Monitoring Horizon Unified Access Gateway

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The VMware Unified Access Gateway (formerly called Access Point) is a platform that provides secure edge services and access to defined resources that reside in the internal network. This allows authorized, external users to access internally located resources in a secure manner.

- Unified Access Gateway can be used for multiple use cases including:
- Remote access to VMware Horizon 7 desktop and applications.
- Reverse proxying of web servers.
- Access to on-premises legacy applications that use Kerberos or header-based authentication with identity bridging from SAML or certificates.
- Provision of AirWatch or Workspace ONE Per App Tunnels and Tunnel Proxy to allow mobile applications secure access to internal services.
- Running the VMware Content Gateway service to allow VMware Content Locker access to internal files shares or SharePoint repositories.

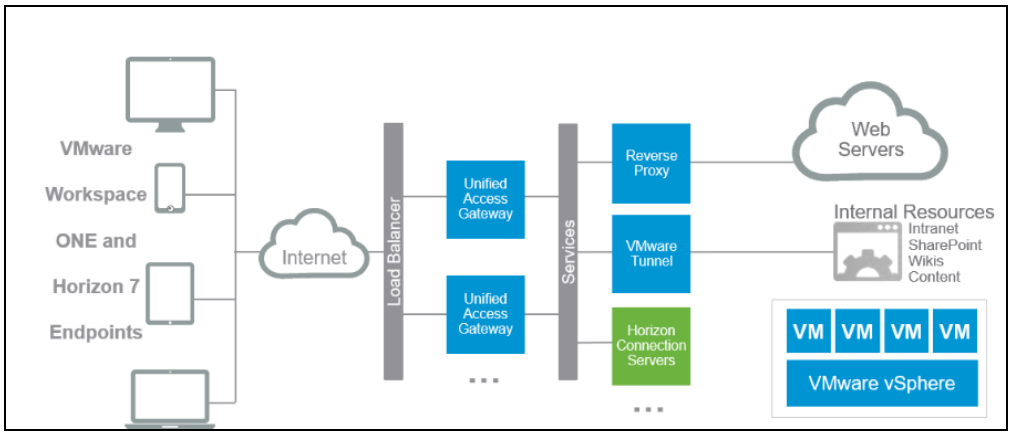

Figure 1.1: How the VMware Unified Access Gateway works

Unified Access Gateway is usually deployed in the DMZ, run on a hardened version of SUSE Linux Enterprise Server 12.

To enhance security options, Unified Access Gateway provides many integration options for authentication, including smart card, certificates, SAML pass-through, RADIUS, and RSA SecurID. The Unified Access Gateway architecture keeps unauthenticated traffic in the DMZ. Traffic is allowed through to the internal network only after authentication has been successful.

Where a Unified Access Gateway is in use, if VMware users complaint that they are unable to access their desktops/applications, administrators should be able to quickly tell what could be causing the inaccessibility. If administrators are not able to promptly detect and rapidly troubleshoot such inaccessibility issues, then unauthenticated users may gain access to critical resources in the internal network. Sometimes, valid users may also be unjustly denied access to resources. Such eventualities can seriously challenge the high security and operational efficiency of the resources in your network. To avoid this, it is imperative that administrators continuously track the status of the gateway and the user sessions on the gateway, proactively detect a potential abnormality, and rapidly initiate measures to avert the anomaly, well before users complain. This is where eG Enterprise helps!

eG Enterprise supports continuous monitoring of the availability and overall status of the VMware Unified Access Gateway and the user sessions on the gateway. In the process, the test quickly detects the inaccessibility of the gateway, reveals the count and type of user sessions that may have been affected by this anomaly, and also points to the probable reasons for the inaccessibility.

This document elaborates on how eG Enterprise monitors the gateway and what metrics it reports.

1.1 How Does eG Enterprise Monitor the Horizon Unified Access Gateway?

eG Enterprise prescribes an *agentless* approach to monitoring the VMware Unified Access Gateway. You can deploy an eG agent on any remote Windows/Linux host in the environment and configure that agent to remotely communicate with and pull metrics from the target gateway appliance. To collect metrics from a gateway appliance, the eG agent makes an HTTP/S connection to the appliance and runs REST API commands on it.

Chapter 2: How to Monitor a Horizon Unified Access Gateway Using eG Enterprise?

The broad steps for monitoring a Horizon Unified Access Gateway are as follows:

- Manage the gateway in the eG admin interface;
- Configure the tests for the managed gateway

Each of these steps have been discussed in detail in the sections that follow.

