions	Indicates the current number of active full VM sessions.	Number	
Linked clone sessions	Indicates the current number of active linked clone View sessions.	Number	A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. This conserves disk space, and allows multiple virtual machines to use the same software installation. Compare the value of this measure with that of the Full VM sessions measure to know what type of sessions are contributing to the current session load on the View server – full VM sessions? or linked-clone sessions?

Measurement	Description	Measurement Unit	Interpretation
PCoIP gateway sessions	Indicates the current number of PCoIP gateway sessions.	Number	In the event of a session overload, you can compare the value of these measures to know the type of sessions that is causing the overload.
Secure gateway sessions	Indicates the current number of Secure gateway sessions.	Number	
Sessions from other sources	Indicates the current number of active View sessions from other sources.	Number	
Application sessions	Indicates the current number of active View application sessions.	Number	In the event of a session overload, you can compare the value of these measures to know the reason for the overload – is it because too many sessions are launching applications? Or is it many sessions are accessing desktops?
Desktop sessions	Indicates the current number of active View desktop sessions.	Number	
Highest all sessions	Indicates the highest recorded number of concurrent View sessions.	Number	This is a good indicator of the maximum concurrent session load that the View server can handle. By observing the variations to this measure over time, you can understand the server capacity and accordingly plan its future resource requirements. The measure also indicates how concurrent licenses were utilized, and helps you determine whether/not more licenses will be required in the future.
Highest full VM sessions	Indicates the highest recorded number of concurrent full VM sessions.	Number	If concurrent session load/usage of concurrent licenses is abnormally high, you can compare the value of this measure with that of the

Measurement	Description	Measurement Unit	Interpretation
			Highest linked- clone sessions to know the type of sessions that may have contributed the most to the erratic usage.
Highest linked clone sessions	Indicates the highest recorded number of concurrent linked- clone sessions.	Number	A linked clone is a copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner. This conserves disk space, and allows multiple virtual machines to use the same software installation. If the value of the *Highest all sessions* measure is abnormally high, you can compare the value of this measure with that of the Highest full VM sessions to know the type of sessions that may have contributed the most to the erratic usage.
Highest PCoIP gateway sessions	Indicates the highest recorded number of concurrent PCoIP gateway sessions.	Number	If the value of the *Highest all sessions* measure is abnormally high, you can compare the value of these three measures to know the type of sessions that may have contributed the most to the erratic usage.
Highest secure gateway sessions	Indicates the highest recorded number of concurrent secure gateway sessions.	Number	
Highest sessions from other sources	Indicates the highest recorded number of concurrent sessions from other sources.	Number	
Highest application	Indicates the highest recorded number of	Number	If the value of the *Highest all sessions* measure is abnormally

Measurement	Description	Measurement Unit	Interpretation
sessions	concurrent application sessions.		high, you can compare the value of these two measures to know the type of sessions that may have contributed the most to the erratic usage.
Highest desktop sessions	Indicates the highest recorded number of concurrent desktop sessions.	Number	
Expiry Date (Days)	Indicates the number of days left for the VMware Horizon View license to expire.	Number	If an evaluation license is in use, this measure will report the number of days left for the license to expire. On the other hand, if a permanent license is obtained, a value *Unlimited* will be displayed indicating that the license will not expire at all.
Local desktop enabled	Indicates whether the local mode license is enabled or not.	Number	This measure will not be available from VMware Horizon View 6.0 onwards, as the 'Local Mode' feature has been deprecated from this version. The idea behind Local Mode is to let VMware Horizon View users run virtual desktops while offline, giving them portability and the ability to run applications even when they are not connected to enterprise servers. That is ideal for supporting employees who travel with laptops, work with multiple PCs at different locations or do not have persistent access to a broadband connection. This measure reports either *Enabled* or *Disabled* while indicating the status of the local

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>mode license. The numeric values that correspond to the above-mentioned states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>0</td></tr></table>Note:
By default, this measure reports the above- mentioned states while indicating the status of the local mode license. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.</td></tr>
<tr><td>View composer enabled</td><td>Indicates whether the View Composer license is enabled or not.</td><td>Number</td><td>This measure reports either Enabled or Disabled while indicating the status of the View Composer license. The numeric values that correspond to the above- mentioned states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>0</td></tr></table>Note:
By default, this measure reports the above- mentioned states while indicating the status of the View</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Composer license. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.

3.3.5 Events Database Connectivity Test

The event database stores information about View events as records in a database rather than in a log file. If the event database is unavailable, you will be compelled to scan the log files for event-related information; log files however, provide only limited information.

With the help of this test, you can promptly detect whether the VMware Horizon Connection Server is able to connect to the event database or not.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server Name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User Name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP

Parameter	Description
	query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* here.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Events database connectivity	Indicates whether the VMware Horizon Connection Server is able to connect to the Events database or not.	Number	This measure reports either *Connected* or *Disconnected* as the status of the event database connectivity. The numeric values that correspond to the above-mentioned states are as follows: State: Connected = 1; Disconnected = 0 If the event database is *Disconnected*, then you may have to look into the log files to obtain the information regarding

Measurement	Description	Measurement Unit	Interpretation
			View events, and the log files contain only limited information. Note: By default, this measure reports the above-mentioned states while indicating the status of the event database connectivity. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.

3.3.6 View Transfer Events

A View Transfer Server is a software service that manages and streamlines data transfers between the datacenter and View desktops that are checked out for use on end users' local systems. Periodic analysis of the events related to this service in the events database, will provide early warnings of transfer issues.

This test reports the number and details of transfer events recorded in the events database.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
DatabaseType	Specify the type of the database in the DatabaseType text box. By default, the DatabaseType is Microsoft SQL.

