Monitoring Citrix StoreFront

eG Enterprise v6

Restricted Rights Legend

Trademarks

Copyright

Table of Contents

Table of Figures

1

Monitoring Citrix Storefront

Citrix StoreFront, which is the successor to Citrix Web Interface, authenticates users to XenDesktop sites, XenApp farms, App Controller (SaaS Apps), and VDI-in-a-Box enumerating and aggregating available desktops and applications into stores that users access through Citrix Receiver for Android, iOS, Linux, Windows, Win8/RT or Receiver for Web sites. Storefront enables next generation features such as:

- Unified StoreFront for XenApp and XenDesktop resources that can also deliver SaaS & Native Mobile applications (through App Controller).
- Simplified Account Provisioning, which enables users to connect to assigned desktops and applications by simply entering their email or server address, or by opening a Provisioning File in Receiver.
- Access from any Receiver with a consistent user experience, including automatic fallback to Receiver for HTML5 on Receiver for Web sites if a native client isn't available locally and can't be installed.
- Synchronization of resource subscriptions across all platforms and devices (Follow-me Apps & Data).
- Cross-farm aggregation and de-duplication, that aggregates and delivers a unique set of applications from multiple farms across different sites.
- Farm-Based Optimal HDX Connection Routing, which enables the use of the nearest NetScaler Gateway for HDX traffic routing independent of the NetScaler Gateway used for initial authentication.

The architecture of the Citrix Storefront is explained in Figure 1.1.

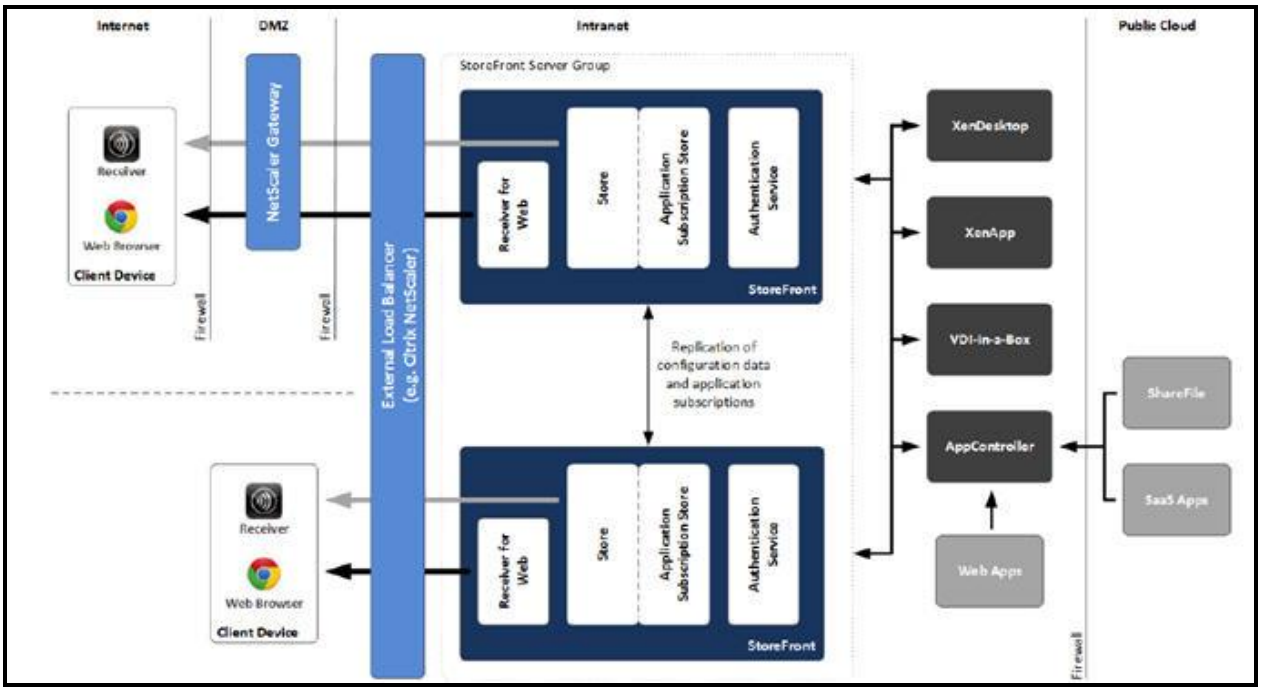

Figure 1.1: The Citrix Storefront architecture

StoreFront consists of the following components:

- **Authentication service:** This service, which is an integral part of StoreFront, authenticates users to XenDesktop sites, XenApp farms, and App Controller (for SaaS apps). The authentication service ensures that users only need to log on to StoreFront/Receiver once.
- **Store:** The store retrieves user credentials from the authentication service to authenticate users to the components providing the resources. The store also enumerates and aggregates the resources currently available from XenDesktop sites, XenApp farms, and App Controller (SaaS Apps). Users access the store through Citrix Receiver or a Receiver for Web site.
- **Application Subscription Store (Data Store):** This store saves and indexes the application or desktop subscriptions of the users on a per-StoreFront Store basis. In contrast to older versions of StoreFront, where an external Microsoft SQL database was required, the new Application Subscription Store uses the built-in Microsoft Windows Extensible Storage Engine to store details of users' app subscriptions locally on StoreFront servers. When joining a StoreFront server to a Server Group the replication of data between all members is configured automatically.
- **Receiver for Web site:** This site enables users to access stores through a webpage. Furthermore, this site can verify the version of Receiver installed locally on the endpoint and guide the user through an upgrade or installation procedure if required. In scenarios where Receiver cannot be locally Receiver for HTML5 can be enabled for the Receiver for Web sites so that users can access resources directly within HTML5-compatible web browsers.
- **Desktop Appliance site:** Desktop Appliance sites provide users of non-domain desktops with an experience similar to that of users with domain-joined desktops. The web browsers on desktop appliances are configured to start in full-screen mode displaying the logon screen for a Desktop Appliance site. When a user logs on to a site, by default, the first desktop (in alphabetical order) available to the user in the store for which the site is configured starts automatically. Desktop Appliance sites are only created by default when StoreFront is installed and configured as part of a XenDesktop installation.
- **XenApp Services site:** Users with older Citrix clients that cannot be upgraded can access stores by configuring their clients with the XenApp Services URL for a store. This site can also be used from domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock.
- **NetScaler Gateway:** Citrix NetScaler Gateway is a physical or virtual appliance, which provides secure remote access to internal resources. The appliance is typically located within the DMZ and exposed to the Internet. When a user connects to NetScaler Gateway they will need to authenticate before any access to internal resources is granted. The access can be controlled by the admin by means of granular application-level policies and action controls.

As already mentioned, the *Citrix Storefront* model of eG Enterprise monitors the health of the storefront and the user authentication.

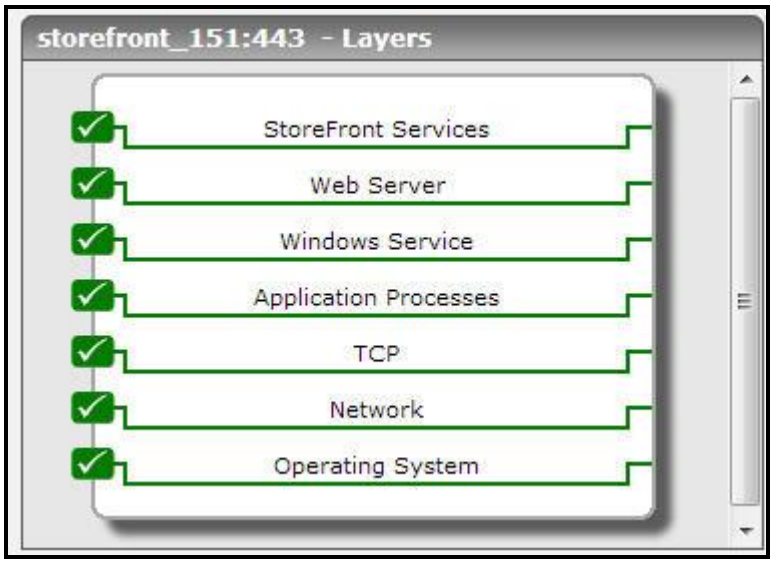

Figure 1.2: The layer model of the Citrix Storefront

Each layer of Figure 1.2 above is mapped to a series of tests that periodically monitors the Citrix Storefront server and checks on the following:

- How well the resources were accessed?
- The time taken to access the resources;
- How well the resources were accessed using the ICA protocol?;
- How well the resources were accessed using the RADE (Rapid Application Delivery) process?;
- The rate at which the users were authenticated based on their chosen language preference;
- The time taken to authenticate the users;
- The rate at which the password change requests from the users were processed?
- The time taken to change the password upon user requests;
- How well the authentication store stores the user information, retrieves the information and deletes the user information?;
- How well the resources and sessions were accessed using the Citrix Dazzle?;
- What is the rate at which the user subscriptions were added, deleted, modified, enabled etc?;
- The time taken to retrieve the user subscriptions from the authentication store;
- How well the users are authenticated to access the controller through the Web Application Delivery service?
- How well the Citrix Storefront is accessed through the XML service?

The **Operating System**, **Network**, **TCP**, **Application Processes**, **Windows Service and Web Server** layers of Citrix XenDesktop Apps are similar to that of a *Windows* server model. Since these tests have been dealt with in the *Monitoring Unix and Windows Servers* document, Section 1.1 focuses on the **Storefront Services** layer.

1.1 The Storefront Services Layer

This layer tracks the rate at which the resources were accessed from the Citrix Sotrefront, the details pertaining to the user subscriptions, the rate at which the users are authenticated based on their language preference, the rate at

which the change password requests from users are processed, the time taken to change the password in the store, the rate at which the applications/resources were accessed through the Citrix Dazzle etc.