2.1 Managing a Horizon Unified Access Gateway

A Horizon Unified Access Gateway Appliance can be managed using eG Enterprise in one of the following ways:

- Automatically discover the gateway appliance and then manage the auto-discovered appliance using the eG admin interface, (OR)
- Manually add the appliance using the eG admin interface

2.1.1 Auto-discovering and Managing a Horizon Unified Access Gateway Appliance

eG Enterprise is capable of automatically discovering the Horizon Unified Access Gateway appliance. An eG agent on the VMware Horizon Connection Server can auto-discover the Horizon Unified Access Gateway appliances talking to it. For this, you first need to deploy and start an eG agent on the connection server, and then enable Agent-based discovery . To enable Agent-based discovery, follow the steps below:

1. Login to the eG admin interface as a user who has been assigned the Admin role.
2. Invoke the Admin tile menu and follow the Infrastructure -> Component -> Discovery menu sequence.
3. Then, follow the Agent Discovery -> Actions -> Enable/Disable node sequence in the tree-structure in the left panel of Figure 2.1.

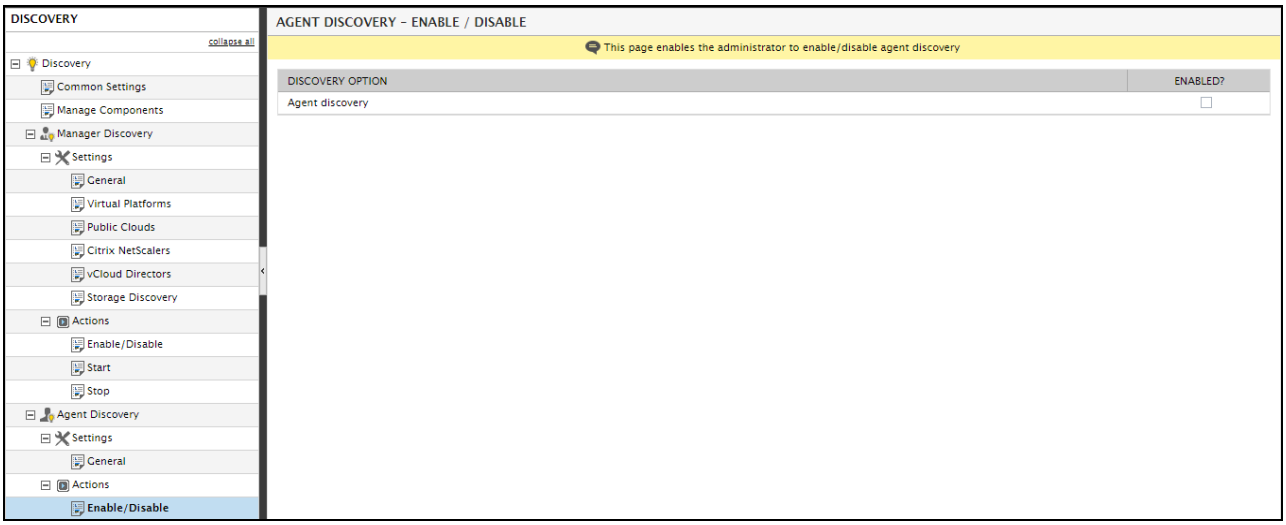

Figure 2.1: Enabling agent-based discovery

4. Select the **ENABLED?** check box in the right panel (see Figure 2.1).
5. A message box depicted by Figure 2.2 will appear. Click the **Yes** button in Figure 2.2 to enable agent-based discovery.

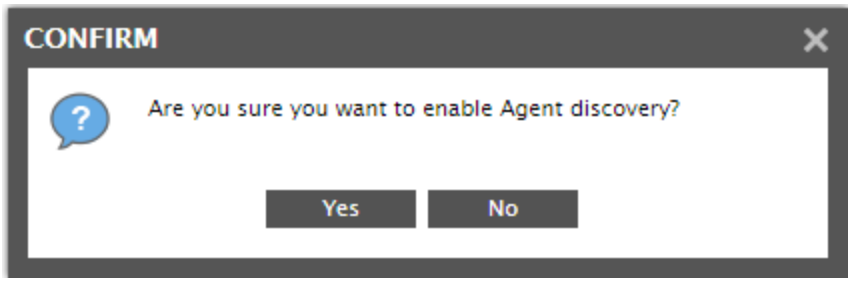

Figure 2.2: A message box prompting you to confirm whether/not you want to enable agent-based discovery

6. Then, follow the Agent Discovery -> Settings -> General node sequence in the tree-structure in the left panel of Figure 2.1. Set the **Discover remote applications** flag in the right panel to **Yes**, and click the **Update** button. This will make sure that the agent on the connection server discovers remote applications/devices - such as the gateway appliance - that interact with it.
7. Once this is done, agent-based discovery will begin. To view the auto-discovered components and manage them, invoke the Admin tile menu and follow the Infrastructure -> Components -> Manage/Unmanage/Delete menu sequence. Figure 2.3 will then appear.