Parameter	Description
DatabaseServer	Specify the IP address of the database server that holds the VMware Horizon Connection Server event database.
DatabasePort	Specify the port of the database server.
Instance	Specify the instance name of the VMware Horizon Connection Server event database. By default, this is set to *none*.
EventsDatabaseName	Specify the name of the database that holds the VMware Horizon Connection Server events.
EventsTableName	Specify the name of the table containing the VMware Horizon View events in the VMware Horizon Connection Server events database.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name and Password	Provide the credentials of the user who has the authorization to execute queries on the Events Database.
Confirm Password	Confirm the password by retyping it here.
Domain	Specify the name of the domain in the Domain text box.
SSL	By default, the SSL flag is set to **No**. If the Microsoft SQL server that is hosting the Events Database is SSL-enabled, set this flag to **Yes**.
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 transfer events	Indicates the total number of transfer events recorded in the events database.	Number	The detailed diagnosis of this measure shows the details of the transfer events.

3.3.7 View Agent Connectivity Test

The View Agent is a software service that is installed on all guest virtual machines, physical systems, or terminal servers in order to allow them to be managed by View Manager.

This agent needs to be installed on VMs to make sure that the VMware Horizon View manager sees the clients that it needs to facilitate. The agent updates the VMware Horizon Connection Server with VM-related information, so that the server knows whether a particular VM is free or is being used by a user.

In the event of the non-availability of the View Agent, the View manager will neither be able to determine the status of VMs (whether a user is logged in or not) nor be able to avail the benefits of the connection monitoring, virtual printing, USB support and single sign-on facilities provided by the agent. To avoid this, you can use this test to periodically monitor the View Agent's connectivity with the Connection server, promptly detect breaks in connection, and fix it before users notice and complain.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The

Parameter	Description
	default port number is *NULL*.
Connection Server Name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User Name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* here.
View Install DIR	Indicate the full path to the install directory of the VMware Horizon Connection Server.
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.

Parameter	Description
	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
View Agent to Broker Connectivity	Indicates whether/not the View Agent is able to connect to the View server.	Percent	If this measure reports the value 100, it indicates that the View agent is able to connect to the server. The value 0 on the other hand suggests that the View agent is not able to connect to the server.

3.4 The Desktop Pools Layer

In VMware Horizon View a Desktop Pool is a managed entity. Within this managed entity you can configure the following options:

- Virtual Machines that are provided to the Connection Server
  - Automated Pools create virtual machines cloned from a base template
  - Manual Pools based on existing Virtual Machines managed by vCenter
  - Manual Pools based on physical desktops, Blade Workstations or Virtual Machines managed by other Visualization Provider
  - Terminal Services Desktop provided by a Terminal Server
- User that are entitled to connect to Virtual Desktops provided by this Desktop Pool
- Assign Users to desktops
- Desktop Pool properties – Automated and Manual Pools have different options

- Desktop Pool Policies
- Updates to existing desktops

You can monitor the composition and usage of the desktop pools using the tests mapped to the **Desktop Pools** layer.

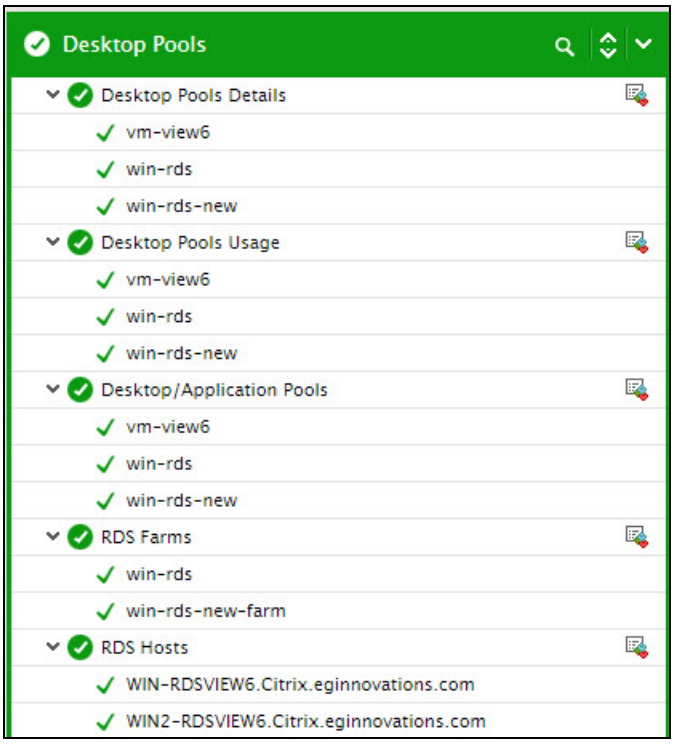

Figure 3.5: The test mapped to the Desktop Pools layer

3.4.1 Application Pools Details Test

This test monitors the status of each application pool configured on the VMware Horizon Connection Server and also reports whether/not each application pool is enabled. In addition, this test also reports the number of RDS hosts that are using each application pool.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each application pool configured on the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* here.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise

Parameter	Description
	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
Is application enabled?	Indicates whether/not this application is enabled.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** Yes / 0 No / 1 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate whether/not this application is enabled. The graph of this measure however, is represented using the numeric equivalents only i.e., 0 or 1. The detailed diagnosis of this measure lists the name of the RDS farms on which the application is enabled.
Application status	Indicates the current		The values reported by this measure

Measurement	Description	Measurement Unit	Interpretation
	status of this application.		and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** Available / 0 Unavailable / 1 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current status of this application. The graph of this measure however, is represented using the numeric equivalents only i.e., 0 or 1.
Total RDS hosts	Indicates the total number of RDS hosts using this application.	Number	The detailed diagnosis of this measure lists the name of the RDS hosts that are using the application.