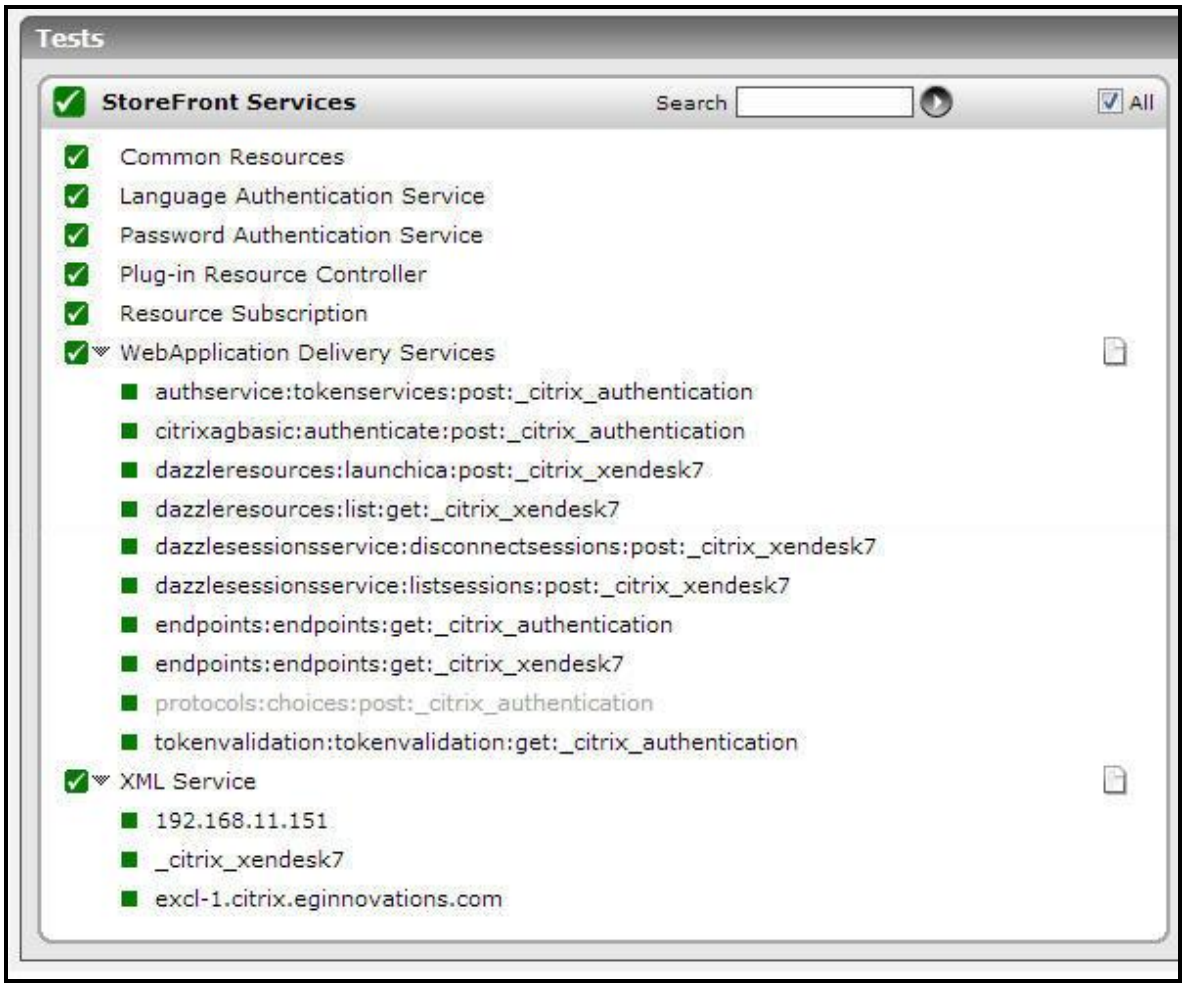

Figure 1.3: The tests mapped to the Storefront Services layer

1.1.1 Common Resources Test

Using this test, you can easily identify the rate at which the resources were accessed from the store, the resources were accessed using ICA protocol and RADE (Rapid Application DElivery) process. In addition, the time taken for accessing the resources using the ICA protocol and the RADE process can also be identified easily.

Purpose	Helps you in identifying the rate at which the resources were accessed from the store, the resources were accessed using ICA protocol and RADE (Rapid Application DElivery) process. In addition, the time taken for accessing the resources using the ICA protocol and the RADE process can also be identified easily.
Target of the test	Citrix Storefront server
Agent deploying the test	An internal/remote 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** – The port number at which the specified HOST listens to. By default, this is 443.		
Outputs of the test	One set of results for the Citrix Storefront server being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	All resources calls: Indicates the rate at which the resources were accessed from the store of this server.	Calls/sec	
	ICA launch calls: Indicates the rate at which the resources were accessed using ICA protocol from the store of this server.	Calls/sec	
	ICA launch average time: Indicates the average time taken to access the resources using the ICA protocol from the store of this server.	Secs	
	Rade launch calls: Indicates the rate at which the resources were accessed using the RADE (Rapid Application Delivery) process from the store of this server.	Calls/sec	
	Rade launch average time: Indicates the average time taken to access the resources using the RADE process from the store of this server.	Secs	

1.1.2 Language Authentication Service Test

In large virtualized environments, at any given point of time, thousands of users from different zones of the world may be trying to access the published applications and virtual desktops. In such a situation, language plays a major role when a user tries to login through the Citrix Receiver. Based on the language preference of the users, the **Language Authentication Service** test helps you to determine the rate at which the users are authenticated and how long it took for the Citrix Storefront to authenticate the users. In addition, this test helps you to identify the rate at which the change password requests have been entertained and the average time taken to change the password.