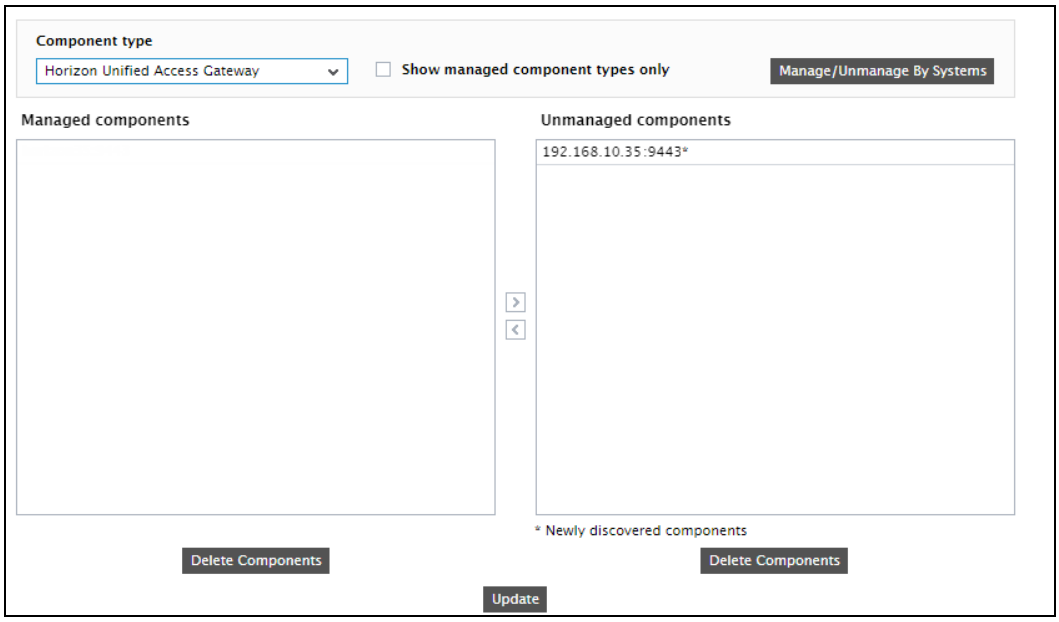

Figure 2.3: Selecting the Horizon Unified Access Gateway

8. Select *Horizon Unified Access Gateway* as the **Component type**. The auto-discovered gateway appliance will then populate the **Unmanaged Components** list of Figure 2.3. To manage a component, select it from the **Unmanaged Components** list, and click the **<** button. Then, click the **Update** button.

9. Once you manage the gateway appliance, proceed to modify its configuration. This is required because, by default, eG Enterprise monitors any component it auto-discovers, in an agent-based manner only. The gateway appliance however, can be monitored only in an agentless manner. To change the monitoring mode of the managed appliance, you need to alter its configuration in eG. For that, first follow the Infrastructure -> Components -> Add/Modify menu sequence in the Admin tile menu. In the page that appears next, select *Horizon Unified Access Gateway* as the **Component type**. The managed gateway appliance will then be displayed therein. Click the button alongside the appliance to edit its configuration. Figure 2.4 will then appear.

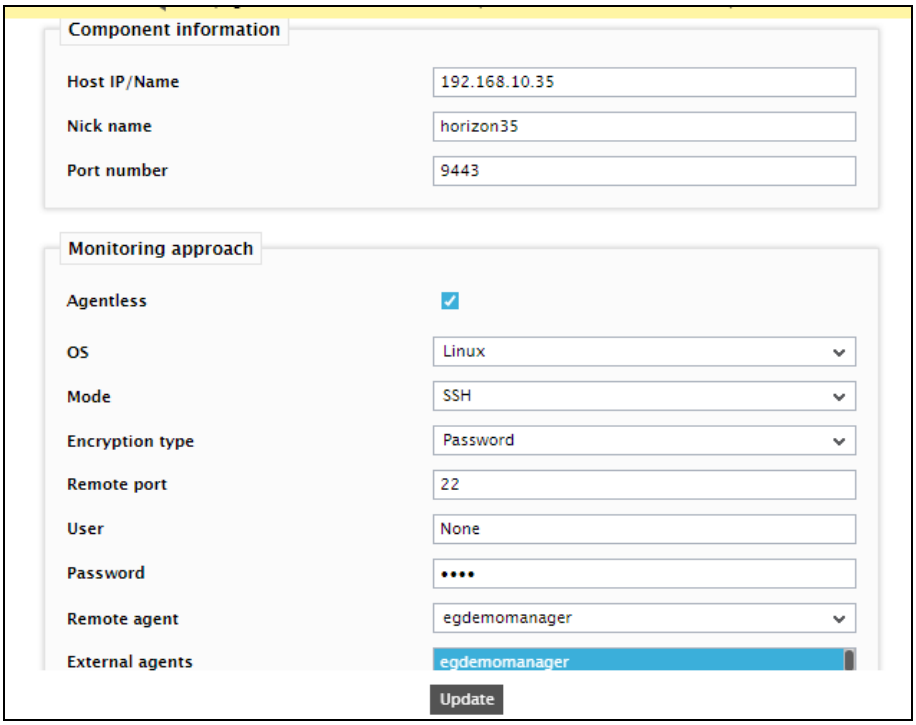

Figure 2.4: Modifying the configuration of the managed gateway appliance

10. Using Figure 2.4, you can change any of the details of the gateway appliance, except its **Host IP/Name**. To change the monitoring approach for the appliance, select the **Agentless** check box in Figure 2.4. Then, select *Linux* as the **OS** and set *SSH* as the **Mode**.

