Monitoring Nimble Storage

eG Enterprise v6.1

Restricted Rights Legend

Trademarks

Copyright

Table of Contents

1

Monitoring Nimble Storage

The Nimble Storage network services appliance provides reliable, scalable, and secure core network services including DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), IPAM (IP Address Management), IF-MAP, and more. The integrated Nimble Storage approach combines the simplicity of appliances with the power of advanced distributed database technology to control and automate services while achieving availability, manageability, visibility, and control unparalleled by conventional solutions based on legacy technologies. The Nimble Storage appliance can be configured and managed through an easy to use Nimble Storage GUI (Graphical User Interface) that works seamlessly in Windows, Linux and Mac environments using standard web browsers.

Nimble Storage arrays efficiently store and serve up data fast enough to satisfy even the most demanding applications, from Microsoft SQL Server to VDI. Using flash SSDs to dynamically cache hot data to accelerate reads and leveraging a write-optimized data layout to speed up data written to storage, Nimble delivers more IOPS than traditional storage at proven sub-millisecond latencies (measured across Nimble's installed base).

Cache Accelerated Sequential Layout (CASL) is the foundation for Nimble Storage's high performance and capacity savings, integrated data protection, and easy lifecycle management.

CASL features include:

Flash-Based Dynamic Cache

Accelerate read access to application data by holding a copy of active "hot" data in flash; customers benefit from high read throughput and low latency.

Write-Optimized Data Layout

Data written by a host is first aggregated or coalesced, then written sequentially as a full stripe to a pool of disk; CASL's sweeping process also consolidates freed up disk space for future writes. Customers benefit from fast sub-millisecond writes and very efficient disk utilization.

Inline Universal Compression

30 to 75 percent with no added latency; customers gain much more usable disk capacity with zero performance impact.

Instantaneous Point-in-Time Snapshots

Fast restores without copying data; customers benefit from a single, simple storage solution for primary and secondary data, frequent and instant backups, and significant capacity savings.

Efficient Integrated Replication

Only copy compressed, changed data to a secondary site at a pre-set schedule; customers benefit from affordable disaster recovery.

Zero-Copy Clones

Created instantly, customers get great space efficiency and performance on cloned volumes, making them ideal for virtualization, virtual desktop infrastructure (VDI) and test and development environments.

eG Enterprise provides a specialized Nimble Storage monitoring model (see Figure 1) to monitor the components of the Nimble Storage and report discrepancies arising in those components.

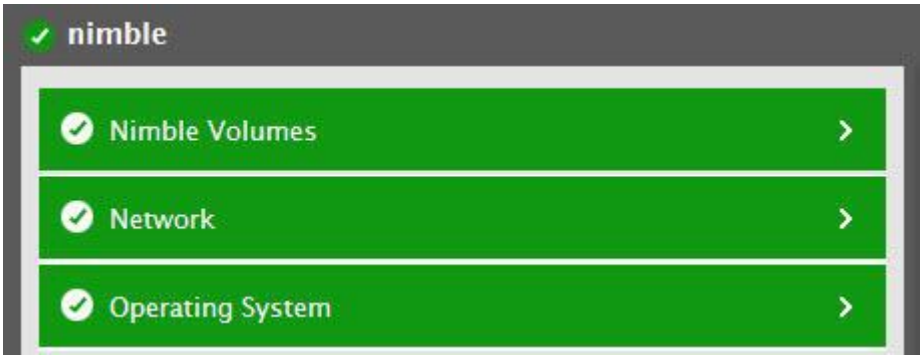

Figure 1: The layer model of the Nimble Storage

Every layer of Figure 1 is mapped to a variety of tests which connect to the SNMP traps and SNMP MIB of the Nimble Storage to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- How many events were triggered for disk failures, fan failures, power supply failures. Temperature failure etc?
- What is the I/O latency of the Nimble Storage?
- How well the read and write operations were performed sequentially and in random?
- How well each volume and disk of the Nimble Storage are utilized?
- How many read requests were catered successfully through the read cache?

Since the **Network** layer has been dealt with *Monitoring Web Servers* document, the sections to come will discuss the remaining layers of Figure 1.

1.1 Pre-requisites to monitor the Nimble Storage

In order to collect the trap messages sent by the target storage, the eG agent should be configured as an SNMP Trap Receiver. To know more on how to configure the eG agent as an SNMP Trap Receiver, refer to the *Handling SNMP Traps using eG Enterprise* document.

1.2 The Operating System Layer

Using the test mapped to this layer, administators can proactively identify the trap messages sent by the storage due to the failure of various critical components of the Nimble Storage and take remedial measures before any serious issues occur.

