Enabling Service Excellence

Monitoring the VMware Horizon Connection Server

eG Enterprise v6

Table of Contents

1

Monitoring the VMware Horizon Connection Server

VMware Horizon Connection Server 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 Connection Server 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 Connection Server 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 Connection Server:

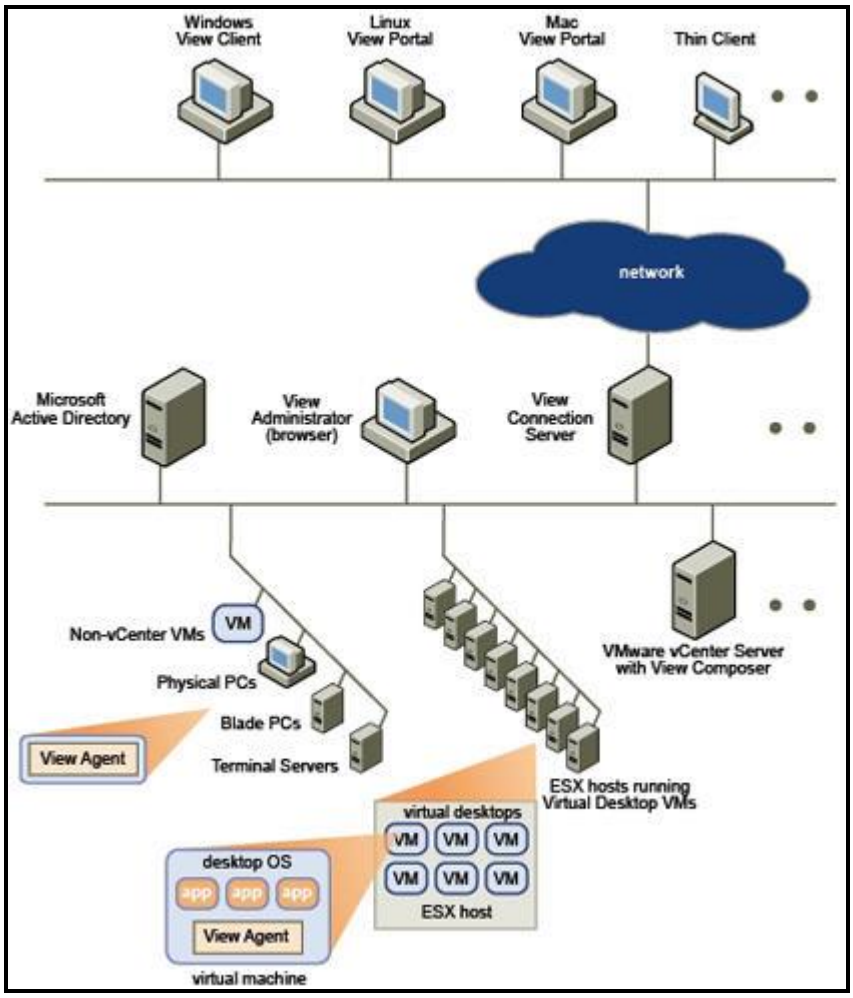

Figure 1.1: The core components of VMware Horizon Connection Server

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 Connection Server 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 Connection Server should be continuously monitored.