11. Configure the credentials of a *read-only user* of the appliance against **User** and **Password**.

12. Finally, select a **Remote agent** and **External agent** for monitoring the appliance, and click the **Update** button to save the changes.

2.1.2 Manually Adding the Horizon Unified Access Gateway

If for some reason eG Enterprise is unable to automatically discover the access gateway, you can manually add the gateway to the eG Enterprise system for monitoring. To achieve this, follow the steps below:

1. First follow the Infrastructure -> Components -> Add/Modify menu sequence in the Admin tile menu. In the page that appears next, select *Horizon Unified Access Gateway* as the

Component type and click on the **Add New Component** button. Figure 2.5 will then appear.

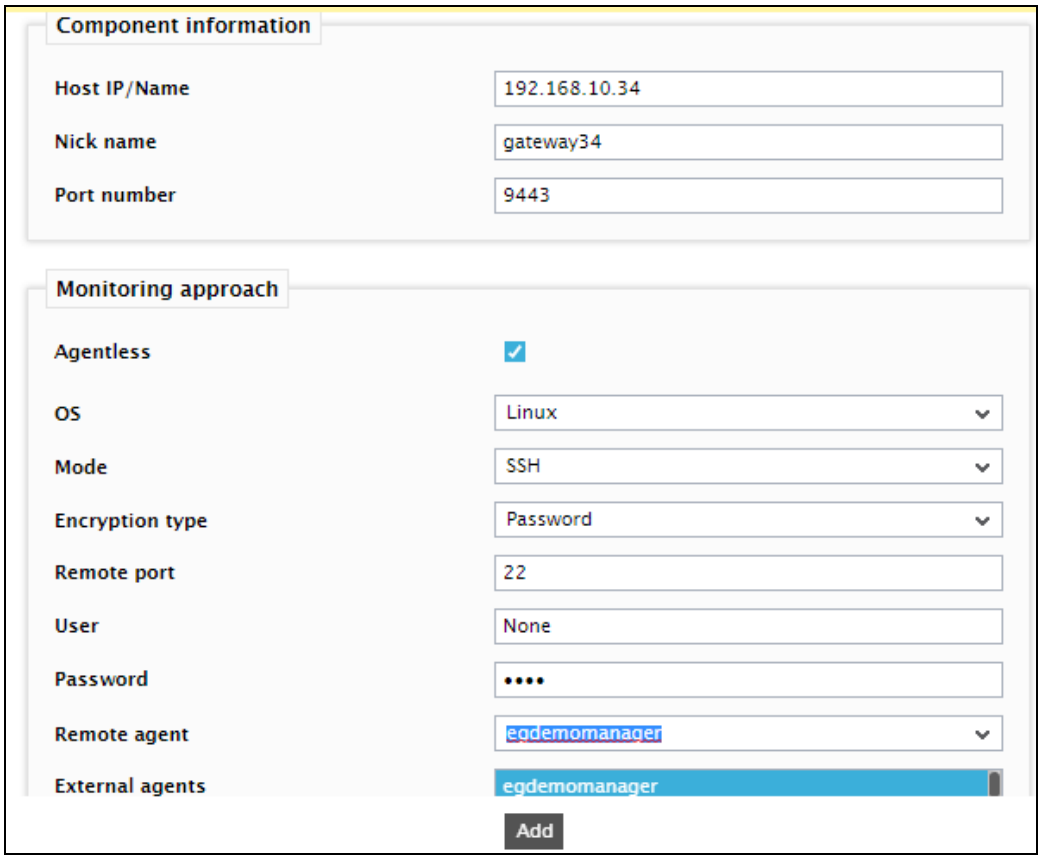

Figure 2.5: Adding a new Horizon Unified Access Gateway appliance

2. In Figure 2.5, provide the **Host IP/Name** of the gateway appliance. Assign a unique **Nick name** to the appliance.
3. Since the gateway appliance is by default monitored in an agentless manner, the **Agentless** check box will be selected by default in Figure 2.5. Select *Linux* as the **OS** and set *SSH* as the **Mode**. Change the SSH **Remote port** (if need be) .
4. Then, against **User** and **Password**, specify the credentials of a *read-only user* of the appliance.
5. Assign a **Remote agent** and **External agent** to the appliance and finally, click **Update** to save the changes.

