Monitoring Citrix WEM Broker

eG Innovations Product Documentation

www.eginnovations.com

Table of Contents

Table of Figures

Chapter 1: Introduction

One of the common reasons for poor user logon experience in a Citrix XenApp/XenDesktop environment is the delay in profile loading and group policy application. Using Citrix Workspace Environment Management (WEM), this delay can be greatly minimized! Citrix WEM uses intelligent resource management and Profile Management technologies to provide the best logon experience to users in Citrix XenApp and XenDesktop deployments (see Figure 1.1).

Figure 1.1 depicts the architecture of Citrix WEM. The WEM Administration Console is where policies are defined and managed, resources are created and assigned, and users are authorized. The settings so defined are communicated to a WEM Broker, which stores the same in a SQL server backend. WEM Agents are deployed on VDAs or physical Windows devices. These agents communicate with the WEM Broker and enforce the settings you configured. An Active Directory server is used to push the settings to users.
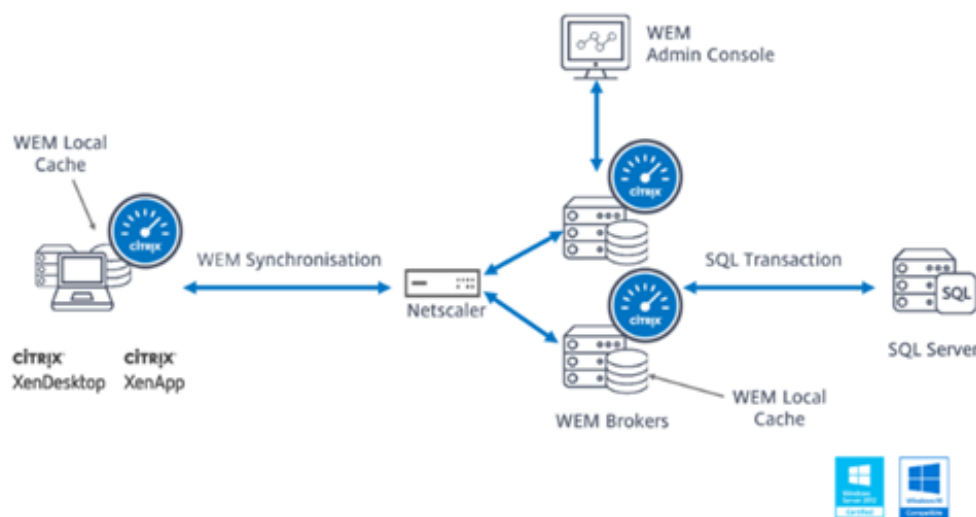

Figure 1.1: Architecture of Citrix WEM

Typically, the WEM agents offload the critical logon processing steps – e.g., group policy application, logon script execution, drive/printer mapping, etc. – and perform them after the logon, thus significantly improving logon speed (see Figure 1.2).
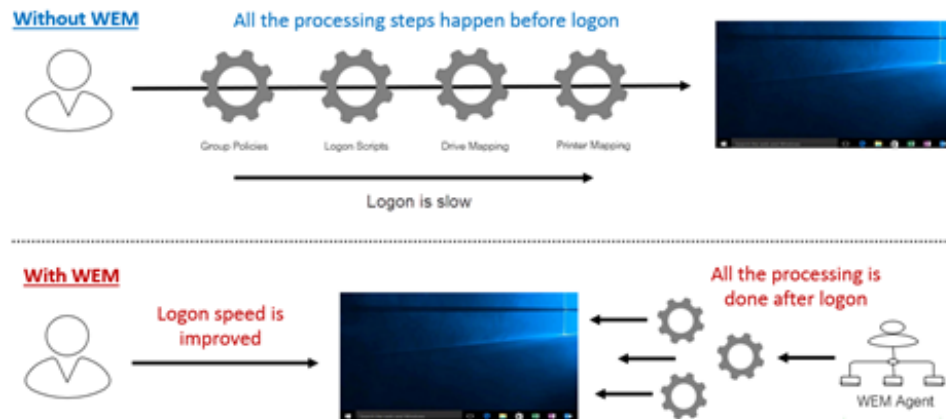
Figure 1.2: How Citrix WEM helps minimize logon time

This is why, where WEM is employed, user logons will be quick and hassle-free. However, if WEM clients – i.e., the WEM agents - experience delays or errors in logon processing, it can cause serious performance issues post logon. In other words, user profile loading, logon script execution, drive mapping etc., can become very slow. Because of such issues, a Citrix user will be unable to access the application/desktop profile, even after logging in quickly.