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

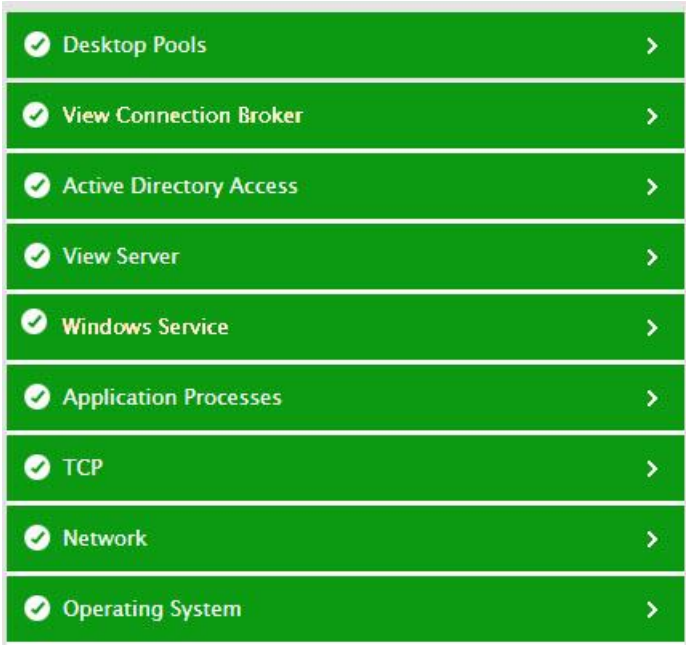

Figure 1.2: Layer model of VMware Horizon Connection Server

Each layer of the Figure 1.2 is mapped to a variety of tests that provide valuable insights into the overall health and performance of VMware Horizon Connection Server 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 broke r enabled?
- Is the VMware Horizon Connection Server server able to connect to the events database?
- Will the VMware Horizon Connection Server 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 1.2. The remaining layers have already been dealt with in the *Monitoring Unix and Windows Servers* document.

1.1 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.

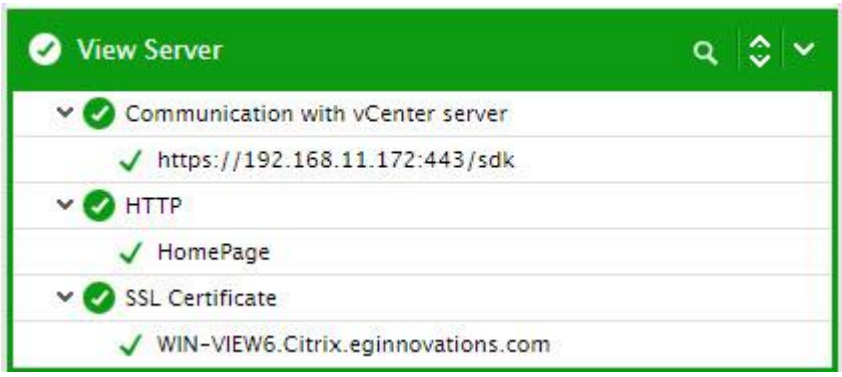

Figure 1.3: The test mapped to the View Server layer

1.1.1 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.

Purpose	Proactively alerts administrators to potential connectivity issues between the View Manager and the vCenter server, and 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	An internal agent

<table>
<tr><td>deploying the test</td><td colspan="3"></td></tr>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The host for which the test is to be configured
3. PORT – Refers to the port used by VMware Horizon Connection Server. The default port number is NULL.
4. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the VMware Horizon Connection Server server being monitored</td></tr>
<tr><td>Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td></td><td>vCenter connectivity:
Indicates whether the vCenter connectivity is available to the View Manager or not.</td><td></td><td>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:
<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.</td></tr>
</table>

1.2 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.

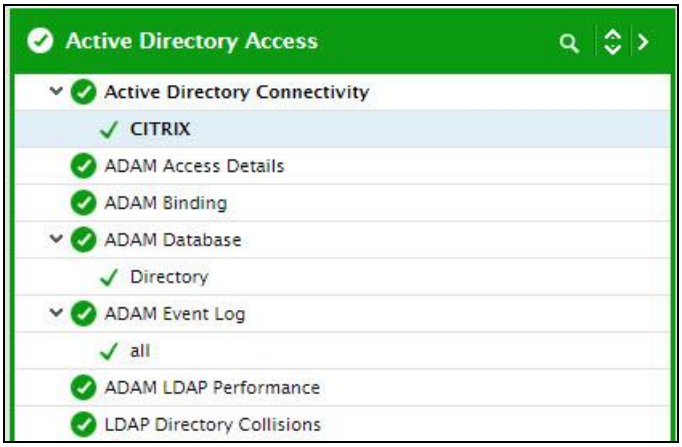

Figure 1.4: The tests mapped to the Active Directory Access layer

1.2.1 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 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 Connection Server - AD server connection, and promptly detect problems in it, so that the connection can be restored before users begin to complaint.