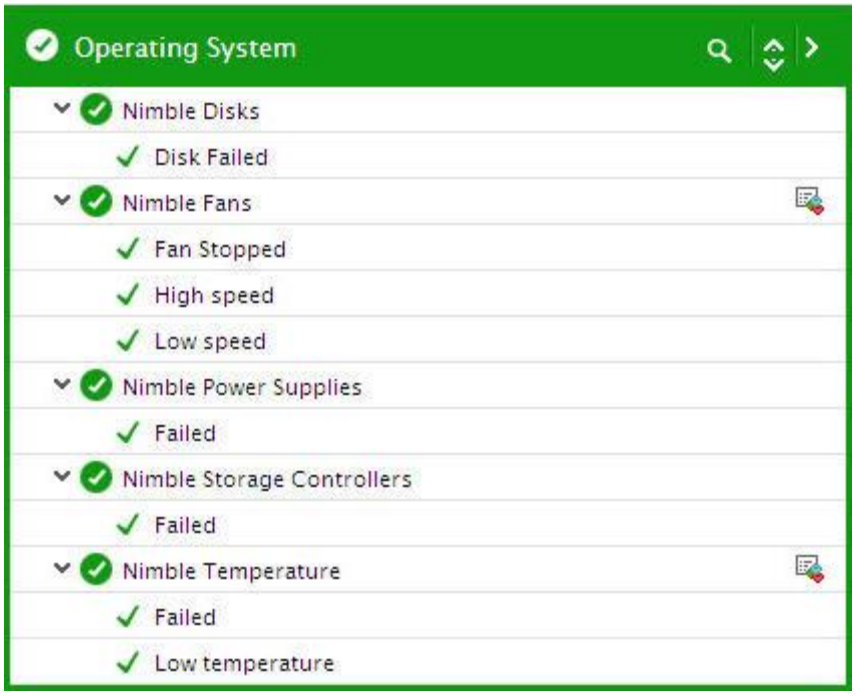

Figure 2: The tests mapped to the Operating System layer

1.2.1 Nimble Disks Test

This test intercepts the disk failure traps sent by the storage, extracts relevant information related to the failure from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the disk failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Purpose	Intercepts the disk failure traps sent by the storage, extracts relevant information related to the failure from the traps, and reports the count of these trap messages to the eG manager
Target of the test	A Nimble Storage
Agent deploying the test	An external 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 at which the specified **HOST** listens. By default, this is NULL.
4. **SOURCEADDRESS** – Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
5. **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: *.1.3.6.1.4.1.9156.1.1.2* and *.1.3.6.1.4.1.9156.1.1.3*. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

   In this case the oidvalue parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface.

   An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**.

   Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be HOST and not Host_system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be:

   Trap5: .1.3.6.1.4.1.9156.1.1.5-any.
6. **SHOWOID** – Specifying **true** against **SHOWOID** will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **false**, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
7. **TRAPOIDS** – By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces.
8. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the

	detailed diagnosis capability for this test, you can do so by specifying *none* against **DD FREQUENCY**. 9. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: 0. ➢ The eG manager license should allow the detailed diagnosis capability ➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.
Outputs of the test	One set of results for each type of failure event triggered on the target Nimble Storage

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Disk failures: Indicates the number of times this event was triggered during the last measurement period.	Number	The failure events may be generated due to the failure of one or more disks of the Nimble Storage. If the failure events are not rectified within a certain pre-defined timeperiod, the storage will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Nimble storage.

1.2.2 Nimble Fans Test

This test intercepts the fan failure traps sent by the switch, extracts relevant information related to the failure from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the fan failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Purpose	Intercepts the fan failure traps sent by the switch, extracts relevant information related to the failure from the traps, and reports the count of these trap messages to the eG manager
Target of the test	A Nimble Storage
Agent deploying the test	An external agent

<table>
<tr>
<td>Configurable parameters for the test</td>
<td>
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 at which the specified HOST listens. By default, this is NULL.
4. SOURCEADDRESS – Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
5. OIDVALUE - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>
In this case the oidvalue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.
An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.
Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be HOST and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDVALUE specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:
Trap5: .1.3.6.1.4.1.9156.1.1.5-any.
6. SHOWOID – Specifying true against SHOWOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter false, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
7. TRAPOIDS – By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
8. DD FREQUENCY - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the
</td>
</tr>
</table>

<table>
<tr><td></td><td colspan="3">detailed diagnosis capability for this test, you can do so by specifying none against DD FREQUENCY.

9. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: 0.