Besides processing delays on the WEM clients, the unavailability, poor responsiveness, and errors in functioning of the WEM broker can also impact WEM performance, and consequently, affect user experience.

Therefore, to assure users of a high quality experience with Citrix at all times, administrators of WEM-enabled environments should continuously monitor the WEM processing times on the clients. Additionally, the WEM broker should also be periodically checked for availability, responsiveness, and operational errors. eG Enterprise provides a specialized monitoring model that offers deep dive visibility into the performance of the *Citrix WEM Broker*.

Chapter 2: How Does eG Enterprise Monitor Citrix WEM Broker?

eG Enterprise monitors the Citrix WEM Broker in an agent-based manner. For this purpose, an eG agent should be deployed on the target Citrix WEM Broker.

2.1 Managing the Citrix WEM Broker

eG Enterprise can automatically discover the Citrix WEM Broker, and also lets you to manually add the component for monitoring. To manage a Citrix WEM Broker manually, do the following:

1. Log into the eG administrative interface.

2. If the Citrix WEM Broker is already discovered, then directly proceed towards managing the broker using the **COMPONENTS – MANAGE/UNMANAGE** page.

3. However, if you are yet to discover the Citrix WEM Broker, then run discovery (Infrastructure -> Components -> Discover) or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **COMPONENTS** page. Remember that components manually added are managed automatically.

Figure 2.1: Adding a Citrix WEM Broker

4. Specify the **Host IP/Name** and the **Nick name** of the Citrix WEM Broker in Figure 2.1. Then click the **Add** button to register the changes.

5. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

Figure 2.2: List of Unconfigured tests to be configured for the Citrix WEM Broker

6. Click on the WEM Database Connectivity test to configure it. To know how to configure the test, refer to Section **3.1.1**.

7. Once the test is configured, signout of the eG administrative interface.

Chapter 3: Monitoring Citrix WEM Broker

eG Enterprise provides you with extensive monitoring capabilities for the Citrix WEM Broker. Every layer of the monitoring model is mapped to a wide variety of tests that the eG agent executes and extracts performance metrics from the target Citrix WEM Broker.
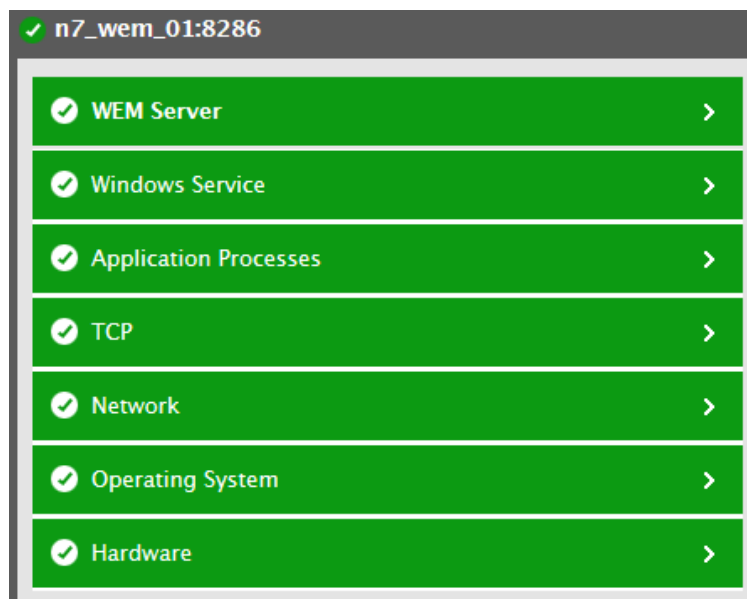
Figure 3.1: The layer model of a Citrix WEM Broker

The metrics thus collected would be useful to figure out accurate answers to the following queries:

- Is the license server available?