<table>
<tr><td>Purpose</td><td colspan="3">Helps you to determine the rate at which the users are authenticated and how long it took for the Citrix Storefront to authenticate the users. In addition, this test helps you to identify the rate at which the change password requests have been entertained and the average time taken to change the password.</td></tr>
<tr><td>Target of the test</td><td colspan="3">Citrix Storefront server</td></tr>
<tr><td>Agent deploying the test</td><td colspan="3">An internal/remote 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 – The port number at which the specified HOST listens to. By default, this is 443.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Citrix Storefront 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>Authenticate calls:
Indicates the rate at which users are authenticated by this citrix storefront based on their chosen language preference.</td><td>Calls/sec</td><td>A high value is desired for this measure.</td></tr>
<tr><td>Authenticate average time:
Indicates the average time taken by this citrix storefront server to authenticate the users.</td><td>Secs</td><td>A low value is desired for this measure. A gradual increase in the value of this measure is an indication of the unavailability of the database that is required for authentication or a performance bottleneck.</td></tr>
<tr><td>Change password calls:
Indicates the rate at which the password change request from the users are processed by this citrix storefront server.</td><td>Calls/sec</td><td></td></tr>
<tr><td></td><td>Change password average time:
Indicates the average time taken by this citrix storefront server nto process the password change request from users.</td><td>Secs</td><td></td></tr>
</table>

1.1.3 Password Authentication Service Test

When a user tries to login to access the virtual machines or published applications using their login credentials from the Citrix Receiver, the Citrix Credential Wallet Service of the Citrix Storefront server helps in authenticating the password entered by the user with the password that is already stored in the authentication store. Using the **Password Authentication Service** test, administrators can easily analyze the rate at which the user information is authenticated by the Citrix Wallet Service and the rate at which the user requests are retrieved and serviced to the users. Additionally, you can idetnify how well the user requests are deleted after being serviced by the Citrix Wallet service. This test is a perfect choice for monitoring the user authentication and the load on the virtualized environment!

Purpose	Analyze the rate at which the user information is authenticated by the Citrix Wallet Service and the rate at which the user requests are retrieved and serviced to the users. Additionally, you can identify how well the user requests are deleted after being serviced by the Citrix Wallet service.		
Target of the test	Citrix Storefront server		
Agent deploying the test	An internal/remote 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** – The port number at which the specified **HOST** listens to. By default, this is 443.		
Outputs of the test	One set of results for the Citrix Storefront server that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Store entry calls: Indicates the rate at which the authentication store stores the entry information i.e., the user requests.	Calls/sec	
	Retrieve entry calls: Indicates the rate at which the user information is retrieved from the authentication store by the Citrix Credential Wallet Service upon user requests.	Calls/sec	
	Delete entry calls: Indicates the rate at which the user requests are deleted after the request is serviced by the Citrix Credential Wallet Service.	Calls/sec	

1.1.4 Plug-in Resource Controller Test

Citrix Dazzle is a plug-in for Citrix Receiver that allows users to subscribe to only those available published resources that they choose.

This test helps the administrators to analyze the rate at which the image responses were received for the resources accessed through the citrix dazzle and the rate at which the resources were actually accessed. In addition, you could analyze the session related information of the resources, the whole body calls and the cache calls that were updated upon user requests.

Purpose	Helps the administrators to analyze the rate at which the image response were received for the resources accessed through the citrix dazzle and the rate at which the resources were actually accessed. In addition, you could analyze the session related information of the resources, the whole body calls and the cache calls that were updated upon user requests.		
Target of the test	Citrix Storefront server		
Agent deploying the test	An internal/remote 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** – The port number at which the specified **HOST** listens to. By default, this is 443.		
Outputs of the test	One set of results for the Citrix Storefront server that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Image response whole body calls: Indicates the rate of image responses received for the resources accessed through the citrix dazzle.	Calls/sec	
	List convert resources calls: Indicates the rate at which the resources were accessed through the citrix dazzle.	Calls/sec	
	List sessions whole body calls: Indicates the rate at which the sessions were accessed through the citrix dazzle.	Calls/sec	

	List whole body calls: Indicates the rate of whole body calls through the citrix dazzle.	Calls/sec	
	Update resources image cache calls: Indicates the rate at which the cache calls are updated upon user requests for image resources.	Calls/Sec	

1.1.5 Resource Subscription Test

In order to identify the load on the virtualized environment i.e., to identify the details of the user subscriptions, use the **Resource Subscription** test.