3.4.2 Desktop Pools Details Test

This test monitors the status and usage of each desktop pool configured on a VMware Horizon Connection Server.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each desktop pool configured on the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection server. The default port number is *NULL*.

Parameter	Description
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
Is pool enabled?	Indicates whether this desktop pool is enabled or not.		This measure reports either *Enabled* or *Disabled* as the status of this desktop pool. The numeric values that correspond to the above- mentioned states are as follows: State: Enabled — Numeric Value: 1 State: Disabled — Numeric Value: 0 **Note:** By default, this measure reports the above- mentioned states while indicating the status of this desktop pool. However, the graph of this measure will be represented using the corresponding numeric

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>equivalents of the states as mentioned in the table above.</td></tr>
<tr><td>Is pool entitled?</td><td>Indicates whether any users or groups have been entitled to access this pool or not.</td><td></td><td>This measure reports either Entitled or UnEntitled as the status of the user in this desktop pool. The numeric values that correspond to the above-mentioned states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Entitled</td><td>1</td></tr><tr><td>UnEntitled</td><td>0</td></tr></table>Note:
By default, this measure reports the above- mentioned states while indicating the status of the user in this desktop pool. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.</td></tr>
<tr><td>Total entitled users in pool</td><td>Indicates the total number of entitled users presents in this pool.</td><td>Number</td><td>The detailed diagnosis of this measure displays the details of entitled users present in this desktop pool.</td></tr>
<tr><td>Local sessions</td><td>Indicates the total number of users present in the local session of this desktop pool.</td><td>Number</td><td>The details of users present in the local sessions can be viewed in the detailed diagnosis.</td></tr>
<tr><td>Remote sessions</td><td>Indicates the total number of users</td><td>Number</td><td>The details of users present in the remote session of this desktop pool</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	present in the remote session of this desktop pool.		can be viewed in the detailed diagnosis.
Total desktops registered	Indicates the total number of registered desktops present in this desktop pool.	Number	The detailed diagnosis of this measure provides the details of the registered desktops.

3.4.3 Desktop Pools Usage Test

This test reports the number and status of desktops in each desktop pool configured on the VMware Horizon Connection Server.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each desktop pool configured on the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
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
Total desktops	Indicates the total number of desktops in this pool.	Number	
Active desktops	Indicates the number of active desktops in this pool.	Number	The detailed diagnosis of this measure provides the details of active desktops.
Inactive desktops	Indicates the number of inactive desktops in this pool.	Number	The detailed diagnosis of this measure provides the details of inactive desktops.
Idle desktops	Indicates the number of idle desktops in this pool.	Number	Identify the idle desktops by viewing the detailed diagnosis of this measure.
Percentage of inactive desktops	Indicates the percentage of inactive desktops in this pool.	Percent	
Desktops utilized	Indicates the percentage of desktops actively used in this pool.	Percent	You can use the detailed diagnosis of the Active desktops measure to know which desktops are actively used.

3.4.4 Horizon Desktop Pools Test

This test monitors the status and usage of each desktop pool configured on a VMware Horizon Connection Server.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each desktop pool configured on the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify

Parameter	Description
	none here.
Report Total	By default, this flag is set to **false**. In this case therefore, the test will only report metrics for every desktop pool of the VMware Horizon Connection Server. If this flag is set to **true**, then the test will report metrics for a *Total* descriptor – the metrics reported by this descriptor will be aggregated across all desktop pools of the target VMware Horizon Connection Server. This way, administrators will receive in-depth insights into the functioning of the desktop pools.
Show Total Desktop DD	By default, this flag is set to **No**, indicating that this test will not report detailed diagnostics for the **Total desktops** measure. This means that the test, by default, will not capture and store the details of every desktop in a pool, in the eG database. This default setting is ideal for large VDI infrastructures, where a single pool can contain hundreds of desktops, as it can help conserve space in the eG database and reduce the strain on the database. However, if your eG database is well-sized and you want to view the complete list of desktops in a pool, enable the detailed diagnosis capability of the **Total desktops** measure by setting this flag to **Yes**.
Remote Session DD	By default, this flag is set to **No**, indicating that this test will not report detailed diagnostics for the **Remote Sessions** measure. This means that the test, by default, will not capture and store the details of the remote sessions to each desktop in a desktop pool, in the eG database. This default setting is ideal for large VDI infrastructures, where a single pool can contain hundreds of desktops, as it can help conserve space in the eG database and reduce the strain on the database. However, if your eG database is well-sized and you want to view the complete list of remote sessions to the desktops in a pool, enable the detailed diagnosis capability of the **Remote Sessions** measure by setting this flag to **Yes**.
Disconnected Desktop DD	By default, this flag is set to **No**, indicating that this test will not report detailed diagnostics for the **Disconnected Desktops** measure. This means that the test, by default, will not capture and store the details of the desktops that were disconnected from a desktop pool, in the eG database. This default setting is ideal for large VDI infrastructures, where a single pool can contain hundreds of desktops, as it can help conserve space in the eG database and reduce the strain on the

Parameter	Description
	database. However, if your eG database is well-sized and you want to view the complete list of desktops that were disconnected from a pool, enable the detailed diagnosis capability of the **Disconnected Desktops** measure by setting this flag to **Yes**.
Disconnected Application DD	By default, this flag is set to **No**, indicating that this test will not report detailed diagnostics for the **Disconnected Applications** measure. This means that the test, by default, will not capture and store the details of the applications (in each desktop pool) that were disconnected from the View Client, in the eG database. This default setting is ideal for large VDI infrastructures, where a single pool can contain hundreds of desktops, as it can help conserve space in the eG database and reduce the strain on the database. However, if your eG database is well-sized and you want to view the complete list of applications that were disconnected from the View Client, enable the detailed diagnosis capability of the **Disconnected Applications** measure by setting this flag to **Yes**.
Maintenance Desktop DD	By default, this flag is set to **No**, indicating that this test will not report detailed diagnostics for the **Maintenance Desktops** measure. This means that the test, by default, will not capture and store the details of the desktops that were in *Maintenance mode* in a desktop pool, in the eG database. This default setting is ideal for large VDI infrastructures, where a single pool can contain hundreds of desktops, as it can help conserve space in the eG database and reduce the strain on the database. However, if your eG database is well-sized and you want to view the complete list of desktops that were in *Maintenance mode* in a desktop pool, enable the detailed diagnosis capability of the **Maintenance Desktops** measure by setting this flag to **Yes**.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *3:1*. This indicates that, by default, detailed measures will be generated every third 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

