Monitoring Nimble Storage

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

CHAPTER 1: INTRODUCTION 1

CHAPTER 2: HOW TO MONITOR THE NIMBLE STORAGE USING EG ENTERPRISE? 3

2.1 Managing the Nimble Storage 3

2.2 Configuring the tests 4

CHAPTER 3: MONITORING NIMBLE STORAGE 6

3.1 The Operating System Layer 6

3.1.1 Nimble Arrays Test 7

3.1.2 Nimble Disks Test 10

3.1.3 Nimble Fans Test 13

3.1.4 Nimble Power Supplies Test 16

3.1.5 Nimble Raids Test 19

3.1.6 Nimble Temperature Test 21

3.1.7 Nimble Storage Controllers Test 24

3.2 The Nimble Volumes Layer 27

3.2.1 Nimble I/O Latency Test 27

3.2.2 Nimble I/O Performance Test 30

3.2.3 Nimble Throughput Test 34

3.2.4 Nimble Volumes Test 37

3.2.5 Nimble Cache Test 41

3.2.6 Nimble Disk Space Test 43

ABOUT EG INNOVATIONS 46

Table of Figures

Figure 2.1: Adding the Nimble Storage 4

Figure 2.2: List of tests that need to be configured for the Nimble Storage 4

Figure 3.1: The layer model of the Nimble Storage 6

Figure 3.2: The tests mapped to the Operating System layer 7

Figure 3.3: The tests mapped to the Nimble Volumes layer 27

Chapter 1: Introduction

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.

Chapter 2: How to Monitor the Nimble Storage Using eG Enterprise?

eG Enterprise monitors the Nimble storage using an **eG external agent** on any remote host. The external agent periodically tracks the SNMP traps and polls the SNMP MIB of the Nimble Storage to collect critical statistics pertaining to its performance.

The broad steps for monitoring Nimble Storage using eG Enterprise are as follows:

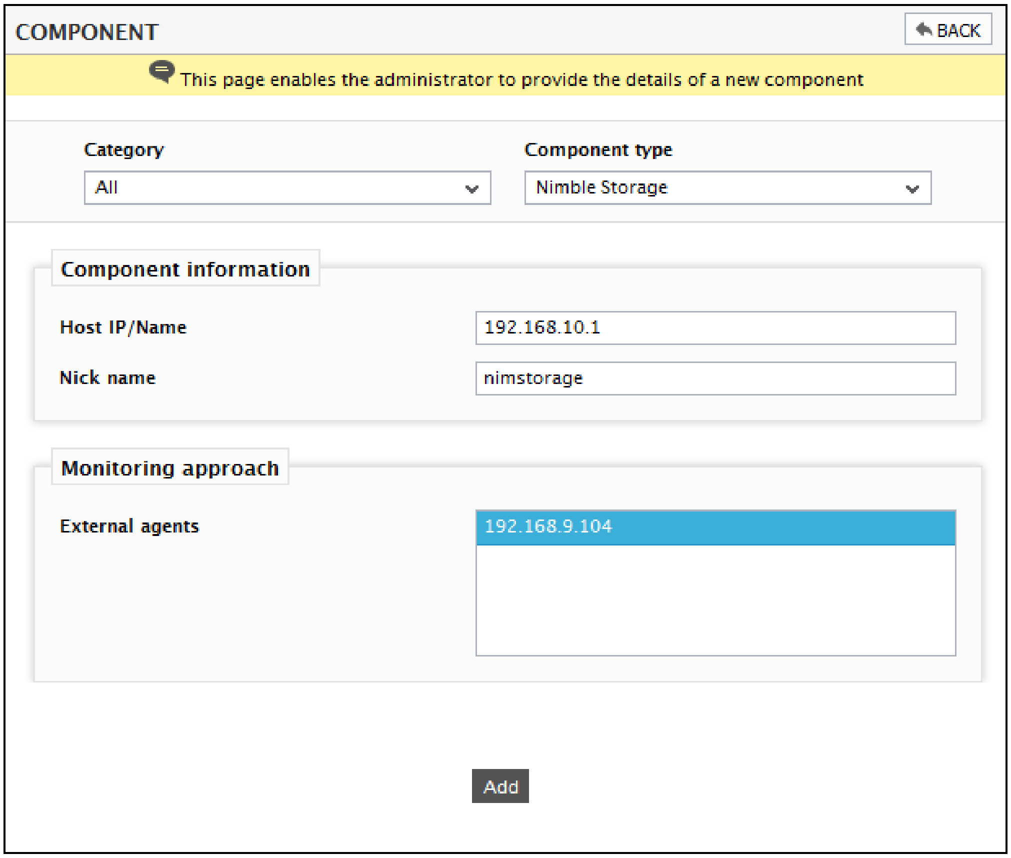
- Managing the Nimble Storage
- Configuring the tests

These steps have been discussed in following sections.