2.2 Configuring Tests for the Horizon Unified Access Gateway

Once the Horizon Unified Access Gateway appliance is managed, sign out of the eG admin interface. Doing so will bring up the list of tests that have to be manually configured for the gateway

appliance (see Figure 2.6).

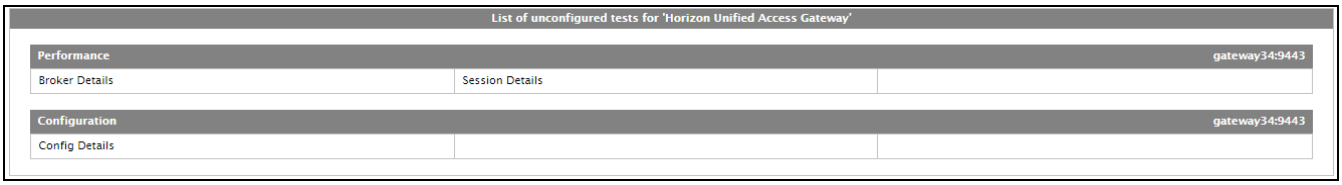

Figure 2.6: List of tests to be configured for the gateway appliance

Click on a Performance test in Figure 2.6 to configure it. For instance, let's say you click on the Broker Details test in Figure 2.6. Figure 2.7 will then appear displaying the parameters that this test takes.

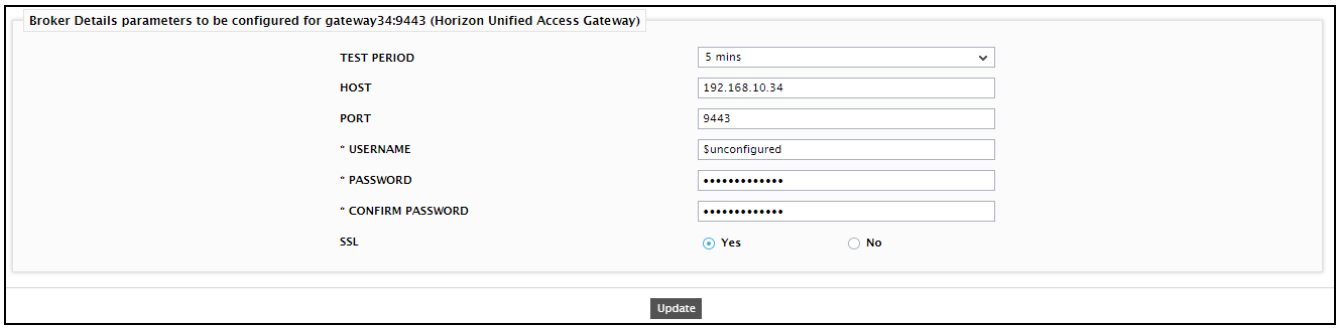

Figure 2.7: Configuring the Broker Details test

To know how to configure the **Broker Details** test, refer to the Section **3.1.1** topic. After configuring the test, click the Update button to save the changes, and then sign out of the admin interface.

Chapter 3: Monitoring the Horizon Unified Access Gateway

To monitor the gateway appliance you have managed, log into the eG user interface as a user with rights to monitor the entire target environment or at least the managed gateway appliance.

eG Enterprise provides a specialized monitoring model for the gateway appliance.

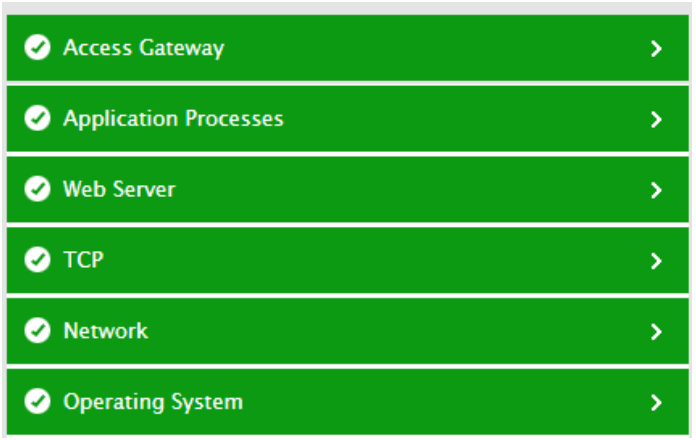

Figure 3.1: Layer model of the Horizon Unified Access Gateway appliance

Each layer of this model is mapped to tests that report a variety of metrics revealing the availability, health, and overall performance of the gateway appliance. Using these metrics, administrators can find quick and accurate answers to the following performance queries:

- Is the gateway appliance accessible and responsive over the network?
- Is the appliance unable to connect to any of the VMware Horizon View Connection servers? If so, which connection server is inaccessible to the appliance?
- Is any connection server responding slowly to the web requests from the appliance, and if so, which one?
- What is the current session load on the appliance?
- Have any logins to the appliance failed?
- Is the backend reachable and running?
- Has any protocol been disabled on the appliance? If so, which ones are disabled - PCoIP? RDP? Blast? UTServer?