➢ The eG manager license should allow the detailed diagnosis capability

➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each type of failure event that occurred on the target Nimble Storage</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>Fan failures:
Indicates the number of events of this type that were triggered during the last measurement period.</td><td>Number</td><td>The failure events may be generated due to the failure of the fans of the Nimble Storage. If the failure events are not rectified within a certain pre-defined timeperiod, the storage system will be shutdown automatically.

Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Nimble Storage.</td></tr>
</table>

1.2.3 Nimble Power Supplies Test

Abnormal power fluctuation to the hardware components often lead to the malfunctioning of the Nimble Storage which when left unnoticed can prove to be fatal to the availability and overall health. This test intercepts the traps sent by the storage, extracts information related to power supply failures from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the abnormalities in the power supply if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Purpose	Intercepts the traps sent by the storage, extracts information related to power supply failures from the traps, and reports the count of these trap messages to the eG manager.
Target of the test	A Nimble Storage
Agent deploying the test	An external 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 at which the specified **HOST** listens. By default, this is NULL.
4. **SOURCEADDRESS** – Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
5. **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: *.1.3.6.1.4.1.9156.1.1.2* and *.1.3.6.1.4.1.9156.1.1.3*. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

   In this case the oidvalue parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface.

   An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**.

   Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be HOST and not Host_system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be:

   Trap5: .1.3.6.1.4.1.9156.1.1.5-any.
6. **SHOWOID** – Specifying **true** against **SHOWOID** will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **false**, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
7. **TRAPOIDS** – By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces.
8. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the

	detailed diagnosis capability for this test, you can do so by specifying *none* against **DD FREQUENCY**. 9. **DETAILED DIAGNOSIS** - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: 0. ➢ The eG manager license should allow the detailed diagnosis capability ➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.
Outputs of the test	One set of results for each type of event that occurred on the target Nimble Storage

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Power supply failures: Indicates the number of times this event was triggered during the last measurement period.	Number	The failure events may be generated due to the failure of one or more Power supply units of the Nimble Storage. If the failure events are not rectified within a certain pre-defined timeperiod, the storage will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Nimble Storage.

1.2.4 Nimble Temperature Test

Abnormal temperature of the hardware components often lead to the malfunctioning of the Nimble Storage which when left unnoticed may affect the overall health. This test the temperature traps sent by the hardware components of the storage, extracts information related to temperature errors/failures from the traps, and reports the count of these trap messages to the eG manager.

Purpose	Intercepts the temperature traps sent by the hardware components of the storage, extracts information related to temperature errors/failures from the traps, and reports the count of these trap messages to the eG manager
Target of the test	A Nimble Storage
Agent deploying the test	An external 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 at which the specified **HOST** listens. By default, this is NULL.
4. **SOURCEADDRESS** – Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
5. **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: *.1.3.6.1.4.1.9156.1.1.2* and *.1.3.6.1.4.1.9156.1.1.3*. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

In this case the oidvalue parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface.

An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**.

Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be HOST and not Host_system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be:

Trap5: .1.3.6.1.4.1.9156.1.1.5-any.

6. **SHOWOID** – Specifying **true** against **SHOWOID** will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **false**, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
7. **TRAPOIDS** – By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces.
8. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the

<table>
<tr><td></td><td colspan="3">detailed diagnosis capability for this test, you can do so by specifying none against DD FREQUENCY.

9. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: 0.

➢ The eG manager license should allow the detailed diagnosis capability

➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each type of event that occurred on the target Nimble Storage</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>Temperature failures:
Indicates the number of times this event was triggered during the last measurement period.</td><td>Number</td><td>The failure events may be generated due to the temperature failure of the hardware components of the Nimble Storage. If the failure events are not rectified within a certain pre-defined timeperiod, the storage will be shutdown automatically.

Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Nimble Storage.</td></tr>
</table>

1.2.5 Nimble Storage Controllers Test

This test intercepts the storage controller failure traps sent by the Nimble Storage, extracts information related to errors/failures from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the abnormalities in the storage controllers if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Purpose	Intercepts the storage controller failure traps sent by the Nimble Storage, extracts information related to errors/failures from the traps, and reports the count of these trap messages to the eG manager
Target of the test	A Nimble Storage
Agent deploying the test	An external 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 at which the specified **HOST** listens. By default, this is NULL.
4. **SOURCEADDRESS** – Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, *10.0.0.1,192.168.10.**. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
5. **OIDVALUE** - Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: *.1.3.6.1.4.1.9156.1.1.2* and *.1.3.6.1.4.1.9156.1.1.3*. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

   In this case the oidvalue parameter can be configured as *Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network*, where *Trap1* and *Trap2* are the display names that appear as descriptors of this test in the monitor interface.

   An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to *Failed:*-F**.