Purpose	Continuously monitors the VMware Horizon Connection Server - AD server connection, and promptly detects 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

<table>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The host for which the test is to be configured
3. PORT – Refers to the port used by VMware Horizon Connection Server. The default port number is NULL.
4. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the VMware Horizon Connection Server server being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Active directory connection state:
Indicates whether the VMware Horizon Connection Server server is able to connect to the Active Directory server or not.</td><td></td><td>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:
<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 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.</td></tr>
</table>

1.2.2 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?

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

Purpose	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? • Which AD service performed the maximum searches on the AD server? • Is the server sized with adequate threads to handle the I/O load?		
Target of the test	An Active Directory or Domain Controller on Windows 2008		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD -** How often should the test be executed 2. **HOST -** The IP address of the machine where the Active Directory is installed. 3. **PORT –** The port number through which the Active Directory communicates. The default port number is 389.		
Outputs of the test	One set of results for every Active Directory being monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

test	**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 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.
	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 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 directory.	Percent	The Local Security Authority (LSA) is the security subsystem responsible for all interactive user authentication and authorization 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 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 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 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 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 performed by the Knowledge Consistency Checker 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 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 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 of searches on the AD server - is it the replication service? the LSA? the KCC? the NSPI? the NTDS? or the SAM?

1.2.3 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.

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

Purpose	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 object to the directory object
Target of the test	An Active Directory or Domain Controller on Windows 2008
Agent deploying the	An internal agent

test			
Configurable parameters for the test	1. **TEST PERIOD -** How often should the test be executed 2. **HOST -** The IP address of the machine where the Active Directory is installed. 3. **PORT –** The port number through which the Active Directory communicates. The default port number is 389.		
Outputs of the test	One set of results for every Active Directory being monitored		
Measurements made by the test	**Measurement**	**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	

1.2.4 ADAM Database Test

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

Purpose	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		
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT –** Refers to the port used by the Windows server		
Outputs of the test	One set of results for every AD server being monitored		
Measurements made by the test	**Measurement**	**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	
	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	

1.2.5 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.

Purpose	Reports statistical information about Active Directory performance recorded in the event log
Target of the test	A VMware Horizon Connection Server server

Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** - The host for which the test is to be configured 3. **PORT –** Refers to the port used by the EventLog Service. Here it is null. 4. **LOGTYPE** – Refers to the type of event logs to be monitored. The default value is *application*. 5. **POLICY BASED FILTER** - Using this page, administrators can configure the event sources, event IDs, and event descriptions to be monitored by this test. In order to enable administrators to easily and accurately provide this specification, this page provides the following options: ➢ Manually specify the event sources, IDs, and descriptions in the **FILTER** text area, or, ➢ Select a specification from the predefined filter policies listed in the **FILTER** box For explicit, manual specification of the filter conditions, select the **NO** option against the **POLICY BASED FILTER** field. This is the default selection. To choose from the list of pre-configured filter policies, or to create a new filter policy and then associate the same with the test, select the **YES** option against the **POLICY BASED FILTER** field. 6. **FILTER** - If the **POLICY BASED FILTER** flag is set to **NO**, then a **FILTER** text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that the **FILTER** text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here: • *OS_events* is the display name that will appear as a descriptor of the test in the monitor UI; • *all* indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify *none*. • Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, *Browse* and *Print* have been excluded from monitoring. Alternatively, you can use *all* to indicate that all the event sources have to be excluded from monitoring, or *none* to denote that none of the event sources need be excluded. • In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The *all* in our example represents that all the event IDs need to be considered while monitoring.