2.1 Managing the Nimble Storage

The eG Enterprise cannot automatically discover the Nimble Storage. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a Nimble Storage component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *Nimble Storage* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.


COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: Nimble Storage

Component information

Host IP/Name: 192.168.10.1

Nick name: nimstorage

Monitoring approach

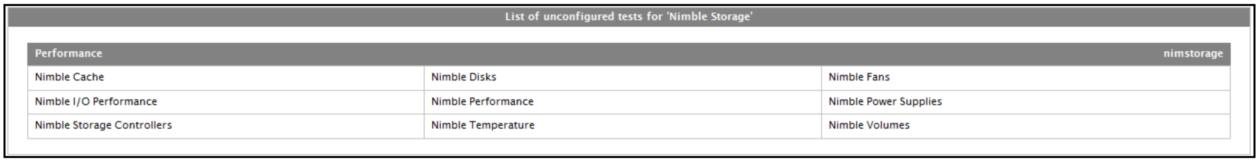
External agents: 192.168.9.104

Figure 2.1: Adding the Nimble Storage

4. Specify the **Host IP** and the **Nick name** for the Nimble Storage in Figure 2.1. Then, click the **Add** button to register the changes.

2.2 Configuring the tests

1. When you attempt to sign out of eG administrative interface, a list of unconfigured tests will appear as shown in Figure 2.2. This list reveals the unconfigured tests that require manual configuration.


List of unconfigured tests for 'Nimble Storage'

Performance		nimstorage
Nimble Cache	Nimble Disks	Nimble Fans
Nimble I/O Performance	Nimble Performance	Nimble Power Supplies
Nimble Storage Controllers	Nimble Temperature	Nimble Volumes

Figure 2.2: List of tests that need to be configured for the Nimble Storage

2. To configure the tests, click on the test names in the list of unconfigured tests. For the details on

configuring the tests, refer to **Monitoring Nimble Storage** chapter.

3. Once all the tests are configured, signout of the eG administrative interface.

Chapter 3: Monitoring Nimble Storage

eG Enterprise provides a specialized Nimble Storage monitoring model (see Figure 3.1) to monitor the components of the Nimble Storage and report discrepancies arising in those components.