This test helps the administrators to identify the rate at which the user subscriptions are added, disposed, enabled, retrieved, removed, modified etc. Additionally, administrators may get to know the time taken to retrieve the user subscriptions from the store and the time taken to modify the user subsciptions.

Purpose	Helps the administrators to identify the rate at which the user subscriptions are added, disposed, enabled, retrieved, removed, modified etc. Additionally, administrators may get to know the time taken to retrieve the user subscriptions from the store and the time taken to modify the user subsciptions.		
Target of the test	Citrix Storefront server		
Agent deploying the test	An internal/remote 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** – The port number at which the specified **HOST** listens to. By default, this is 443.		
Outputs of the test	One set of results for the Citrix Storefront server that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Add subscriptions calls: Indicates the rate at which the user subscriptions were added to the store of this server.	Calls/sec	
	Dispose calls: Indicates the rate at which the user subscriptions were disposed from the store of this server.	Calls/sec	

	Enabled calls: Indicates the rate at which the user subscriptions were enabled on this server.	Calls/sec	
	Get subscriptions calls: Indicates the rate at which the subscriptions were retrieved from the store of this server.	Calls/sec	
	Get subscriptions average time: Indicates the average time taken to retrieve the user subscriptions from the store.	Secs	
	Remove subscriptions calls: Indicates the rate at which the subscriptions were removed from the store.	Calls/sec	
	Remove subscriptions average time: Indicates the average time taken to remove the subscriptions from the store.	Secs	
	Save changes calls: Indicates the rate at which the changes made to the user subscriptions were saved on the store.	Calls/sec	
	Update subscription calls: Indicates the rate at which the user subscriptions were updated on the store.	Calls/sec	

1.1.6 Web Application Delivery Services Test

The Citrix Self service plugin is used to customize the applications that are frequently used by the users in the Citrix Receiver dashboard, once the users are authenticated on the Citrix Storefront.

This test reports the rate at which the users are authenticated to access the controller while accessing the applications through the Citrix Self service plugin and the time taken for authenticating the users to access the controller.

Purpose	Reports the rate at which the users are authenticated to access the controller while accessing the applications through the Citrix Self service plugin and the time taken for authenticating the users to access the controller.
Target of the	Citrix Storefront server

test			
Agent deploying the test	An internal/remote 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** – The port number at which the specified **HOST** listens to. By default, this is 443.		
Outputs of the test	One set of results for the web application delivery service that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Controller action calls: Indicates the rate at which the users accessing through the Citrix Self service plugin are authenticated to access the controller.	Calls/sec	
	Controller action average time: Indicates the average time taken for authenticating the users accessing the controller through the Citrix Self service plugin.	Secs	

1.1.7 XML Service Test

The XML Service supplies the Citrix Storefront and the users connected through the Citrix Storefront with the name of the applications that are available in the virtual environment.

This test helps you in identifying the rate at which the web interface is accessed through the XML service and the rate at which the errors were generated when there was a glitch in accessing the web interface through the service.

Purpose	Helps you in identifying the rate at which the web interface is accessed through the XML service and the rate at which the errors were generated when there was a glitch in accessing the web interface through the service.
Target of the test	Citrix Storefront server
Agent deploying the test	An internal/remote 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 – The port number at which the specified HOST listens to. By default, this is 443.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Citrix Storefront server being monitored</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>Network traffic calls:
Indicates the rate at which the web interface is accessed through the XML service.</td><td>Calls/sec</td><td></td></tr>
<tr><td>Network traffic error calls:
Indicates the rate at which the errors were generated while the web interface was accessed through the XML service.</td><td>Calls/sec</td><td></td></tr>
</table>

1.1.8 Citrix Delivery Service Log Test

This test periodically scans the Citrix Delivery Service logs for configured patterns of errors/warnings and promptly captures and reports error/warning messages that match the specified patterns.

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: a. *OS_events* is the display name that will appear as a descriptor of the test in the monitor UI; b. *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*. c. 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. d. 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.

e. 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.

f. 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.

g. 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.