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

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

Note:

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

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

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

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

<table>
<tr><td></td><td colspan="3">7. USEWMI - The eG agent can either use WMI to extract event log statistics or directly parse the event logs using event log APIs. If the USEWMI flag is YES, then WMI is used. If not, the event log APIs are used. This option is provided because on some Windows 2000 systems (especially ones with service pack 3 or lower), the use of WMI access to event logs can cause the CPU usage of the WinMgmt process to shoot up. On such systems, set the USEWMI parameter value to NO.
8. 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.
9. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the FILTER configured</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Errors:
This refers to the number of AD error events that were generated.</td><td>Number</td><td>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.</td></tr>
<tr><td>Information count:
This refers to the number of information events generated when the test was last executed.</td><td>Number</td><td>A change in the value of this measure may indicate infrequent but successful operations performed by the AD server.
The detailed diagnosis capability, if enabled, lists the description of specific events.</td></tr>
</table>

	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 generated when the test was last executed.	Number	This measure is applicable only for Windows 2008/Windows 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.

1.2.6 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.

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

Purpose	To monitor the interactions between clients and the AD server over LDAP, and to promptly capture slowdowns in LDAP searches and binds
Target of the test	An Active Directory or Domain Controller on Windows 2008
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD -** How often should the test be executed 2. **HOST -** The IP address of the machine where the Active Directory is installed. 3. **PORT –** The port number through which the Active Directory communicates. The default port number is 389.		
Outputs of the test	One set of results for every Active Directory being monitored		
Measurements made by the test	**Measurement**	**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 bind.	Secs	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 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 per second.	Binds/Sec	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. A high value is desired for this measure. A very low value could indicate network problems.

1.2.7 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.

Purpose	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)
Target of the test	A VMware Horizon Connection Server
Agent deploying the test	An internal agent
Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT –** Refers to the port used by VMware Horizon Connection Server. The default port number is NULL. 4. **VIEW INSTALL DIR** - Indicate the full path to the install directory of the VMware Horizon Connection Server server.
Outputs of the test	One set of results for the VMware Horizon Connection Server server being monitored

<table>
<tr><th>Measurements made by the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td rowspan="4"></td><td>Collision entry references found:

Indicates the number of collision references currently found in the ADAM database.</td><td>Number</td><td rowspan="2">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 upgrade while LDAP replication is inoperative.

When colliding entries exist in the LDAP directory (ADAM database), identify what those entries are and resolve the collision.</td></tr>
<tr><td>Collision entries found:

Indicates the number of collision entries currently found in the ADAM database.</td><td>Number</td></tr>
<tr><td>Deleted entry references found:

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:

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 Values while indicating whether/not collision references were found in the LDAP directory. However, in the graph of this measure, the same will be indicates using the corresponding numeric equivalents of the states as mentioned in the table above.</td></tr>
</table>

1.3 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 Connection Server server