- How well the license server is responding to connection requests?

- How many error events were generated and are logged in the event logs?

- How many information and warning messages were generated and logged in the event logs?

- How many critical and verbose messages were generated and logged in the event logs?

- Is the WEM database server available?

- What is the response time of the WEM database server?

- How many records were fetched from the WEM database server?

- Is the query executed by the database server successful or not?

- Is the database connection to the Citrix WEM Broker available?

The sections to come will discuss the **WEM Server** layer only, as the remaining layers have already been dealt with in the *Monitoring Unix and Windows Servers* document.

3.1 The WEM Server Layer

Using the tests associated with this layer, administrators can figure out the availability and responsiveness of the license server, the event messages generated by the event logs of the broker and the availability and responsiveness of the WEM database server connected to the target Citrix WEM Broker. This way, administrators can be proactively alerted to error messages and the WEM database server that is poor to respond.
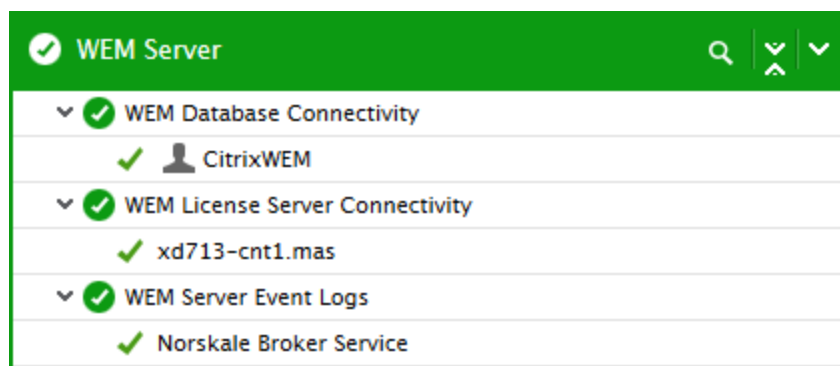
Figure 3.2: The tests associated with the WEM Server layer

3.1.1 WEM Database Connectivity Test

This test monitors the availability and response time of the WEM database server from an external agent perspective.

Target of the test : A Citrix WEM Broker

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each WEM database server connected to the target Citrix WEM Broker being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *8286*.

Parameter	Description
Database IP	By default, this parameter is set to none indicating that the Microsoft SQL server connected to the target Citrix WEM Broker and the Citrix WEM Broker are installed on the same host. However, if the Microsdot SQL Server is installed on a different host, then specify the IP address of the Microsoft SQL server connected to the target Citrix WEM Broker in this text box.
Database Port	The port number through which the Microsoft SQL server communicates with the target Citrix WEM Broker. By default, *1433* is displayed here.
Instance	In this text box, enter the name of a specific Microsoft SQL instance that is to be monitored. The default value of this parameter is " default". To monitor a Microsoft SQL instance named "CFS", enter this as the value of the Instance parameter.
User	By default, the target Citrix WEM Broker needs to be configured with the Microsoft SQL server 2008 and above. Therefore, while monitoring the Microsoft SQL server 2008, provide the name of a SQL user with the CONNECT SQL, VIEW ANY DATABASE, and VIEW SERVER STATE roles.
Password	The password of the specified user.
Confirm Password	Confirm the password by retyping it here.
SSL	If the target Citrix WEM Broker being monitored is an SSL-enabled server, then set the SSL flag to Yes. If not, then set the SSL flag to No.
Domain	By default, none is displayed in the Domain text box. If the 'SQL server and Windows' authentication has been enabled for the server being monitored, then the Domain can continue to be none. On the other hand, if 'Windows only' authentication has been enabled, then, in the Domain text box, specify the Windows domain in which the managed Microsoft SQL server exists. Also, in such a case, the User name and Password that you provide should be that of a user authorized to access the monitored SQL server.
ISNTLMV2	In some Windows networks, NTLM (NT LAN Manager) may be enabled. NTLM is a suite of Microsoft security protocols that provides authentication, integrity, and confidentiality to users. NTLM version 2 ("NTLMv2") was concocted to address the security issues present in NTLM. By default, the IsNTLMv2 flag is set to No, indicating that NTLMv2 is not enabled by default on the target Microsoft SQL host. Set this flag to Yes if NTLMv2 is enabled on the target host.
Database	The name of the database to connect to. The default is "CitrixWem". To monitor multiple databases, ensure that the database names are provided as a colon-separated list. Alternatively, you can use the semi-colon as the separator for the database names.
Query	The select query to execute. The default is "SELECT * FROM master.dbo.spt_