Parameter	Description
	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
Desktop source	Indicates the source of this desktop pool.		This measure reports either Enabled or Disabled as the status of this desktop pool. The numeric values that correspond to the above-mentioned states are as follows: State: Remote Desktop Services — Numeric Value: 1 State: vCenter (instant clone) — Numeric Value: 2 State: vCenter (linked clone) — Numeric Value: 3 State: vCenter — Numeric Value: 4 State: Others — Numeric Value: 5 **Note:** By default, this measure reports the above-mentioned states while indicating the source of this desktop pool. However, the graph of this measure will be represented using the corresponding

Measurement	Description	Measurement Unit	Interpretation
			numeric equivalents of the states as mentioned in the table above.
Desktops with agent unreachable	Indicates the number of desktops in this pool that are currently in the *Agent unreachable* state.	Number	
Provisioned desktops	Indicates the number of desktops in this pool that are currently in the *Provisioned* state.	Number	A non-zero value for this measure indicates that one/more desktops in the pool are powered-off or suspended.
Desktops with agent disabled	Indicates the number of desktops in this pool that are currently in the *Agent Disabled* state.	Number	
Invalid IP desktops	Indicates the number of desktops in this pool that are currently in the *Invalid IP* state.	Number	
Desktops where agent needs reboot	Indicates the number of desktops in this pool that are currently in the *Agent needs reboot* state.	Number	
Desktops with protocol failure	Indicates the number of desktops in this pool that are currently in the *Protocol failure* state.	Number	
Domain failure desktops	Indicates the number of desktops in this pool that are currently in the *Domain failure* state.	Number	
Already used desktops	Indicates the number of desktops in this pool that are currently in the *Already used* state.	Number	If a desktop that is set to refresh on log off is reset, the desktop goes into the Already Used state.

Measurement	Description	Measurement Unit	Interpretation
Desktops with configuration errors	Indicates the number of desktops in this pool that are currently experiencing configuration errors.	Number	A high value for this measure indicates that many errors occurred during desktop configuration. This is worrisome and should be investigated.
Desktops with provisioning errors	Indicates the number of desktops in this pool that are currently experiencing provisioning errors.	Number	A high value for this measure indicates that many errors occurred during desktop provisioning. This is worrisome and should be investigated.
Unassigned user connected desktops	Indicates the number of desktops in this desktop pool that are currently in the *Unassigned user connected* state.	Number	
Unassigned user disconnected desktops	Indicates the number of desktops in this desktop pool that are currently in the *Unassigned user disconnected* state.	Number	
Provisioning desktops	Indicates the number of desktops in this pool that are currently in the *Provisioning* state.	Number	A non-zero value for this measure indicates that desktops in the pool are being provisioned.
Waiting for agent desktops	Indicates the number of desktops in this pool that are currently in *Waiting for agent* state.	Number	
Startup desktops	Indicates the number of desktops in this pool that are currently in the *Startup* state.	Number	
Is pool enabled?	Indicates whether this desktop pool is enabled or not.		This measure reports either Enabled or Disabled as the status of this desktop pool. The numeric values that correspond to the above-mentioned states are as follows:

<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>State</th><th>Numeric Value</th></tr>
<tr><td>Enabled</td><td>1</td></tr>
<tr><td>Disabled</td><td>0</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned states while indicating the status of this desktop pool. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.
</td></tr>
<tr><td>Pool type</td><td>Indicates the pool type.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:
<table>
<tr><th>Measure Value</th><th>Description</th><th>Numeric Value</th></tr>
<tr><td>Manual</td><td>Manual desktop pools are a collection of existing vCenter Server virtual machines, physical computers, or third-party virtual machines. In automated or manual pools, each Windows machine is available for one user to access remotely at a time.</td><td>2</td></tr>
<tr><td>RDS</td><td>RDS desktop pools are not a collection of Windows machines, but instead, provide users</td><td>1</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Description</th><th>Numeric Value</th></tr>
<tr><td></td><td>with desktop sessions on RDS hosts. Multiple users can have desktop sessions on an RDS host simultaneously.</td><td></td></tr>
<tr><td>Automated Desktop Pool</td><td></td><td>3</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the pool type. However, in the graph of this measure, the same will be represented using the corresponding numeric equivalents only.
</td></tr>
<tr><td>Is pool entitled?</td><td>Indicates whether any users or groups have been entitled to access this pool or not.</td><td></td><td>This measure reports either Entitled or UnEntitled as the status of the user in this desktop pool. The numeric values that correspond to the above-mentioned states are as follows:
<table>
<tr><th>State</th><th>Numeric Value</th></tr>
<tr><td>Entitled</td><td>1</td></tr>
<tr><td>UnEntitled</td><td>0</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned states while indicating the status of the user in this desktop pool. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.</td></tr>
<tr><td>Total entitled users</td><td>Indicates the total</td><td>Number</td><td>The detailed diagnosis of this measure</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
in pool	number of entitled users present in this pool.		displays the details of entitled users present in this desktop pool.
Local sessions	Indicates the total number of local sessions to the desktops in this pool.	Number	The details of the local sessions can be viewed in the detailed diagnosis.
Remote sessions	Indicates the total number of remote sessions to the desktops in this desktop pool.	Number	The details of the remote sessions can be viewed in the detailed diagnosis.
Total desktops	Indicates the total number of desktops in this pool.	Number	Use the detailed diagnosis of this measure, if enabled, to know the desktops in this pool.
Connected desktops	Indicates the number of desktops in this pool that are in active sessions and have active remote connections to a View client.	Number	The detailed diagnosis of this measure provides the details of the connected desktops.
Disconnected desktops	Indicates the number of desktops in this pool that are in active sessions but are disconnected from the View client.	Number	The detailed diagnosis of this measure provides the details of disconnected desktops.
Idle desktops	Indicates the number of idle desktops in this pool.	Number	Identify the idle desktops by viewing the detailed diagnosis of this measure.
Percentage of disconnected desktops	Indicates the percentage of disconnected desktops in this pool.	Percent	A value close to 100% for this measure could indicate that almost all the desktops in the pool are disconnected from the View client. This is a cause for serious concern and requires immediate attention.
Desktops utilization	Indicates the percentage of desktops actively used in this pool.	Percent	Ideally, the value of this measure should be high.
Connected applications	Indicates the number of applications in this pool	Number	