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. **STATELESS ALERTS** - Typically, the eG manager generates email alerts only when the state of a specific measurement changes. A state change typically occurs only when the threshold of a measure is violated a configured number of times within a specified time window. While this ensured that the eG manager raised alarms only when the problem was severe enough, in some cases, it may cause one/more problems to go unnoticed, just because they did not result in a state change. For example, take the case of the EventLog test. When this test captures an error event for the very first time, the eG manager will send out a **CRITICAL** email alert with the details of the error event to configured recipients. Now, the next time the test runs, if a different error event is captured, the eG manager will keep the state of the measure as **CRITICAL**, but will not send out the details of this error event to the user; thus, the second issue will remain hidden from the user. To make sure that administrators do not miss/overlook critical issues, the eG Enterprise monitoring solution provides the **stateless alerting** capability. To enable this capability for this test, set the **STATELESS ALERTS** flag to **Yes**. This will ensure that email alerts are generated for this test, regardless of whether or not the state of the measures reported by this test changes.

9. **EVENTS DURING RESTART** - By default, the **EVENTS DURING RESTART** flag is set to **Yes**. This ensures that whenever the agent is stopped and later started, the events that might have occurred during the period of non-availability of the agent are included in the number of events reported by the agent. Setting the flag to **No** ensures that the agent, when restarted, ignores the events that occurred during the time it was not available.

10. **DDFORINFORMATION** – eG Enterprise also provides you with options to restrict the amount of storage required for event log tests. Towards this end, the **DDFORINFORMATION** and **DDFORWARNING** flags have been made available in this page. By default, both these flags are set to **Yes**, indicating that by default, the test generates detailed diagnostic measures for information events and warning events. If you do not want the test to generate and store detailed measures for information events, set the **DDFORINFORMATION** flag to **No**.

11. **DDFORWARNING** – To ensure that the test does not generate and store detailed measures for warning events, set the **DDFORWARNING** flag to **No**.

12. **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**.

<table>
<tr><td></td><td colspan="3">13. 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 FILTER configured</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>Information messages:

This refers to the number of application 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 one or more applications.

Please check the Citrix Delivery Service Logs in the Event Log Viewer for more details.</td></tr>
<tr><td>Warnings:

This refers to the number of warnings that were generated when the test was last executed.</td><td>Number</td><td>A high value of this measure indicates problems with the broker that may not have an immediate impact, but may cause future problems in one or more machines of this broker.

Please check the Citrix Delivery Service Logs in the Event Log Viewer for more details.</td></tr>
<tr><td>Error messages:

This refers to the number of application error events that were generated.</td><td>Number</td><td>A very low value (zero) indicates that the system is in a healthy state and all applications are running smoothly without any potential problems.

An increasing trend or high value indicates the existence of problems like loss of functionality or data in one or more applications.

Please check the Citrix Delivery Service Logs in the Event Log Viewer for more details.</td></tr>
</table>

	Critical messages: Indicates the number of critical events that were generated when the test was last executed.	Number	A critical event is one that an application or a component cannot automatically recover from. This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems. A very low value (zero) indicates that the system is in a healthy state and all applications are running smoothly without any potential problems. An increasing trend or high value indicates the existence of fatal/irrepairable problems in one or more applications. The detailed diagnosis of this measure describes all the critical application events that were generated during the last measurement period. Please check the Citrix Delivery Service Logs in the Event Log Viewer for more details.
	Verbose messages: Indicates the number of verbose events that were generated when the test was last executed.	Number	Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better. This measure is applicable only for Windows 2008/Windows Vista/Windows 7 systems. The detailed diagnosis of this measure describes all the verbose events that were generated during the last measurement period. Please check the Citrix Delivery Service Logs in the Event Log Viewer for more details.

1.1.9 Server Groups Test

StoreFront can be configured either on a single server or as a multiple server deployment where two/more servers are grouped under a server group. Server groups not only provide additional capacity, but also greater availability.

To know the number and names of servers in a server group, use the **Server Groups** test.