   Typically, if a valid value is specified for an OID in the *OID-value* pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID *.1.3.6.1.4.1.9156.1.1.2* is found to be HOST and not Host_system, then the test ignores OID *.1.3.6.1.4.1.9156.1.1.2* while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your **OIDVALUE** specification should be: *DisplayName:OID-any*. For instance, to ensure that the test monitors the OID *.1.3.6.1.4.1.9156.1.1.5*, which in itself, say represents a failure condition, then your specification would be:

   Trap5: .1.3.6.1.4.1.9156.1.1.5-any.
6. **SHOWOID** – Specifying **true** against **SHOWOID** will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **false**, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
7. **TRAPOIDS** – By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces.
8. **DD FREQUENCY** - Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the

<table>
<tr><td></td><td colspan="3">detailed diagnosis capability for this test, you can do so by specifying none against DD FREQUENCY.

9. DETAILED DIAGNOSIS - To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the On option. To disable the capability, click on the Off option.

The option to selectively enabled/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: 0.

➢ The eG manager license should allow the detailed diagnosis capability

➢ Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each type of event that occurred on the target Nimble Storage</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>Controller failures:

Indicates the number of times this event was triggered during the last measurement period.</td><td>Number</td><td>The failure events may be generated due to the failure of the storage controllers of the Nimble Storage. If the failure events are not rectified within a certain pre-defined timeperiod, the storage will be shutdown automatically.

Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Nimble Storage.</td></tr>
</table>

1.3 The Nimble Volumes Layer

Using the test mapped to this layer, administators can proactively be alerted to potential issues in read/write operations, I/O operations throughput, decreasing disk latency, volume utilization, read cache utilization etc.

Figure 3: The tests mapped to the Nimble Volumes layer

1.3.1 Nimble I/O Latency Test

This test helps you to figure out the average time taken to process the read and write operations on the Nimble Storage. Using this test, administrators can figure out if there exists any road blocks to the rapid rading/writing to the Nimble Storage and rectify the same before end users start complaining.

Purpose	Helps you to figure out the average time taken to process the read and write operations on the Nimble Storage.
Target of the test	A Nimble Storage
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Nimble Storage 3. **SNMPPORT** – The SNMP Port number of the Nimble Storage (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the encryptflag is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Nimble Storage over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the target Nimble Storage that is to be 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>Read latency:
Indicates the average time taken to process the read operations during the last measurement period.</td><td>Secs</td><td rowspan="2">Very high values for these measures are indicative of the existence of road-blocks to rapid reading/writing by the Nimble Storage.
By observing the variations in these measures over time, you can understand whether the latencies are sporadic or consistent. Consistent delays in reading/writing could indicate that there are persistent bottlenecks (if any) in the Nimble Storage to speedy I/O processing.</td></tr>
<tr><td>Write latency:
Indicates the average time taken to process the write operations during the last measurement period.</td><td>Secs</td></tr>
</table>

1.3.2 Nimble I/O Performance Test

This test monitors the I/O operations of the Nimble storage system and reports how well the I/O operations were read from/written to sequentially and in random. This way, administrators can analyze the throughput of the Nimble Storage system and take remedial measures before any discrepancies arise.

Purpose	Reports the current status of each physical node service of the Nimble Storage system
Target of the test	A Nimble Storage
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Nimble Storage 3. **SNMPPORT** – The SNMP Port number of the Nimble Storage (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

	6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Nimble Storage over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for the target Nimble Storage that is to be monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Sequential read IOPS: Indicates the rate at which I/O operations were read sequentially during the last measurement period.	IOPS	
	Sequential write IOPS: Indicates the rate at which I/O operations were written sequentially during the last measurement period.	IOPS	A high value is desired for this measure. A low value for this measure may indicate a poor throughput thus resulting in a decrease in the free space and the performance of the disks.
	Random read IOPS: Indicates the rate at which random I/O operations were read during the last measurement period.	IOPS	
	Random write IOPS: Indicates the rate at which random I/O operations were written during the last measurement period.	IOPS	

1.3.3 Nimble Performance Test

This test reports the rate at which the data is read from and written to the Nimble Storage sequentially and at random. Using this test, administrators can easily figure out if there are any performance bottlenecks and rectify the same before any serious issues crop up.