Measurement	Description	Measurement Unit	Interpretation
	that are in active sessions and have active remote connections to a View client.		
Disconnected applications	Indicates the number of applications in this pool that are in active sessions but are disconnected from the View client.	Number	
Ready desktops	Indicates the number of desktops in this pool that are in the *READY* state currently.	Number	
Error desktops	Indicates the number of desktops in this pool that are in the *Error* state currently.	Number	A non-zero value for this measure is a cause for concern, as it indicates that one/more desktops in the pool have experienced an unknown error.
Maintenance desktops	Indicates the number of desktops in this pool that are in the *Maintenance mode* presently.	Number	When a desktop is in the Maintenance mode, users cannot log in or use that desktop.
Deleting desktops	Indicates the number of desktops in this pool that are currently in the *Deleting* state.	Number	A non-zero value for this measure indicates that one/more desktops in the pool have been marked for deletion, and will be deleted soon.
Customizing desktops	Indicates the number of desktops in this pool that are presently in the *Customizing* state.	Number	A non-zero value for this measure indicates that one/more desktops in an automated pool are being customized.
Provisioning desktops	Indicates the number of desktops in this pool that are currently in the *Provisioning* state.	Number	A non-zero value for this measure indicates that desktops in the pool are being provisioned.
Provisioned	Indicates the number of	Number	A non-zero value for this measure

Measurement	Description	Measurement Unit	Interpretation
desktops	desktops in this pool that are currently in the *Provisioned* state.		indicates that one/more desktops in the pool are powered-off or suspended.
Desktops with provisioning errors	Indicates the number of desktops in this pool that are currently experiencing provisioning errors.	Number	A high value for this measure indicates that many errors occurred during desktop provisioning. This is worrisome and should be investigated.
Unknown desktops	Indicates the number of desktops in this pool that are currently in an *Unknown* state.	Number	Ideally, the value of this measure should be 0.
Available desktops	Indicates the number of desktops in this pool that are currently in the *Available* state.	Number	This refers to the number of desktops that are powered on and ready for an active connection.
Already used desktops	Indicates the number of desktops in this pool that are currently in the *Already used* state.	Number	If a desktop that is set to refresh on log off is reset, the desktop goes into the Already Used state.
Active entitled users utilization	Indicates the percentage of entitled users currently active in this pool, who are accessing View via PCoIP.	Percent	
Spare desktops	Indicates the number of spare (powered on) desktops that are to be maintained in this pool.	Number	Generally, you want the number of spare desktops at least to equal the number of users that log in within a short time span (usually a few minutes). These reserves ensure that users have an available desktop. You should monitor user-login activity and adjust the settings accordingly.
Maximum desktops	Indicates the maximum number of desktops that can be accommodated in this pool.	Number	

Measurement	Description	Measurement Unit	Interpretation
Minimum desktops	Indicates the minimum number of desktops to be maintained in this pool.	Number	
PCoIP Sessions	Indicates the number of PCoIP sessions to the desktops in this desktop pool.	Number	The details of the PCoIP sessions can be viewed in the detailed diagnosis.
Blast Sessions	Indicates the number of Blast sessions to the desktops in this desktop pool.	Number	The details of the Blast sessions can be viewed in the detailed diagnosis.
RDP sessions	Indicates the number of RDP sessions to the desktops in this desktop pool.	Number	The details of the RDP sessions can be viewed in the detailed diagnosis.

3.4.5 Horizon RDS Farms Test

Farms are collections of RDS hosts and facilitate the management of those hosts. Farms can have a variable number of RDS hosts and provide a common set of applications or RDS desktops to users. When you create an RDS desktop pool or an application pool, you must specify a farm. To know the composition of an RDS farm and track the status of the desktops and applications in the farm, take the help of the RDS Farms test. For every RDS farm, this test reports the count of RDS hosts in the farm, the number and type of sessions active in that farm, and the state of desktops and applications in that farm.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each RDS farm managed by the VMware Horizon Connection Server being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed

Parameter	Description
Host	The host for which the test is to be configured
Port	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* here.
Show RDS Host DD	By default, this flag is set to **No**, indicating that this test will not report detailed diagnostics for the **RDS Hosts** measure. This means that the test, by default, will not capture and store the details of every RDS host in a farm, in the eG database. This default setting is ideal for large RDS farms characterized by hundreds of hosts, as it helps conserve space in the eG database and reduce the strain on the database. However, if your eG database is well-sized and you want to