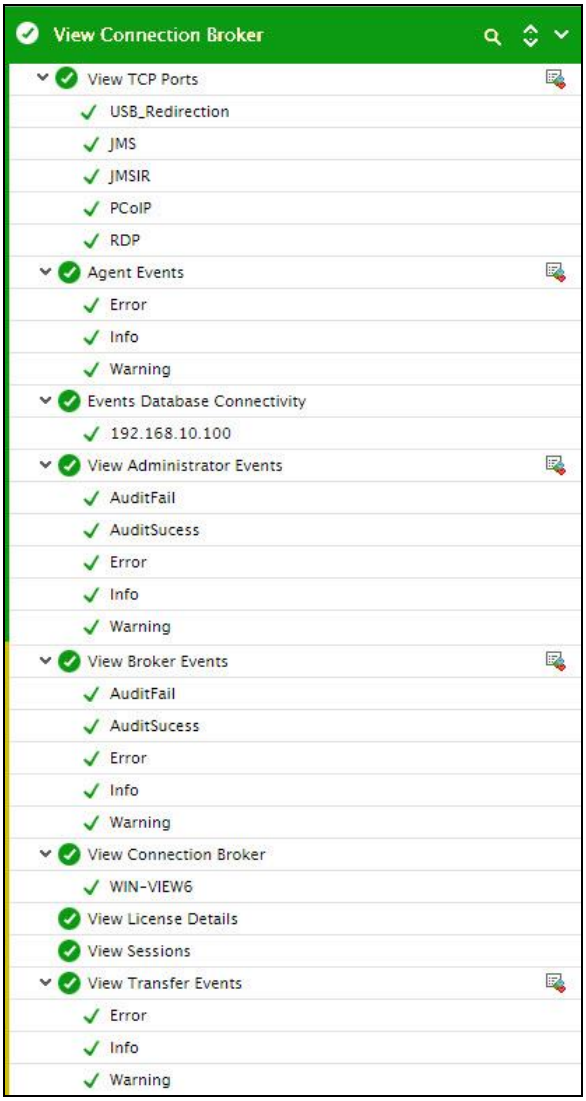

Figure 1.5: The tests mapped to the View Connection Broker layer

1.3.1 View TCP Ports Test

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

Purpose	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)		
Target of the test	A VMware Horizon Connection Server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT –** Refers to the port used by VMware Horizon Connection Server. The default port number is NULL. 4. **TARGETS** - Specify either a comma-separated list of port numbers that are to be tested (eg., 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.		
Outputs of the test	One set of results for each **TARGET** configured for monitoring		
Measurements made by the test	**Measurement**	**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.	Secs	An increase in response time can be caused by several factors such as a server bottleneck, a configuration problem with the DNS server, a network problem, etc.

1.3.2 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.

Purpose	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

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 Connection Server. The default port number is NULL. 4. **DATABASETYPE** - Specify the type of the database in the **DATABASETYPE** text box. By default, the **DATABASETYPE** is MSSql. 5. **DATABASESERVER** - Specify the IP address of the database server that holds the VMware Horizon Connection Server event database. 6. **DATABASEPORT** - Specify the port of the database server. 7. **INSTANCE** - Specify the instance name of the VMware Horizon Connection Server event database. By default, this is set to *none*. 8. **EVENTSDATABASENAME** - Specify the name of the database that holds the VMware Horizon Connection Server events. 9. **EVENTSTABLENAME** - Specify the name of the table containing the VMware Horizon Connection Server events in the VMware Horizon Connection Server events database. 10. **USER** and **PASSWORD** - Provide the credentials of the user who has the authorization to execute queries on the Events Database. 11. **CONFIRM PASSWORD** - Confirm the password by retyping it in the **CONFIRM PASSWORD** text box. 12. **DOMAIN** - Specify the name of the domain in the **DOMAIN** text box. 13. **SSL** - By default, the **SSL** flag is set to **No**. If the MSSql server that is hosting the Events Database is SSL-enabled, set this flag to **Yes**. 14. **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**. 15. **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**. 16. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against **DD FREQUENCY**.

	17. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG 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.		
Outputs of the test	One set of results for the VMware Horizon Connection Server server being monitored		
Measurements made by the test	**Measurement**	**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 of other events in the database.	Number	For complete details of the other events, use the detailed diagnosis of this measure.

1.3.3 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.

Purpose	Reports the current status of the connection broker		
Target of the test	A VMware Horizon Connection Server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT –** Refers to the port used by VMware Horizon Connection Server. The default port number is NULL. 4. **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.		
Outputs of the test	One set of results for the VMware Horizon Connection Server server being monitored		
Measurements	**Measurement**	**Measurement Unit**	**Interpretation**

made by the test	**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 values that correspond to the above-mentioned states are as follows: **State** / **Numeric Value** Enabled: 1 Disabled: 0 **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.

1.3.4 Horizon Connection Server Licensing Usage Test

By tracking the number and type of sessions to the VMware Horizon Connection Server connection broker, administrators can not only understand the load on their VMware Horizon Connection Server server, but can also determine how their VMware Horizon Connection Server licenses are being utilized. Such useful insights on load and license usage are provided by the **Horizon Connection Server Licensing Usage** test. This test reports the total number of sessions on the VMware Horizon Connection Server 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.