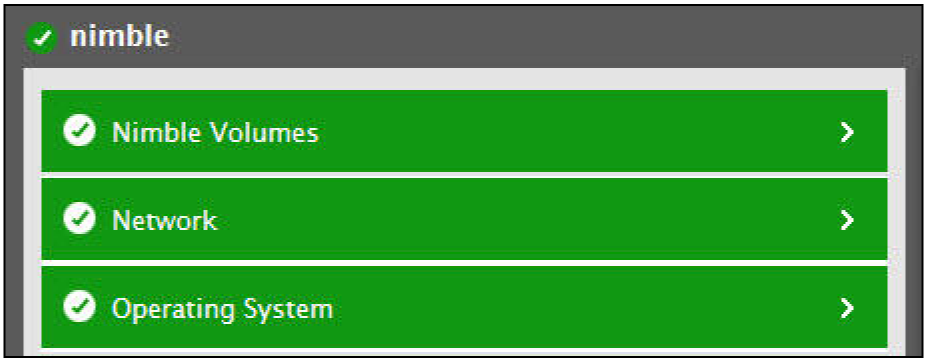


Figure 3.1: The layer model of the Nimble Storage

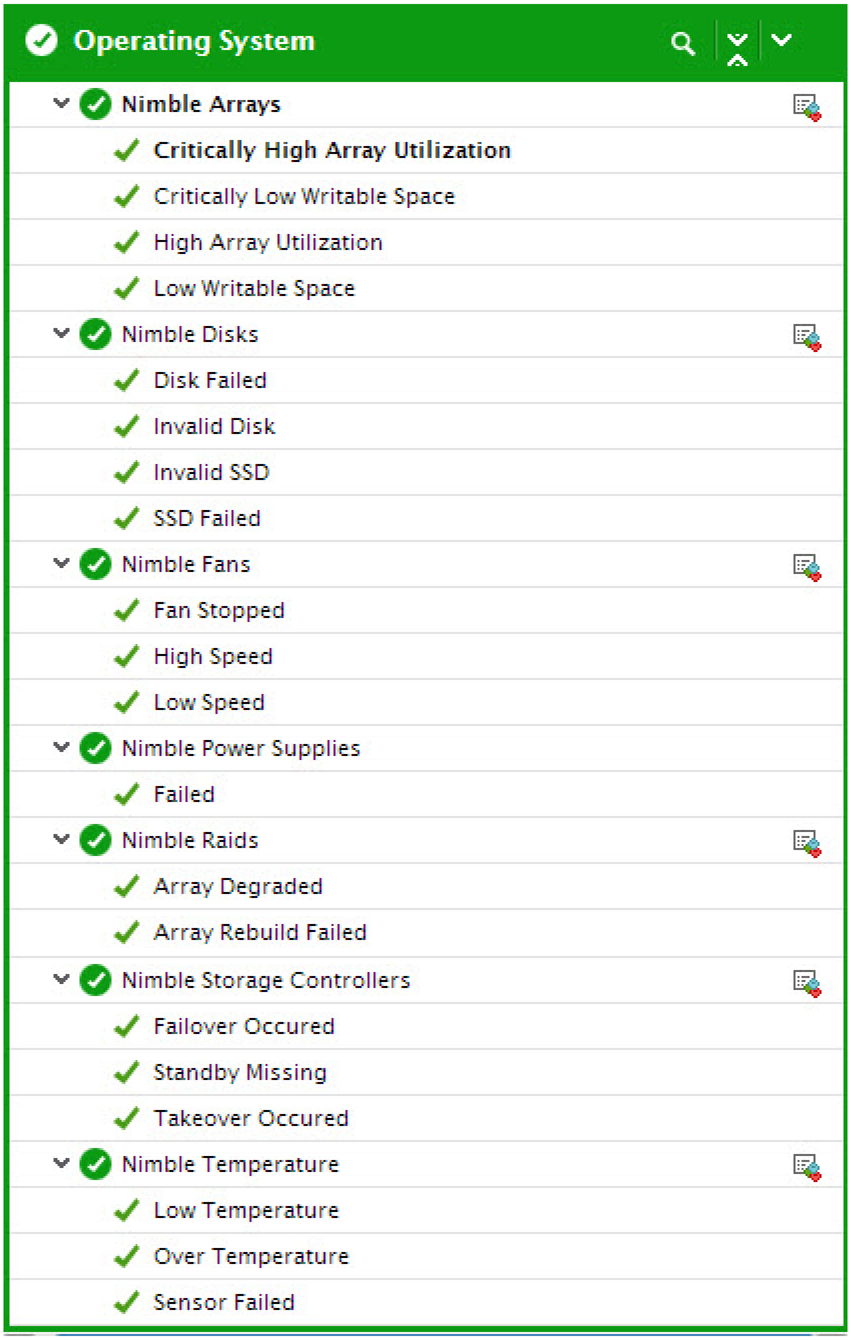
Every layer of the layer model is mapped to a variety of tests which connect to the SNMP traps and SNMP MIB of the Nimble Storage to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- 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 within the *Monitoring Unix and Windows Servers* document, the sections to come will discuss the remaining layers of the layer model.

3.1 The Operating System Layer

Using the test mapped to this layer, administrators 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.



Operating System

- Nimble Arrays
  - Critically High Array Utilization
  - Critically Low Writable Space
  - High Array Utilization
  - Low Writable Space
- Nimble Disks
  - Disk Failed
  - Invalid Disk
  - Invalid SSD
  - SSD Failed
- Nimble Fans
  - Fan Stopped
  - High Speed
  - Low Speed
- Nimble Power Supplies
  - Failed
- Nimble Raids
  - Array Degraded
  - Array Rebuild Failed
- Nimble Storage Controllers
  - Failover Occured
  - Standby Missing
  - Takeover Occured
- Nimble Temperature
  - Low Temperature
  - Over Temperature
  - Sensor Failed

Figure 3.2: The tests mapped to the Operating System layer

3.1.1 Nimble Arrays Test

This test intercepts the array 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 array failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event triggered on the target Nimble Storage.