Parameter	Description
	view the complete list of RDS hosts in a farm, enable the detailed diagnosis capability of the **RDS hosts** measure by setting this flag to **Yes**.
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
RDS hosts	Indicates the number of RDS hosts in this farm.	Number	
Application pools	Indicates the number of application pools in this farm.	Number	Application pools let you deliver applications to many users. The applications in application pools run on a farm of RDS hosts.
Local sessions	Indicates the number of local sessions to	Number	

Measurement	Description	Measurement Unit	Interpretation
	desktops/applications in this farm.		
Remote sessions	Indicates the number of remote sessions to desktops/applications in this farm.	Number	
Connected desktops:	Indicates the number of desktops in this farm that are in active sessions and have active remote connections to a View client.	Number	
Disconnected desktops	Indicates the number of desktops in this farm that are in active sessions but are disconnected from the View client.	Number	A non-zero value is a cause for concern.
Connected applications	Indicates the number of applications in this farm that are in active sessions and have active remote connections to a View client.	Number	
Disconnected applications	Indicates the number of applications in this farm that are in active sessions but are disconnected from the View client.	Number	A non-zero value warrants close scrutiny.
Is enabled?	Indicates whether/not this farm is enabled.		This measure a value *Yes* if the farm is enabled and *No*, if otherwise. The numeric values that correspond to the above-mentioned states are as follows: State: Yes — Numeric Value: 1 State: No — Numeric Value: 0

Measurement	Description	Measurement Unit	Interpretation
			Note: By default, this measure reports the above-mentioned states while indicating the status of this farm. However, the graph of this measure will be represented using the corresponding numeric equivalents of the states as mentioned in the table above.
PCoIP Sessions	Indicates the number of PCoIP sessions to the desktops/applications in this farm.	Number	The details of the PCoIP sessions can be viewed in the detailed diagnosis.
Blast Sessions	Indicates the number of Blast sessions to the desktops/applications in this farm.	Number	The details of the Blast sessions can be viewed in the detailed diagnosis.
RDP sessions	Indicates the number of RDP sessions to the desktops/applications in this farm.	Number	The details of the RDP sessions can be viewed in the detailed diagnosis.

3.4.6 Horizon RDS Hosts Test

RDS hosts are server computers that have Windows Remote Desktop Services and View Agent installed. These servers host applications and desktop sessions that users can access remotely. To know the status of each RDS host, what type of sessions are active on each RDS host in a farm and to determine the status of desktops/applications on each host, use the RDS Hosts test.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each RDS host managed by the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Connection Server name	Specify the name of the target VMware Horizon Connection Server that is to be monitored.
User name	By default, eG Enterprise uses a dual approach i.e., uses VMware PowerCLI and LDAP queries to collect metrics from the target VMware Horizon Connection Server 7 (or above). This dual approach ensures that the metrics are collected more faster than the LDAP query-only approach used for the prior versions of the VMware Horizon Connection Server. Administrators need to install the VMware PowerCLI on the target VMware Horizon Connection server and configure the eG agent to communicate with that CLI to pull the metrics. PowerCLI is a command-line and scripting tool built on Windows PowerShell, which enables easy management, configuration, and automation of vSphere and vCloud environments. With the help of this CLI, the eG agent collects metrics from the target server more quickly than the LDAP approach that was used to collect metrics from VMware Horizon Connection Server version 6 and below. In order to collect metrics using VMware PowerCLI, administrators need to specify the name of the user possessing *read-only administrator* role in the VMware Horizon Management Console.
Password	Specify the password corresponding to the user here.
Confirm Password	Confirm the password by retyping it here.
Domain Name	Specify the name of the domain to which the VMware Horizon Connection Server belongs to. If the target VMware Horizon Connection Server does not belong to any domain, specify *none* here.
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

Parameter	Description
	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
Local sessions	Indicates the number of local sessions to desktops /applications on this host.	Number	
Remote sessions	Indicates the number of remote sessions to desktops /applications on this host.	Number	
PCoIP Sessions	Indicates the number of PCoIP sessions to the desktops/applications in this host.	Number	The details of the PCoIP sessions can be viewed in the detailed diagnosis.
Blast Sessions	Indicates the number of Blast sessions to the desktops/applications in this host.	Number	The details of the Blast sessions can be viewed in the detailed diagnosis.

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Connected desktop sessions</td><td>Indicates the number of desktops on this host that are in active sessions and have active remote connections to a View client.</td><td>Number</td><td></td></tr>
<tr><td>Disconnected desktop sessions</td><td>Indicates the number of desktops on this host that are in active sessions but are disconnected from the View client.</td><td>Number</td><td>A non-zero value is a cause for concern.</td></tr>
<tr><td>Connected applications</td><td>Indicates the number of applications on this host that are in active sessions and have active remote connections to a View client.</td><td>Number</td><td></td></tr>
<tr><td>Disconnected applications</td><td>Indicates the number of applications on this host that are in active sessions but are disconnected from the View client.</td><td>Number</td><td>A non-zero value warrants close scrutiny.</td></tr>
<tr><td>Status</td><td>Indicates the current status of this host.</td><td></td><td>The values that this measure can take and its corresponding numeric values are discussed in the table below:<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>1</td></tr><tr><td>Unassigned user dis-connected</td><td>2</td></tr><tr><td>Unassigned user con-nected</td><td>3</td></tr><tr><td>Error</td><td>4</td></tr></table></td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Provisioning error</td><td>5</td></tr>
<tr><td>Configuration error</td><td>6</td></tr>
<tr><td>Already used</td><td>7</td></tr>
<tr><td>Domain failure</td><td>8</td></tr>
<tr><td>Protocol failure</td><td>9</td></tr>
<tr><td>Agent needs reboot</td><td>10</td></tr>
<tr><td>Invalid ip</td><td>11</td></tr>
<tr><td>Agent unreach-able</td><td>12</td></tr>
<tr><td>Agent disabled</td><td>13</td></tr>
<tr><td>Startup</td><td>14</td></tr>
<tr><td>Maintenance</td><td>15</td></tr>
<tr><td>Deleting</td><td>16</td></tr>
<tr><td>Waiting for agent</td><td>17</td></tr>
<tr><td>Customizing</td><td>18</td></tr>
<tr><td>Provisioning</td><td>19</td></tr>
<tr><td>Disconnected</td><td>20</td></tr>
<tr><td>Connected</td><td>21</td></tr>
<tr><td>Available</td><td>22</td></tr>
<tr><td>Provisioned</td><td>23</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values to indicate the current status of this host. However, the graph of this measure will represent the same using the numeric equivalents only.
</td></tr>
<tr><td>Maximum</td><td>Indicates the maximum</td><td>Number</td><td></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
connections	connections that can be provided to the desktops/applications on this host.		
RDP sessions	Indicates the number of RDP sessions to the desktops/applications in this host.	Number	The details of the RDP sessions can be viewed in the detailed diagnosis.