Parameter	Description
	monitor". If the target Microsoft SQL database server is installed as case sensitive, then the value of query parameter must be case sensitive. If multiple databases are specified in the Database text box, then you will have to provide multiple queries here separated by a semi-colon (;) - for eg., ELECT * FROM master.dbo.spt_monitor;select * from alarm. Every Database being monitored, should have a corresponding Query specification.
IsPassive	If the value chosen is Yes, then the MS SQL server under consideration is a passive server in a SQL cluster. No alerts will be generated if the server is not running. Measures will be reported as "Not applicable" by the agent if the server is not up.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option.
	The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:
	• The eG manager license should allow the detailed diagnosis capability
	• Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
SQL server availability	Indicates the availability of the database server.	Percent	A value of 100 indicates that the database server is currently available and a value 0 indicates that the database server is currently unavailable. A database server may be unavailable either when the server has not been started or due to misconfiguration/malfunctioning of the database server.
Connection time to database server	Indicates the time taken by this server to connect to the database server.	Secs	A low value is desired for this measure. A high value could indicate a connection

Measurement	Description	Measurement Unit	Interpretation
			bottleneck. Whenever the Total response time measure soars, you may want to check the value of this measure to determine whether a connection latency is causing the poor responsiveness of the server.
Records fetched	Indicates the number of records that were fetched from the database.	Number	If the value of this measure is 0, then it indicates that no records have been fetched from the database.
Query processor availability	Indicates whether the database query is executed successfully or not.	Percent	A value of 100 for this measure indicates that the query was executed successfully. The value 0 on the other hand indicates that the query failed. In the event that the SQL server availability measure reports the value 0, check the value of this measure to figure out whether the failed query is the reason why that measure reported server unavailability.
Query execution time	Indicates the time taken by the database server to execute a query.	Secs	A high value could indicate that one/more queries to the database are taking too long to execute. Inefficient/badly designed queries to the database often run for long periods. If the value of this measure is higher than that of the Database connection availability measure, you can be rest assured that long running queries are the ones causing the responsiveness of the server to suffer.
Total response time	Indicates the time taken by the database server to respond to a user query.	Secs	This measure is the sum total of the Connection time to database server and Query execution time measures. A low value is desired for this measure. A gradual/sudden increase in response time is indicative of a bottleneck at the

Measurement	Description	Measurement Unit	Interpretation
			database server.
Database connection availability	Indicates whether the database connection is currently available or not.	Percent	A value of 100 for this measure indicates that the database connection is available. The value 0 on the other hand indicates that the database connection is unavailable. A connection to the database may be unavailable if the database is down or if the database is listening on a port other than the one configured for it in the eG manager or owing to a poor network link. If the SQL server availability measure reports the value 0, then, you can check the value of this measure to determine whether/not it is due to the unavailability of a connection to the server.

3.1.2 WEM License Server Connectivity Test

This test promptly alerts administrators to the sudden non-availability of the license server and the time taken by the license server to respond to connection requests. Using this test, administrators may be alerted to the poor responsiveness of the license server.

Target of the test : A Citrix WEM Broker

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the target Citrix WEM Broker being monitored

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The IP address of the host for which the test is being configured.
Port	The port number at which the specified Host listens to. By default, this is *8286*.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Availability	Indicates the availability of TCP connection between the license server and the broker.	Percent	If the license server is available, a value of 100 is shown and if the license server is not available, a value of 0 is shown.
Response time	Indicates the time taken by the license server to respond to connection requests.	Secs	A low value is desired for this measure. A sudden or steady increase in this value could indicate a slowdown while connecting to the license server. This could be owing to a network congestion. Further investigation is however required to isolate the exact reason for the latency.

