Monitoring VMware Horizon Security Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

CHAPTER 1: INTRODUCTION 3

CHAPTER 2: HOW TO MONITOR VMWARE HORIZON SECURITY SERVER USING EG ENTERPRISE? 6

2.1 Managing the VMware Horizon Security Server 6

CHAPTER 3: MONITORING THE VMWARE HORIZON SECURITY SERVER 8

3.1 The Security Server Layer 9

3.1.1 Connection Server Details Test 9

3.1.2 Session details Test 10

ABOUT EG INNOVATIONS 15

Table of Figures

Figure 1.1: VMware Horizon Security Servers in a DMZ deployment 4
Figure 2.1: Adding a VMware Horizon Security Server for monitoring 7
Figure 3.1: The layer model of the VMware Horizon Security Server 8
Figure 3.2: The test mapped to the Security Server layer 9

Chapter 1: Introduction

A security server is an instance of Horizon View Connection Server that adds an additional layer of security between the internet and the internal network. A security server resides within a DMZ and acts as a proxy host for connections inside your trusted network. Each security server is paired with an instance of View Connection Server and forwards all traffic to that instance. The following example clearly illustrates how a Horizon View Security Server is deployed in an infrastructure.

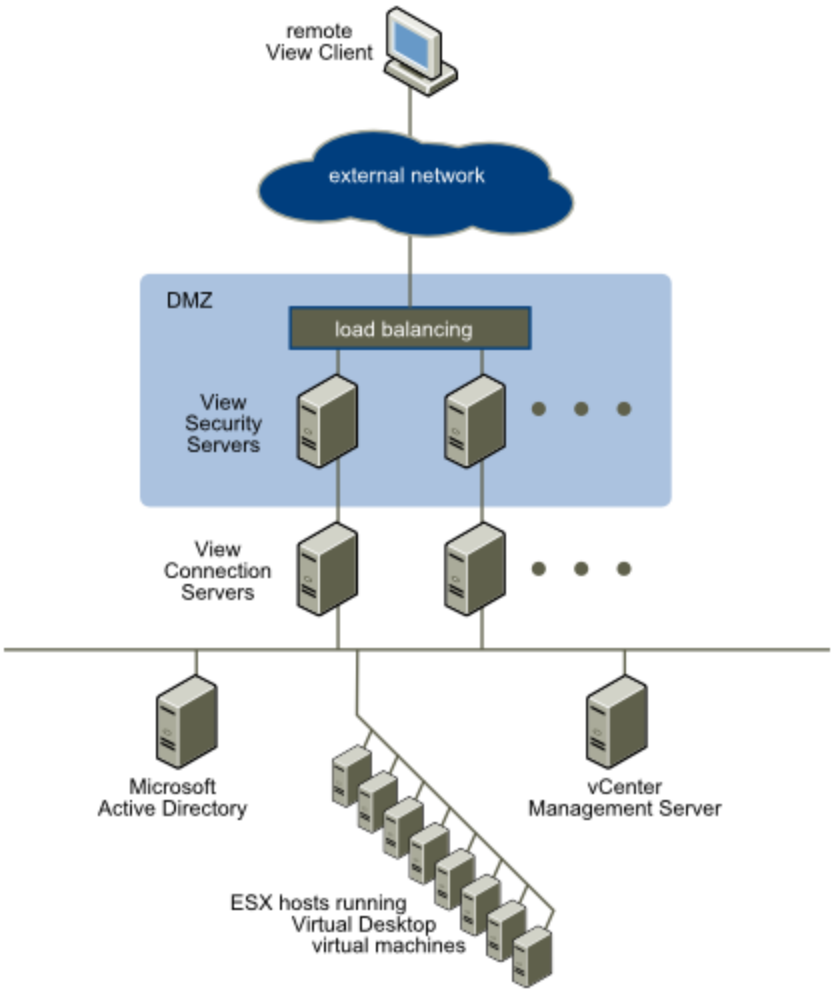

Figure 1.1: VMware Horizon Security Servers in a DMZ deployment

When remote users connect to a security server, they must successfully authenticate before they can access View desktops. With appropriate firewall rules on both sides of the DMZ, the topology shown in Figure 1 is suitable for accessing View desktops from client devices located on the Internet. If more than one Security servers are used, then a hardware or software load balancing solution should be installed. In large environments where a considerable number of users authenticate via the VMware Horizon Security Server to access the View desktops provisioned through the VMware Horizon Connection Server, it is essential for the administrators to check the availability of the VMware Horizon Connection Server and figure out the time taken by the Connection Server to provision the View desktops. It is also essential for the administrators to keep tab on the load on the Security Server. Therefore, it is necessary to monitor the load on the VMware Horizon Security Server round the clock. In the forthcoming chapters, let us discuss on how too monitor the VMWare Horizon Security Server in detail.

Chapter 2: How to Monitor VMware Horizon Security Server Using eG Enterprise?

To monitor the VMware Horizon Security Server, eG Enterprise employs an agent-based approach. The broad steps for monitoring the server using this approach are as follows:

1. Deploy an eG agent on the taget host that is to be monitored. Use the installation procedure detailed in the *eG Installation Guide* to install the eG agent.
2. Manage the target VMware Horizon Security Server using eG administrative interface. See Section **2.1**
3. Finally, start the eG agent. To know how the start the eG agent, refer to the *eG Installation Guide*.

2.1 Managing the VMware Horizon Security Server

To manage a target VMware Horizon Security Server using eG Enterprise, do the following:

1. Login to the eG administrative interface.
2. Invoke the Admin tile menu and select the Add/Modify option from the Components menu of the Infrastructure tile.
3. Then, select the *VMware Horizon Security Server* as the **Component type** and click the **Add New Component** button. Figure 2.1 will then appear.