The **Access Gateway** topic discusses the tests mapped to and measures reported by the **Access Gateway** layer of Figure 3.1. For details on the **Web Server** layer, refer to the *Monitoring IIS Web*

Servers document. All other layers have been dealt with elaborately in the *Monitoring Unix and Windows Servers* document.

3.1 The Access Gateway Layer

Using the tests mapped to this layer, administrators can periodically check whether the gateway appliance is able to access the connection servers it is associated with. Additionally, the overall session activity on the appliance can be tracked and the status of the different protocols can be determined.

Figure 3.2: The tests mapped to the Access Gateway layer

3.1.1 Broker Details Test

If users complain that they are unable to access their desktops/applications, then administrators should quickly figure out what could have caused the inaccessibility - is it because the gateway appliance itself is unavailable? Or is it because, the appliance is unable to reach the Horizon Connection Server managing those desktops/applications? Using the Broker Details test, administrators can periodically check the availability and responsiveness of every Horizon Connection Server with which the target gateway appliance interacts, accurately isolate the unavailable brokers, and thus figure out if the broker unavailability has contributed to the inaccessibility issues that users are experiencing.

Target of the test : A Horizon Unified Access Gateway

Agent deploying the test: An external agent

Outputs of the test : One set of results for each VMware Horizon Connection server connected to the target Horizon Unified Access Gateway

Configurable parameters for the test

Parameters	Description
Test Period	This indicates how often should the test be executed.

Parameters	Description
Host	The host for which the test is to be configured.
Port	Refers to the port used by the Horizon Unified Access Gateway appliance. By default, this is 9443.
Username, Password, Confirm Password	This test emulates a user accessing the HTTP/S URL of a connection server, and in the process, reports the availability and responsiveness of that server. To establish this connection and report metrics, the test requires *read-only* permissions. Therefore, configure the credentials of a read-only user in the **USERNAME** and **PASSWORD** parameters. Confirm the **PASSWORD** by retyping it in the **CONFIRM PASSWORD** text box.
SSL	By default, the appliance is SSL-enabled. This is why, the SSL flag is set to **Yes** by default. In case the appliance is not SSL-enabled, then set this flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Web availability	Indicates whether/not this connection server responded successfully to the HTTP/S request from the target gateway appliance.	Percent	The value 100 for this measure indicates the availability of the connection server, and the value 0 indicates non-availability. A quick look at the values reported by this measure across connection servers will help you swiftly identify the connection servers that are unavailable and have hence failed to respond to connection requests from the gateway appliance. Availability failures could be caused by several factors such as the connection server process(es) being down, the connection server being misconfigured, a network failure, etc. Temporary unavailability may also occur if the web server is overloaded. Availability is determined based on the response code returned by the server. A response code between 200 to 300 indicates that the server is available.

Measurement	Description	Measurement Unit	Interpretation
Data transfer time	Indicates the time taken for a data transfer between target gateway appliance and this connection server.	Secs	If the value of this measure is unusually high, it could denote a problem.
Content length	The size of the content returned by this connection server.	KB	Typically the content length returned by the server for a specific URL should be the same across time. Any change in this metric may indicate the need for further investigation on the connection server side.
Content validity	This measure validates whether this connection server was successful in executing the request made to it.	Percent	A value of 100% indicates that the content returned by the test is valid. A value of 0% indicates that the content may not be valid. This capability for content validation is especially important. This is because, the gateway may have hit the connection server's URL successfully, but the connection server may reply back with an invalid HTML page, where an error message may have been reported. In this case, the *Web availability* measure will be 100 % (since we got a valid HTML response), but the *Content validity* measure will return the value 0.
Response code	The response code returned by the server for the simulated request.	Number	A value between 200 and 300 indicates a good response. A 4xx value indicates a problem with the requested content (eg., page not found). A 5xx value indicates a server error.
Total response time	Indicates the time taken by this connection server to respond to the requests it receives from the target gateway appliance	Secs	Response time being high denotes a problem. Poor response times may be due to the server being overloaded or misconfigured.
Server response time	This measure indicates the	Secs	While the total response time may

Measurement	Description	Measurement Unit	Interpretation
	time period between when the connection was established with this connection server and when the server sent back a HTTP response header to the monitored gateway appliance.		depend on several factors, the server response time is typically, a very good indicator of a server bottleneck (e.g., because all the available server threads or processes are in use).
TCP connect time	This measure quantifies the time for establishing a TCP connection to this connection server host.	Secs	Typically, the TCP connection establishment time must be very small (of the order of a few milliseconds). Since TCP connection establishment is handled at the OS-level, rather than by the application, an increase in this value signifies a system-level bottleneck on the host that supports the connection server.
TCP connection availability	This measure indicates whether the test managed to establish a TCP connection to this connection server.	Percent	Failure to establish a TCP connection may imply that either the connection server process is not up, or that the process is not operating correctly. In some cases of extreme overload, the failure to establish a TCP connection may be a transient condition. As the load subsides, the server may start functioning properly again.