Purpose	Reports the rate at which the data is read from and written to the Nimble Storage sequentially and at random
Target of the test	A Nimble Storage
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Nimble Storage 3. **SNMPPORT** – The SNMP Port number of the Nimble Storage (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

	6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Nimble Storage over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.
Outputs of the test	One set of results for the target Nimble Storage that is to be monitored

Measurements made by the test	Measurement	Measurement Unit	Interpretation
	Sequential read data: Indicates the rate at which data is read sequentially during the last measurement period.	MB/Sec	
	Sequential write data: Indicates the rate at which data is written sequentially during the last measurement period.	MB/Sec	A high value is desired for this measure. If the value of this measure is high, then it indicates that the disk of the Nimble Storage is being utilized optimally. If the value of this measure decreases gradually, then it indicates that there is an abnormal increase in the disk latency.
	Random read data: Indicates the rate at which random data is read during the last measurement period.	MB/Sec	
	Random write data: Indicates the rate at which random data is written during the last measurement period.	MB/Sec	

1.3.4 Nimble Volumes Test

For users to be able to read from/write data into volumes quickly, the volumes must be online and adequate space must be available in the volumes. Slowdowns in data storage/retrieval can be attributed to storage space contentions experienced by one/more volumes or I/O processing bottlenecks. In the event of such slowdowns, administrators need to swiftly isolate the following:

- Are the volumes currently online?
- Which volumes are over-utilized?
- Which volumes are overloaded?

The **Nimble Volumes** test provides accurate answers to these questions. With the help of these answers, you can quickly diagnose the root-cause of slowdowns when reading from/writing into a volume.

Purpose	Helps quickly identify problematic volumes and accurately diagnose the root-cause of slowdowns when reading from/writing into a volume
Target of the test	A Nimble Storage
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Nimble Storage 3. **SNMPPORT** – The SNMP Port number of the Nimble Storage (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the encryptflag is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Nimble Storage over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each volume of the Nimble Storage that is to be 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>Is the volume online?:
Indicates whether/not this volume is online.</td><td></td><td>This measure reports the value Yes if this volume is currently online and the value No if otherwise.
The values reported by this measure and their numeric equivalents are available in the table below:<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>Note:
This measure reports the Measure Values listed in the table above while indicating whether this volume is currently online or not. However, in the graph of this measure, the state is indicated using only the Numeric Values listed in the above table.</td></tr>
<tr><td>Total space:
Indicates the total capacity of this volume.</td><td>TB</td><td></td></tr>
<tr><td>Used space:
Indicates the amount of space that is already utilized in this volume.</td><td>TB</td><td>If the value of this measure is close to that of the Total space measure, it indicates that the volume is running out of space.</td></tr>
</table>

	Free space: Indicates the amount of spacec that is currently available for use in this volume.	TB	A high value is desired for this measure.
	Space utilization: Indicates the percentage of space that is utilized in this volume.	Percent	A low value is desired for this measure.
	Free space utilization: Indicates the percentage of space that is available for use in this volume.	Percent	A high value is desired for this measure.
	iSCSI connections: Indicates the number of iSCSI connections established to this volume.	Number	This measure is a good indicator of the current workload on the volume.

1.3.5 Nimble Cache Test

Using this test, administrators can identify how well the read cache of the Nimble Storage is utilized.

Purpose	Helps administrators identify how well the read cache of the Nimble Storage is utilized
Target of the test	A Nimble Storage
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Nimble Storage 3. **SNMPPORT** – The SNMP Port number of the Nimble Storage (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the encryptflag is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

	15. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Nimble Storage over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for the target Nimble Storage that is to be monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Read cache hits: Indicates the rate at which read requests were successfully fulfilled by the read cache during the last measurement period.	Hits/sec	A high value is desired for this measure.

1.3.6 Nimble Disk Space Test

This test helps administrators figure out the space utilized by the volumes and snapshots on the Nimble Storage array.

To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence: Agents -> Tests -> Enable/Disable, pick *Nimble Storage* as the **Component type**, *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **<<** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Purpose	Helps administrators to figure out the space utilized by the volumes and snapshots on the Nimble Storage array.
Target of the test	A Nimble storage
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The IP address of the Nimble Storage 3. **SNMPPORT** – The SNMP Port number of the Nimble Storage (161 typically) 4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **USERNAME** – This parameter appears only when **v3** is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: ➢ **MD5** – Message Digest Algorithm ➢ **SHA** – Secure Hash Algorithm 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the encryptflag is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types: ➢ **DES** – Data Encryption Standard ➢ **AES** – Advanced Encryption Standard 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. DATA OVER TCP – By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the Nimble Storage over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the target Nimble Storage that is to be 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>Data used on disk for volumes:
Indicates the amount of space used by the volumes on the storage array.</td><td>TB</td><td></td></tr>
<tr><td>Data used on disk for snapshots:
Indicates the amount of space used by the snapshots on the storage array.</td><td>TB</td><td></td></tr>
</table>

2 Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **Nimble Storage**. 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.