Purpose	Reports the number of servers in a server group
Target of the test	Citrix Storefront server
Agent deploying the test	An internal/remote 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 – The port number at which the specified HOST listens to. By default, this is 443.
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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Citrix Storefront 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>Number of servers:
Indicates the number of servers in the server group.</td><td>Number</td><td>Use the detailed diagnosis of this measure to know which servers are part of the server group.</td></tr>
</table>

1.1.10 Server Details Test

In a Storefront server group, configuration information and details of users' application subscriptions are stored on and synchronized between all the servers in that group. This means that if a StoreFront server becomes unavailable for any reason, users can continue to access their stores using the remaining servers. Meanwhile, the configuration and subscription data on the failed server are automatically updated when it reconnects to the server group.

If a server in a group is unable to synchronize its data with other members of the group or is taking too long to do so, Storefront will not be able to deliver on its promise of high availability. Administrators should hence periodically check whether the StoreFront server being monitored is in sync with other servers in that group, and if not, figure out what is causing the non-sync – is it because the server is taking an abnormally long time to synchronize its data with other group members? The **Server Details** test helps administrators find answers to this question! This test promptly captures any data non-sync that may exist between a monitored server and the server group to which it belongs and also reveals if it is owing to latencies in synchronization.

Purpose	Promptly captures any data non-sync that may exist between a monitored server and the server group to which it belongs and also reveals if it is owing to latencies in synchronization.

<table>
<tr><td>Target of the test</td><td colspan="3">Citrix Storefront server</td></tr>
<tr><td>Agent deploying the test</td><td colspan="3">An internal/remote 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 – The port number at which the specified HOST listens to. By default, this is 443.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the Citrix Storefront 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>Synchronization status:
Indicates whether/not the contents are in sync with all Storefront servers in the group.</td><td></td><td>The values that this measure can take and their corresponding numeric values are as follows:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Sync not done</td><td>0</td></tr><tr><td>Sync completed</td><td>100</td></tr></table>
Note:
By default, this measure reports the Measure Values listed above to indicate the synchronization state. The graph of this measure however, represents the same using numeric equivalents only.</td></tr>
<tr><td></td><td>Synchronization duration:
Indicates the time taken for synchronization.</td><td>Secs</td><td>A high value or a consistent increase in the value of this measure is a cause for concern, as it indicates synchronization delays.</td></tr>
</table>

1.1.11 Stores Test

StoreFront stores enumerate and aggregate desktops and applications from XenDesktop sites, XenApp farms, and AppController, making these resources available to users. You can create as many stores as you need; for example, you might want to create a store for a particular group of users or to aggregate a specific set of resources.

If users complain that they are unable to access a store, administrators should be able to instantly figure what is causing the inaccessibility – is it because the store is unavailable? or is because of the store's poor responsiveness to user requests? This is where the **Stores** test helps! This test auto-discovers the stores configured on the Storefront server and reports the availability and responsiveness of each store, so that unavailable and unresponsive stores can be accurately isolated.

<table>
<tr><td>Purpose</td><td colspan="3">Auto-discovers the stores configured on the StoreFront server and reports the availability and responsiveness of each store, so that unavailable and unresponsive stores can be accurately isolated</td></tr>
<tr><td>Target of the test</td><td colspan="3">Citrix Storefront server</td></tr>
<tr><td>Agent deploying the test</td><td colspan="3">An internal/remote 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 – The port number at which the specified HOST listens to. By default, this is 443.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the each store configured on the Citrix Storefront 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>Availability:
Indicates whether/not this store is available.</td><td></td><td>The values that this measure can take and their corresponding numeric values are as follows:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Not available</td><td>0</td></tr><tr><td>Available</td><td>100</td></tr></table>
Note:
By default, this measure reports the Measure Values listed above to indicate the availability of a store. The graph of this measure however, represents the same using the numeric equivalents only.</td></tr>
<tr><td></td><td>Response time:
Indicates the time taken by this store to respond to user requests.</td><td>Secs</td><td>A high value or a consistent increase in the value of this measure is a cause for concern, as it indicates poor responsiveness.</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 **Citrix StoreFront**. 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.