3.1.2 Session Details Test

If user sessions are unable to access their desktops/applications, and the Broker Details test does not reveal any connectivity issues with the connection server, then administrators need to figure out where else the bottleneck could be - could the gateway appliance itself be unreachable? could sessions be failing at login? or is the protocol used disabled on the appliance? The Session Details test leads you to the source of this bottleneck!

This test tracks user sessions to the gateway appliance and discovers the different type of sessions handled by the appliance, in terms of the protocol used - eg., PCoIP sessions, RDP sessions, Blast sessions etc. The test then reports the status of each session type, thus indicating the types of

sessions that are disabled, unreachable, or not running on the appliance. The test also periodically checks the status of the appliance and reports abnormalities (if any). Using detailed diagnostics, you can even accurately pinpoint the reason for the abnormal status. In addition, the test also tracks session logins and alerts administrators if any login fails. With the help of this test therefore, administrators can quickly determine why user sessions are unable to reach their desktops/applications.

Target of the test : A Horizon Unified Access Gateway

Agent deploying the test: A remote agent

Outputs of the test : One set of results for the target Horizon Unified Access Gateway being monitored.

Configurable parameters for the test

Parameters	Description
Test Period	This indicates 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 Horizon Unified Access Gateway appliance. By default, this is 9443.
Username, Password, Confirm Password	This test emulates a user accessing the HTTP/S URL of a connection server, and in the process, reports the availability and responsiveness of that server. To establish this connection and report metrics, the test requires *read-only* permissions. Therefore, configure the credentials of a read-only user in the **USERNAME** and **PASSWORD** parameters. Confirm the **PASSWORD** by retyping it in the **CONFIRM PASSWORD** text box.
SSL	By default, the appliance is SSL-enabled. This is why, the SSL flag is set to **Yes** by default. In case the appliance is not SSL-enabled, then set this flag to **No**.
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

Parameters	Description
	• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of the monitored gateway appliance.		The values that this measure can report and their corresponding numeric values are detailed in the table below: **Measure Value** / **Numeric Value** Running / 1 Not Running / 2 Partial Running / 3 Disabled / 4 Idle / 5 Not Reachable / 6 **Note:** By default, this measure reports the Measure Values listed in the table above to indicate the current status of the gateway appliance. In the graph of the measure however, the same is indicated using the numeric equivalents only. If this measure reveals that the gateway appliance is in an abnormal state presently, then, you can use the detailed diagnosis of this measure to determine the reason for the abnormal status.
Current sessions	Indicates the current number of sessions on the	Number	The value of this measure includes all protocol sessions.

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>gateway appliance.</td><td></td><td></td></tr>
<tr><td>Authenticated sessions</td><td>Indicates the number of authenticated sessions.</td><td>Number</td><td></td></tr>
<tr><td>High water mark sessions</td><td>Indicates the high water mark of sessions count on the gateway appliance.</td><td>Number</td><td>By tracking the variations to this measure over time, you can figure out the maximum number of sessions the appliance can handle.</td></tr>
<tr><td>Broker status</td><td>Indicates the current status of the VMware Hrizon Connection server connected to the target Access Gatway.</td><td></td><td>The values that this measure can report and their corresponding numeric values are detailed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Running</td><td>1</td></tr><tr><td>Not Running</td><td>2</td></tr><tr><td>Partial Running</td><td>3</td></tr><tr><td>Disabled</td><td>4</td></tr><tr><td>Idle</td><td>5</td></tr><tr><td>Not Reachable</td><td>6</td></tr></table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of the connection broker. In the graph of the measure however, the same is indicated using the numeric equivalents only.
If this measure reveals that the broker is in an abnormal state presently, then, you can use the detailed diagnosis of this measure to determine the reason for this abnormal status.</td></tr>
<tr><td>Success logins</td><td>Indicates the number of logins that were</td><td>Number</td><td>Ideally, the value of this measure should be high.</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>successful.</td><td></td><td></td></tr>
<tr><td>Failed logins</td><td>Indicates the number of logins that failed.</td><td>Number</td><td>Ideally, the value of this measure should be 0.</td></tr>
<tr><td>Backend status</td><td>Indicates the current status of the backend.</td><td></td><td>The values that this measure can report and their corresponding numeric values are detailed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Running</td><td>1</td></tr><tr><td>Not Running</td><td>2</td></tr><tr><td>Partial Running</td><td>3</td></tr><tr><td>Disabled</td><td>4</td></tr><tr><td>Idle</td><td>5</td></tr><tr><td>Not Reachable</td><td>6</td></tr></table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate the current status of the backend. In the graph of the measure however, the same is indicated using the numeric equivalents only.