Purpose	Reports the total number of sessions on the VMware Horizon Connection Server 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

<table>
<tr><td>Agent deploying the test</td><td colspan="3">An internal agent</td></tr>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The host for which the test is to be configured
3. PORT – Refers to the port used by VMware Horizon Connection Server. The default port number is NULL.
4. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the VMware Horizon Connection Server server being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>All sessions:
The number of View sessions currently active.</td><td>Number</td><td>This is a good indicator of the current session load on View.</td></tr>
<tr><td>Checkedout VM sessions:
Indicates the current number of sessions in which VMs are checked out for use as local desktops.</td><td>Number</td><td>This measure will not be available from VMware Horizon Connection Server 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?</td></tr>
<tr><td>Full VM sessions:
Indicates the current number of active full VM sessions.</td><td>Number</td><td></td></tr>
</table>

	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?
	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 *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 sessions: Indicates the highest recorded number of concurrent application sessions.	Number	If the value of the *Highest all sessions* measure is abnormally 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	

<table>
<tr>
<td></td>
<td>Expiry Date (Days):

Indicates the number of days left for the VMware Horizon Connection Server license to expire.</td>
<td>Number</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>Local desktop enabled:

Indicates whether the local mode license is enabled or not.</td>
<td>Number</td>
<td>This measure will not be available from VMware Horizon Connection Server 6.0 onwards, as the 'Local Mode' feature has been deprecated from this version.

The idea behind Local Mode is to let VMware Horizon Connection Server 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 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>
</table>

	View composer enabled: Indicates whether the View Composer license is enabled or not..	Number	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: **State** / **Numeric Value** Enabled: 1 Disabled: 0 **Note:** By default, this measure reports the above-mentioned states while indicating the status of the View 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.

1.3.5 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.

Purpose	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

<table>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The host for which the test is to be configured
3. PORT – Refers to the port used by VMware Horizon Connection Server. The default port number is NULL.
4. DATABASETYPE - Specify the type of the database in the DATABASETYPE text box. By default, the DATABASETYPE is MSSql.
5. DATABASESERVER - Specify the IP address of the database server that holds the VMware Horizon Connection Server event database.
6. DATABASEPORT - Specify the port of the database server.
7. INSTANCE - Specify the instance name of the VMware Horizon Connection Server event database. By default, this is set to none.
8. EVENTSDATABASENAME - Specify the name of the database that holds the VMware Horizon Connection Server events.
9. EVENTSTABLENAME - Specify the name of the table containing the VMware Horizon Connection Server events in the VMware Horizon Connection Server events database.
10. USER and PASSWORD - Provide the credentials of the user who has the authorization to execute queries on the Events Database.
11. CONFIRM PASSWORD - Confirm the password by retyping it in the CONFIRM PASSWORD text box.
12. DOMAIN - Specify the name of the domain in the DOMAIN text box.
13. SSL - By default, the SSL flag is set to No. If the MSSql server that is hosting the Events Database is SSL-enabled, set this flag to Yes.
14. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the VMware Horizon Connection Server server being monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Total transfer events:
Indicates the total number of transfer events recorded in the events database.</td><td>Number</td><td>The detailed diagnosis of this measure shows the details of the transfer events.</td></tr>
</table>

1.3.6 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 Connection Server manager sees the clients that it needs to facilitate. The agent updates the VMware Horizon Connection Server 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 View server, promptly detect breaks in connection, and fix it before users notice and complain.

Purpose	Periodically monitors the View Agent's connectivity with the View 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		
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 Connection Server. The default port number is NULL. 4. **VIEW INSTALL DIR** - Indicate the full path to the install directory of the VMware Horizon Connection Server server.		
Outputs of the test	One set of results for the VMware Horizon Connection Server server being monitored		
Measurements made by the test	**Measurement**	**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.

1.4 The Desktop Pools Layer

In VMware Horizon Connection Server 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 Virtualisation 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.