3.4.7 Horizon Application Launches Test

The virtual desktops/applications are launched by clients on the VMware Horizon Connection server. To know the exact number of applications that were launched and the average time taken to launch an application, use the **Horizon Application Launches** test. Using this test, you can also figure out the number of applications that failed to launch and the maximum time taken to launch an application. This way, administrators can identify those applications that took too long to launch and the users who attempted to launch the applications.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection Server being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Logfile Path	In the Logfile Path text box, specify the full path to the *debug-<current date>* file where the details of the applications launched through the VMware Horizon Connection Server is stored. By default, the file will be available in the *C:\Program files\VMware\VDM* directory. If the file indeed resides in its default location, set the Logfile Path to *none*. On the other hand, if the file has been installed in a different

Parameters	Description
	location, provide the full path to that location against the Logfile Path.
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
Launched applications	Indicates the number of applications that were launched.	Number	The detailed diagnosis of this measure if enabled, lists the applications that were launched, the session ID, the username, the time taken to launch the application, the machine ID, the server address and server port, the Client IP address etc.
Max launch time	Indicates the maximum time taken to launch an application.	Secs	The detailed diagnosis of this measure helps you to identify the application that took too long to be launched. The detailed diagnosis

Measurement	Description	Measurement Unit	Interpretation
			of this measure if enabled lists the Session ID, the user who is accessing the application, the time taken to launch the application (in secs), the machine ID, the server address, the server port, the server protocol and the client IP address.
Avg launch time	Indicates the average time taken to launch the applications.	Secs	A high value for this measure is a cause of concern.
Failed applications	Indicates the number of applications that failed.	Number	The detailed diagnosis of this measure if enabled, lists the Session ID, the user who is accessing the desktop, the Client IP, the Client address, the error message describing the reason for the failure of the desktops.

3.4.8 Horizon Desktop Launches Test

The virtual desktops/applications are launched by clients on the VMware Horizon View Connection server. To know the exact number of virtual desktops that were launched and the average time taken to launch a desktop, use the **Horizon Desktop Launches** Test. Using this test, you can also figure out the number of desktops that failed to launch and the maximum time taken to launch a desktop. This way, administrators can identify those desktops that took too long to launch and the users who attempted to launch the desktops.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection Server being monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
Logfile Path	In the Logfile Path text box, specify the full path to the *debug-<current date>* file where the details of the applications launched through the Horizon view connection server is stored. By default, the file will be available in the *C:\Program files\VMware\VDM* directory. If the file indeed resides in its default location, set the Logfile Path to *none*. On the other hand, if the file has been installed in a different location, provide the full path to that location against the Logfile Path.
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
Launched desktops	Indicates the number of desktops that were	Number	The detailed diagnosis of this measure if enabled lists the

Measurement	Description	Measurement Unit	Interpretation
	launched.		Session ID, the user who is accessing the desktop, the time taken to launch the desktop, the machine ID, the server address, the server port, the server protocol and the client IP address.
Max launch time	Indicates the maximum time taken to launch a desktop.	Seconds	A sudden/gradual increase in the value of this measure is a cause of concern. Use the detailed diagnosis of this measure to figure out the desktop that too the maximum time to launch. The detailed diagnosis of this measure if enabled lists the Session ID, the user who is accessing the desktop, the time taken to launch the desktop (in secs), the machine ID, the server address, the server port, the server protocol and the client IP address.
Avg launch time	Indicates the average time taken to launch the desktops.	Seconds	A high value for this measure is a cause of concern.
Failed desktops	Indicates the number of desktops that failed.	Number	The detailed diagnosis of this measure if enabled lists the Session ID, the user who is accessing the desktop, the Client IP, the Client address, the error message describing the reason for the failure of the desktops.