If this measure reveals that the backend is in an abnormal state presently, then, you can use the detailed diagnosis of this measure to determine the reason for this abnormal status.</td></tr>
<tr><td>Edge service status</td><td>Indicates the current status of the Edge service.</td><td></td><td>The values that this measure can report and their corresponding numeric values are detailed in the table below:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Running</td><td>1</td></tr>
<tr><td>Not Running</td><td>2</td></tr>
<tr><td>Partial Running</td><td>3</td></tr>
<tr><td>Disabled</td><td>4</td></tr>
<tr><td>Idle</td><td>5</td></tr>
<tr><td>Not Reachable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of the backend. In the graph of the measure however, the same is indicated using the numeric equivalents only.
If this measure reveals that the Edge service is in an abnormal state presently, then, you can use the detailed diagnosis of this measure to determine the reason for this abnormal status.
</td></tr>
<tr><td>PCoIP status</td><td>Indicates the current status of the PCoIP protocol.</td><td></td><td>The values that this measure can report and their corresponding numeric values are detailed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Running</td><td>1</td></tr>
<tr><td>Not Running</td><td>2</td></tr>
<tr><td>Partial Running</td><td>3</td></tr>
<tr><td>Disabled</td><td>4</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>Idle</td><td>5</td></tr>
<tr><td>Not Reachable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of the PCoIP protocol. In the graph of the measure however, the same is indicated using the numeric equivalents only.
If this measure reveals that PCoIP protocol is in an abnormal state presently, then, you can use the detailed diagnosis of this measure to determine the reason for this abnormal status.
</td></tr>
<tr><td>PCoIP sessions</td><td>Indicates the current number of PCoIP sessions.</td><td>Number</td><td></td></tr>
<tr><td>Max PCoIP sessions</td><td>Indicates the high watermark of PCoIP sessions.</td><td>Number</td><td></td></tr>
<tr><td>Blast status</td><td>Indicates the current status of the Blast protocol.</td><td></td><td>The values that this measure can report and their corresponding numeric values are detailed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Running</td><td>1</td></tr>
<tr><td>Not Running</td><td>2</td></tr>
<tr><td>Partial Running</td><td>3</td></tr>
<tr><td>Disabled</td><td>4</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>Idle</td><td>5</td></tr>
<tr><td>Not Reachable</td><td>6</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of the Blast protocol. In the graph of the measure however, the same is indicated using the numeric equivalents only.
If this measure reveals that the Blast protocol is in an abnormal state presently, then, you can use the detailed diagnosis of this measure to determine the reason for this abnormal status.
</td></tr>
<tr><td>Blast sessions</td><td>Indicates the current number of Blast sessions.</td><td>Number</td><td></td></tr>
<tr><td>Max Blast sessions</td><td>Indicates the high watermark of Blast sessions.</td><td>Number</td><td></td></tr>
<tr><td>RDP status</td><td>Indicates the current status of the RDP protocol.</td><td></td><td>
The values that this measure can report and their corresponding numeric values are detailed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Running</td><td>1</td></tr>
<tr><td>Not Running</td><td>2</td></tr>
<tr><td>Partial Running</td><td>3</td></tr>
<tr><td>Disabled</td><td>4</td></tr>
<tr><td>Idle</td><td>5</td></tr>
<tr><td>Not Reachable</td><td>6</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>Note:

By default, this measure reports the Measure Values listed in the table above to indicate the current status of the RDP protocol. In the graph of the measure however, the same is indicated using the numeric equivalents only.

If this measure reveals that the RDP protocol is in an abnormal state presently, then, you can use the detailed diagnosis of this measure to determine the reason for this abnormal status.</td></tr>
<tr><td>RDP sessions</td><td>Indicates the current number of RDP sessions.</td><td>Number</td><td></td></tr>
<tr><td>Max RDP sessions</td><td>Indicates the high watermark of RDP sessions.</td><td>Number</td><td></td></tr>
<tr><td>UDP tunnel server status</td><td>Indicates the current status of the Utserver protocol.</td><td></td><td>The values that this measure can report and their corresponding numeric values are detailed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Running</td><td>1</td></tr><tr><td>Not Running</td><td>2</td></tr><tr><td>Partial Running</td><td>3</td></tr><tr><td>Disabled</td><td>4</td></tr><tr><td>Idle</td><td>5</td></tr><tr><td>Not Reachable</td><td>6</td></tr></table>
Note:

By default, this measure reports the</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Measure Values listed in the table above to indicate the current status of the Utserver protocol. In the graph of the measure however, the same is indicated using the numeric equivalents only. If this measure reveals that the Utserver protocol is in an abnormal state presently, then, you can use the detailed diagnosis of this measure to determine the reason for this abnormal status.
UDP tunnel server sessions	Indicates the current number of Utserver sessions.	Number	
Max UDP tunnel server sessions	Indicates the high watermark of Utserver sessions.	Number	

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.