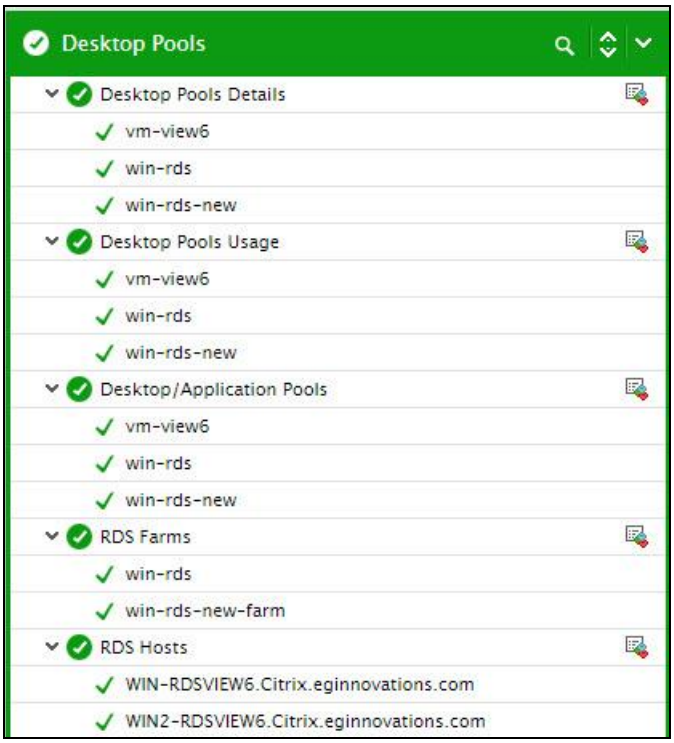

Figure 1.6: The test mapped to the Desktop Pools layer

1.4.1 Desktop Pools Details Test

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

Purpose	Reports the current status of the connection broker
Target of the	A VMware Horizon Connection Server

test	
Agent deploying the test	An internal agent
Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT –** Refers to the port used by VMware Horizon Connection Server. The default port number is NULL. 4. **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.
Outputs of the test	One set of results for each desktop pool configured on the VMware Horizon Connection Server server being monitored

<table>
<tr><th>Measurements made by the test</th><th>Measurement</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td rowspan="2"></td><td>Is pool enabled?:
Indicates whether this desktop pool is enabled or not.</td><td></td><td>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>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>Is pool entitled?
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>
</table>

	Total entitled users in pool: Indicates the total number of entitled users presents in this pool.	Number	The detailed diagnosis of this measure displays the details of entitled users present in this desktop pool.
	Local sessions: Indicates the total number of users present in the local session of this desktop pool.	Number	The details of users present in the local sessions can be viewed in the detailed diagnosis.
	Remote sessions: Indicates the total number of users present in the remote session of this desktop pool.	Number	The details of users 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.

1.4.2 Desktop Pools Usage Test

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

Purpose	Reports the number and status of desktops in each desktop pool configured on the VMware Horizon Connection Server server
Target of the test	A VMware Horizon Connection Server
Agent deploying the test	An internal agent

Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT –** Refers to the port used by VMware Horizon Connection Server. The default port number is NULL. 4. **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.		
Outputs of the test	One set of results for the VMware Horizon Connection Server server being monitored		
Measurements made by the test	**Measurement**	**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.

1.4.3 Desktop/Application Pools Test

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

server.

Purpose	Monitors the status and usage of each desktop pool configured on a VMware Horizon Connection Server server		
Target of the test	A VMware Horizon Connection Server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT –** Refers to the port used by VMware Horizon Connection Server. The default port number is NULL. 4. **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**. 5. **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**. 6. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively 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.		
Outputs of the test	One set of results for each desktop pool configured on the VMware Horizon Connection Server server being monitored		
Measurements	**Measurement**	**Measurement Unit**	**Interpretation**

made by the test	**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** / **Numeric Value** Enabled: 1 Disabled: 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 equivalents of the states as mentioned in the table above.

<table>
<tr>
<td></td>
<td>Pool type:

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 with desktop sessions on RDS hosts. Multiple users can have desktop sessions on an RDS host simultaneously.</td><td>1</td></tr>
<tr><td>Automated Desktop Pool</td><td>Automated desktop pools use a vCenter Server virtual machine template or snapshot to create a pool of identical virtual machines.</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>
</table>

	Is pool entitled? Indicates whether any users or groups have been entitled to access this pool or not.		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: **State** / **Numeric Value** Entitled: 1 UnEntitled: 0 **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.
	Total entitled users in pool: Indicates the total number of entitled users present in this pool.	Number	The detailed diagnosis of this measure 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 that are in active sessions and have active remote connections to a View client.	Number	
	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 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 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	
	Minimum desktops: Indicates the minimum number of desktops to be maintained in this pool.	Number	

1.4.4 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.