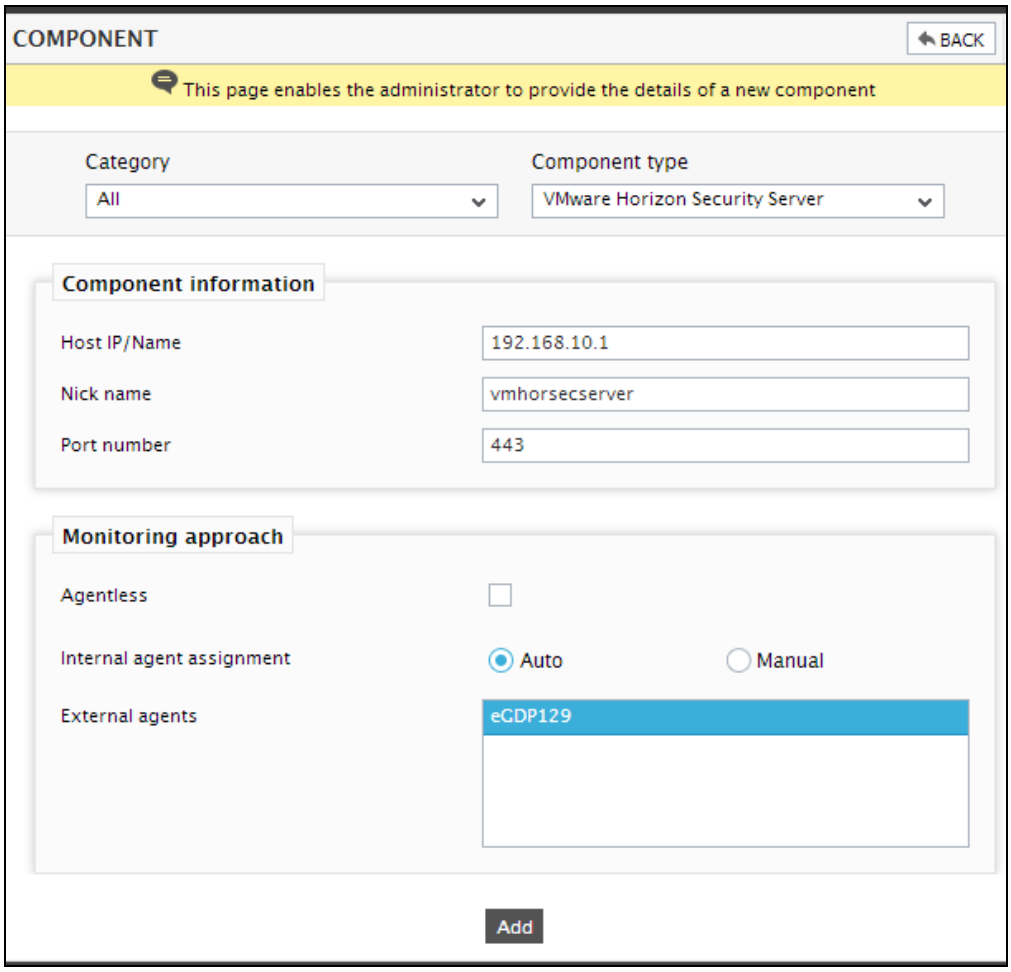

Figure 2.1: Adding a VMware Horizon Security Server for monitoring

4. In Figure 2.1, provide the **Host IP/Name** of the VMware Horizon Security Server to be monitored. Then, provide a **Nick name** for the server.
5. The **Port number** will be set as 443 by default. If the server is listening on a different port in your environment, then override this default setting.
6. Finally, click the **Add** button to add the server for monitoring.

Chapter 3: Monitoring the VMware Horizon Security Server

eG Enterprise offers a specialized monitoring model to monitor the VMware Horizon Security Server which periodically evaluates the service levels achieved by the VMware Horizon Security Server , and proactively alerts administrators to potential performance troubles.

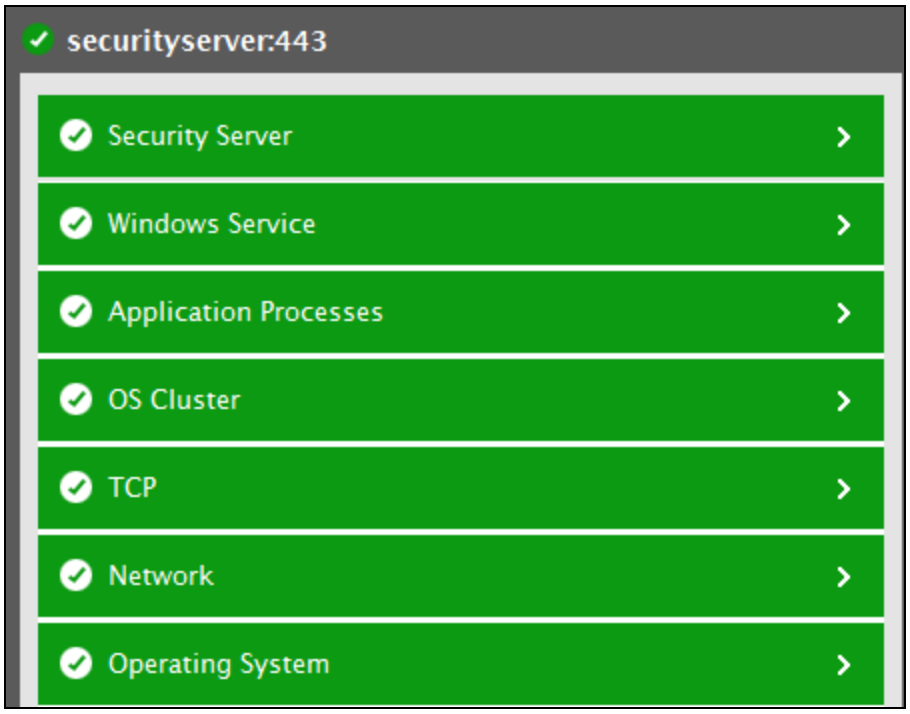

Figure 3.1: The layer model of the VMware Horizon Security Server

Each layer of Figure 3.1 is mapped to a variety of tests that provide valuable insights into the overall performance of the VMware Horizon Security Server. 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 when accessed remotely via the VMware Horizon Security Server?
- How long does it take to access the desktops provisioned by the VMware Horizon Connection Server when accessed remotely via the VMware Horizon Security Server?
- How many view sessions were initiated through the VMware Horizon Security server?
- How many PCoIP and gateway sessions initiated through the VMware Horizon Security Server?
- What is the highest recorded number of concurrent PCoIP gateway sessions, secure gateway sessions, linked clone sessions initiated through the security server?