3.4.9 Pool Launch Error Details Test

The events database stores information about desktop pool launch events as records in a database rather than in a log file. This database serves as a rich source of information on the status of and problems encountered by VMware Horizon Connection Server. Using the **Pool Launch Error Details** test, administrators can periodically query the events database for the count of errors that the VMware Horizon Connection Server has encountered during desktop pool launch events, and also view the details of such events. With the help of these details, administrators can easily and effectively troubleshoot issues affecting the operations of VMware Horizon Connection Server.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
DatabaseType	Specify the type of the database in the DatabaseType text box. By default, the DatabaseType is Microsoft SQL.
DatabaseServer	Specify the IP address of the database server that holds the VMware Horizon Connection Server event database.
DatabasePort	Specify the port of the database server.
Instance	Specify the instance name of the VMware Horizon Connection Server event database. By default, this is set to *none*.
EventsDatabaseName	Specify the name of the database that holds the VMware Horizon Connection Server events.
EventsTableName	Specify the name of the table containing the VMware Horizon View events in the VMware Horizon Connection Server events database.
User and Password	Provide the credentials of the user who has the authorization to execute queries

Parameter	Description
	on the Events Database.
Confirm Password	Confirm the password by retyping it here.
Domain	Specify the name of the domain in the Domain text box.
SSL	By default, the SSL flag is set to **No**. If the Microsoft SQL server that is hosting the Events Database is SSL-enabled, set this flag to **Yes**.
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 third 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
Launch errors	Indicates the total number of errors recorded in the database during the last measurement period.	Number	Ideally, value of this measure should be zero. For complete details of the errors occurred during the desktop pool launch events, use the detailed diagnosis of this measure.

3.4.10 Pool Provisioning Error Details Test

The events database stores information about desktop pool provisioning events as records in a database rather than in a log file. This database serves as a rich source of information on the status of and problems encountered by VMware Horizon Connection server. Using the **Pool Provisioning Error Details** test, administrators can periodically query the events database for the count of errors that the VMware Horizon Connection server has encountered during desktop pool provisioning events, and also view the details of such events. With the help of these details, administrators can easily and effectively troubleshoot issues affecting the operations of VMware Horizon Connection server.

Target of the test : A VMware Horizon Connection server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
DatabaseType	Specify the type of the database in the DatabaseType text box. By default, the DatabaseType is Microsoft SQL.
DatabaseServer	Specify the IP address of the database server that holds the VMware Horizon Connection Server event database.
DatabasePort	Specify the port of the database server.
Instance	Specify the instance name of the VMware Horizon Connection Server event database. By default, this is set to *none*.
EventsDatabaseName	Specify the name of the database that holds the VMware Horizon Connection Server events.
EventsTableName	Specify the name of the table containing the VMware Horizon View events in the VMware Horizon Connection Server events database.

Parameter	Description
User and Password	Provide the credentials of the user who has the authorization to execute queries on the Events Database.
Confirm Password	Confirm the password by retyping it here.
Domain	Specify the name of the domain in the Domain text box.
SSL	By default, the SSL flag is set to **No**. If the Microsoft SQL server that is hosting the Events Database is SSL-enabled, set this flag to **Yes**.
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 third 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
Provisioning errors	Indicates the total number of errors recorded in the database during the last measurement period.	Number	Ideally, value of this measure should be zero. For complete details of the errors occurred during the desktop pool provisioning events, use the detailed diagnosis of this measure.

3.4.11 ThinApp Repository Test

ThinApp is an application virtualization tool that packages virtual applications into executable files and allows distribution of the applications across the virtual environment. The ThinApp packages reside on a ThinApp repository in a network share. This way, administration and sharing of the applications across the virtual environment become easier. As an administrator, you can copy a full ThinApp package from the repository to the virtual desktop. You can also place a shortcut on the virtual desktop that points to the ThinApp package on the repository. It is therefore imperative that availability of the repository is critical to access the applications reside in it. If the repository is found to be inaccessible due to network connectivity failure between the View Connection server and the repository, the applications reside in the repository also become unavailable to users. This in turn impacts the user experience and degrade the performance of the Connection server. To prevent such eventualities, you should continuously monitor the availability of the ThinApp repositories. The **ThinApp Repository** test helps you in this regard!

This test auto-discovers all the ThinApp repositories that are registered with the VMWare Horizon Connection server and reports availability of each ThinApp repository.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each *ThinApp repository* that is registered with the the VMWare Horizon Connection server.

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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
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**.

Parameter	Description
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.

Configurable parameters for the test

1. **TEST PERIOD** – How often should the test be executed.
2. **HOST** – The host for which the test is to be configured.
3. **PORT** – Refers to the port used by VMware Horizon View Connection Server. The default port number is NULL.
4. **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**.
5. **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
Availability:	Indicates whether/not the this repository is available.	Percent	A value of 100 indicates that this repository is available. The value 0 indicates that the repository is not available. The detailed diagnosis of the measure appears only if the value of this measure is 0. The detailed diagnosis reveals the network path of ThinApp repository which is not available.

3.4.12 ThinApps Test

You can assign the ThinApp virtual applications from the ThinApp repository to desktops and pools that have virtual machine sources in the following ways:

- **Streaming** - Shortcuts to the ThinApp virtual applications are created on the desktops. These shortcuts point to the applications on the network share that hosts the ThinApp repositories. Users must have access to the network share to run streamed ThinApp applications.
- **Full** - Full ThinApp virtual applications are installed on the local file systems of the desktops.

To know the exact number of desktops to which a specific application from a particular repository was assigned and how the applications were assigned on the desktops, use the **ThinApps** test. This way, you can identify those applications that were frequently accessed and the installation type in which the applications were assigned to the desktops.

Target of the test : A VMware Horizon Connection Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each *ThinApp repository:application* pair that is registered with the VMware Horizon Connection 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	Refers to the port used by VMware Horizon Connection Server. The default port number is *NULL*.
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
Assignments	Indicates the number of desktops to which this application on this repository was assigned.	Number	Compare the value of this measure across the applications to identify which application on a particular repository is assigned mostly. The detailed diagnosis of this measure

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>reveals the name of desktops to which the application was assigned.</td></tr>
<tr><td>Application type</td><td>Indicates the type of this application on this repository.</td><td></td><td>The numeric values that correspond to the measure values discussed above are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Full</td><td>1</td></tr><tr><td>Stream</td><td>2</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values while indicating type of this application. However, in the graph of this measure, the same will be indicated using the corresponding numeric equivalents of the types as mentioned in the table above.</td></tr>
</table>

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.