3.1.3 WEM Server Event Logs Test

This test monitors the events generated by the event log service and reports errors, if any.

Target of the test : A Citrix WEM Broker

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each event log generated for the target Citrix WEM Broker being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	Refers to the port used by the EventLog Service. Here it is null.
LogType	Refers to the type of event logs to be monitored. The default value is *Norskale Broker Service*.
PolicyFilter	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:

Parameter	Description
	• 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 PolicyFilter 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 PolicyFilter field.
Filter	If the PolicyFilter flag is set to **No**, then a Filter text area will appear, wherein you will have to specify the event sources, event IDs, and event descriptions to be monitored. This specification should be of the following format: *{Displayname}:{event_sources_to_be_included}:{event_sources_to_be_excluded}:{event_IDs_to_be_included}:{event_IDs_to_be_excluded}:{event_descriptions_to_be_included}:{event_descriptions_to_be_excluded}*. For example, assume that the Filter text area takes the value, *OS_events:all:Browse,Print:all:none:all:none*. Here:
	• *OS_events* is the display name that will appear as a descriptor of the test in the monitor UI;
	• *All* indicates that all the event sources need to be considered while monitoring. To monitor specific event sources, provide the source names as a comma-separated list. To ensure that none of the event sources are monitored, specify *none*.
	• Next, to ensure that specific event sources are excluded from monitoring, provide a comma-separated list of source names. Accordingly, in our example, *Browse* and *Print* have been excluded from monitoring. Alternatively, you can use *all* to indicate that all the event sources have to be excluded from monitoring, or *none* to denote that none of the event sources need be excluded.
	• In the same manner, you can provide a comma-separated list of event IDs that require monitoring. The *All* in our example represents that all the event IDs need to be considered while monitoring.
	• Similarly, the *none* (following *all* in our example) is indicative of the fact that none of the event IDs need to be excluded from monitoring. On the other hand, if you want to instruct the eG Enterprise system to ignore a few event IDs during

Parameter	Description

monitoring, then provide the IDs as a comma-separated list. Likewise, specifying *all* makes sure that all the event IDs are excluded from monitoring.

- The *all* which follows implies that all events, regardless of description, need to be included for monitoring. To exclude all events, use *none*. On the other hand, if you provide a comma- separated list of event descriptions, then the events with the specified descriptions will alone be monitored. Event descriptions can be of any of the following forms - *desc**, or *desc*, or *desc*,or *desc**, or *desc1*desc2*, etc. *desc* here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.

- In the same way, you can also provide a comma-separated list of event descriptions to be excluded from monitoring. Here again, the specification can be of any of the following forms: *desc**, or *desc*, or *desc*,or *desc**, or *desc1*desc2*, etc. *desc* here refers to any string that forms part of the description. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters. In our example however, none is specified, indicating that no event descriptions are to be excluded from monitoring. If you use *all* instead, it would mean that all event descriptions are to be excluded from monitoring.

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

Note:

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

On the other hand, if the PolicyFilter 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}

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

Parameter	Description
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Information	This refers to the number of application information events generated when the test was last executed.	Number	A change in the value of this measure may indicate infrequent but successful operations performed by one or more applications. Please check the Norskale Agent Service Logs in the Event Log Viewer for more details.
Warnings	This refers to the number of warnings that were generated when the test was last executed.	Number	A high value of this measure indicates problems 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 Norskale Agent Service Logs in the Event Log Viewer for more details.

Measurement	Description	Measurement Unit	Interpretation
Errors	This refers to the number of application error events that were generated.	Number	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 Norskale Agent Service Logs in the Event Log Viewer for more details.
Critical errors	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 Norskale Agent Service Logs in the Event Log Viewer for more details.
Verbose	Indicates the number of verbose events that were generated when the test	Number	Verbose logging provides more details in the log entry, which will enable you to troubleshoot issues better.

Measurement	Description	Measurement Unit	Interpretation
	was last executed.		**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 Norskale Agent Service Logs in the Event Log Viewer for more details.

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.