Purpose	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

<table>
<tr><td>Configurable parameters for the test</td><td colspan="3">1. TEST PERIOD – How often should the test be executed
2. HOST – The host for which the test is to be configured
3. PORT – Refers to the port used by VMware Horizon 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. 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 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.
6. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.
The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
• The eG manager license should allow the detailed diagnosis capability
• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each RDS farm managed by the VMware Horizon Connection Server server being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>RDS hosts:
Indicates the number of RDS hosts in this farm.</td><td>Number</td><td></td></tr>
<tr><td>Application pools:
Indicates the number of application pools in this farm.</td><td>Number</td><td>Application pools let you deliver applications to many users. The applications in application pools run on a farm of RDS hosts.</td></tr>
<tr><td>Local sessions:
Indicates the number of local sessions to desktops/applications in this farm.</td><td>Number</td><td></td></tr>
</table>

	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.

<table>
<tr>
<td></td>
<td>Is enabled?
Indicates whether/not this farm is enabled.</td>
<td></td>
<td>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:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the status of a farm. However, in the graph of this measure, the same will be represented using the corresponding numeric equivalents only.</td>
</tr>
<tr>
<td></td>
<td>Maximum connections:
Indicates the maximum number of connections that can be established with this farm.</td>
<td>Number</td>
<td>Periodically, it would be good practice to compare the sum of the Local sessions and Remote sessions measures of a farm with the value of this measure. This comparison is sure to reveal whether the farm can accept additional connection requests, or is about to exhaust the allocated connections. In such a case, you may want to choose between the following corrective measures:
• Identify and terminate all idle connections, so as to make room for newer connection requests;
• Increase the maximum number of connections that the farm can support</td>
</tr>
</table>

1.4.5 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 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.

Purpose	To know what type of sessions are active on each RDS host in a farm and to determine the status of desktops/applications on each host		
Target of the test	A VMware Horizon Connection Server		
Agent deploying the test	An internal agent		
Configurable parameters for the test	1. **TEST PERIOD** – How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT –** Refers to the port used by VMware Horizon 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.		
Outputs of the test	One set of results for each RDS host managed by the VMware Horizon Connection Server server being monitored		
Measurements made by the test	**Measurement**	**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 farm.	Number	

	Connected desktops: Indicates the number of desktops on this host that are in active sessions and have active remote connections to a View client.	Number	
	Disconnected desktops: Indicates the number of desktops on this host 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 on this host that are in active sessions and have active remote connections to a View client.	Number	
	Disconnected applications: Indicates the number of applications on this host 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 host is enabled.		This measure a value *Yes* if the host is enabled and *No*, if otherwise. The numeric values that correspond to the above-mentioned states are as follows: **Measure Value** / **Numeric Value** Yes — 1 No — 0 **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating whether/not a host is enabled. However, in the graph of this measure, the same will be represented using the corresponding numeric equivalents only.

<table>
<tr>
<td></td>
<td>Maximum connections:

Indicates the maximum number of connections that can be established with this host.</td>
<td>Number</td>
<td>Periodically, it would be good practice to compare the sum of the Local sessions and Remote sessions measures of an RDS host with the value of this measure. This comparison is sure to reveal whether the host can accept additional connection requests, or is about to exhaust the allocated connections. In such a case, you may want to choose between the following corrective measures:

• Identify and terminate all idle connections, so as to make room for newer connection requests;

• Increase the maximum number of connections that the host can support</td>
</tr>
<tr>
<td></td>
<td>Status:

Indicates whether/not this host is available.</td>
<td></td>
<td>The values that this measure can report and their corresponding numeric values are listed in the table below:

<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Available</td><td>100</td></tr>
<tr><td>Agent unreachable</td><td>0</td></tr>
</table>

Note:

By default, this measure reports the above-mentioned Measure Values to indicate the availability of a host. However, in the graph of this measure, the same will be represented using the corresponding numeric equivalents only.</td>
</tr>
</table>

2

Conclusion

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

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