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

3.1 The Security Server Layer

Using this layer, administrators can determine the availability of the VMware Horizon Connection Server when accessed remotely via the VMware Horizon Security Server. In addition, if the connection server is available, then administrator can figure out the response time of the connection server. Also, the load on the Security server can be monitored at ease!

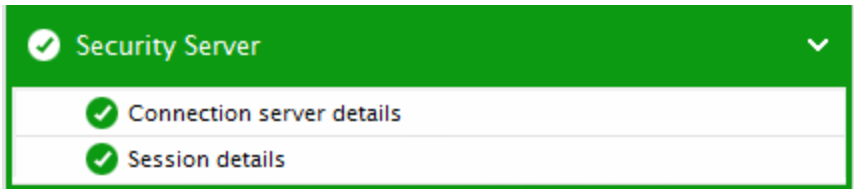

Figure 3.2: The test mapped to the Security Server layer

3.1.1 Connection Server Details Test

This test reports whether/not the VMware Horizon Connection server is available. If available, the test additionally reports the responsiveness of the server.

Target of the test : A VMware Horizon Security Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the target VMware Horizon Security server being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the target VMware Horizon Security server. The default port number is *443*.
Connection Server Port	Specify the port through which the target VMWare Horizon Security server communicates with the VMware Horizon Connection server. By default, this is 4001.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Availability	Indicates whether/not the VMware Horizon Connection server is available.	Percent	The value 100 indicates that the VMware Horizon Connection server is available. The value 0 for this measure indicates that the server is not available.
Response time	Indicates the time taken by the VMware Horizon Connection server to respond to requests from the target VMware Horizon Security server.	Seconds	Ideally, the value of this measure should be low. A high value or a steady increase in the value of this measure is a cause for concern, as it indicates poor responsiveness. This can be caused by factors such as a server bottleneck or a configuration problem.

3.1.2 Session details Test

By tracking the number and type of sessions to the VMware Horizon View Connection Server through the VMware Horizon Security Server, administrators can understand the load on their VMware Horizon Security Server. Such useful insights on load are provided by the **Session details** test.

This test reports the total number of sessions on the VMware Horizon Connection Server through the VMware Horizon Security 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 plan the capacity of the VMware Horizon Connection Server.

Target of the test : A VMware Horizon Security Server

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the target VMware Horizon Security Server being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	Refers to the port used by the target VMware Horizon Security server. The default port number is *443*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
All sessions	The number of View sessions initiated through the security server that are currently active.	Number	This is a good indicator of the current session load on View.
Full VM sessions	Indicates the current number of active full VM sessions that are initiated through the security server.	Number	
Linked clone sessions	Indicates the current number of active linked clone View sessions that are initiated through the security server.	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 initiated through the security server.	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.

Measurement	Description	Measurement Unit	Interpretation
Secure gateway sessions	Indicates the current number of Secure gateway sessions initiated through the security server.	Number	
Sessions from other sources	Indicates the current number of active View sessions that are initiated through the security server from other sources.	Number	
Application sessions	Indicates the current number of active View application sessions that are initiated through the security server.	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 that are initiated through the security server.	Number	
Highest all sessions	Indicates the highest recorded number of concurrent View sessions initiated through the security server.	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 initiated through the security server.	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

Measurement	Description	Measurement Unit	Interpretation
			the most to the erratic usage.
Highest linked clone sessions	Indicates the highest recorded number of concurrent linked-clone sessions initiated through the security server.	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 initiated through the security server.	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 initiated through the security server.	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	Number	

Measurement	Description	Measurement Unit	Interpretation
	recorded number of concurrent desktop sessions initiated through the security server.		

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.