Configurable parameters for the test

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>Test Period</td><td>How often should the test be executed.</td></tr>
<tr><td>Host</td><td>The host for which the test is to be configured.</td></tr>
<tr><td>Port</td><td>The port at which the specified Host listens. By default, this is <i>NULL</i>.</td></tr>
<tr><td>Source Address</td><td>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.</td></tr>
<tr><td>OID Value</td><td>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*.</td></tr>
</table>

Parameters	Description
	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. In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be: Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any. Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.
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.
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.
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

Parameters	Description
	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
Traps count	Indicates the number of times this event was triggered during the last measurement period.	Number	Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Nimble storage array.

3.1.2 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event triggered on the target Nimble Storage.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>Port</td><td>The port at which the specified Host listens. By default, this is <i>NULL</i>.</td></tr>
<tr><td>Source Address</td><td>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.</td></tr>
<tr><td>OID Value</td><td><p>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:</p>
<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>
<p>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.</p>
<p>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*.</p>
<p>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:</p>
<p>Trap5: .1.3.6.1.4.1.9156.1.1.5-any.</p>
<p>In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your</p></td></tr>
</table>

Parameters	Description
	specification should be: Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any. Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.
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.
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.
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
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.

3.1.3 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event that occurred on the target Nimble Storage.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port at which the specified Host listens. By default, this is *NULL*.
Source Address	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.

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>OID Value</td><td>
<p>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:</p>
<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>
<p>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.</p>
<p>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*.</p>
<p>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:</p>
<p>Trap5: .1.3.6.1.4.1.9156.1.1.5-any.</p>
<p>In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:</p>
<p>Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any.</p>
<p>Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.</p>
</td></tr>
<tr><td>ShowOID</td><td>Specifying True against ShowOID will ensure that the detailed diagnosis of this test</td></tr>
</table>

Parameters	Description
	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.
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.
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
Fan failures	Indicates the number of events of this type that were triggered during the last measurement period.	Number	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

Measurement	Description	Measurement Unit	Interpretation
			automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Nimble Storage.

3.1.4 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of event that occurred on the target Nimble Storage.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port at which the specified Host listens. By default, this is *NULL*.
Source Address	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.
OID Value	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

Parameters **Description**

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.

In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:

Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any.

Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.

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.

TrapOIDs — By default, this parameter is set to *all*, indicating that the eG agent considers all the

Parameters	Description
	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.
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
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

Measurement	Description	Measurement Unit	Interpretation
			indication of performance degradation of the Nimble Storage.

3.1.5 Nimble Raids Test

This test intercepts the RAID 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 array failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event triggered on the target Nimble Storage.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port at which the specified Host listens. By default, this is *NULL*.
Source Address	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.
OID Value	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>Parameters</th><th>Description</th></tr>
<tr><td></td><td>
<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>
<p>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.</p>
<p>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*.</p>
<p>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:</p>
<p>Trap5: .1.3.6.1.4.1.9156.1.1.5-any.</p>
<p>In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:</p>
<p>Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any.</p>
<p>Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.</p>
</td></tr>
<tr><td>ShowOID</td><td>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.</td></tr>
<tr><td>TrapOIDs</td><td>By default, this parameter is set to <i>all</i>, 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-</td></tr>
</table>

Parameters	Description
	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.
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
Traps count	Indicates the number of times this event was triggered during the last measurement period.	Number	Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Nimble storage RAIDs.

3.1.6 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of event that occurred on the target Nimble Storage.

Configurable parameters for the test

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>Test Period</td><td>How often should the test be executed.</td></tr>
<tr><td>Host</td><td>The host for which the test is to be configured.</td></tr>
<tr><td>Port</td><td>The port at which the specified Host listens. By default, this is <i>NULL</i>.</td></tr>
<tr><td>Source Address</td><td>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.</td></tr>
<tr><td>OID Value</td><td>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>
<p>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.</p>
<p>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*.</p>
<p>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</p></td></tr>
</table>

Parameters	Description
	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. In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be: Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any. Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.
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.
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.
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

Parameters	Description
	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
Temperature 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 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.

3.1.7 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of event that occurred on the target Nimble Storage.

Configurable parameters for the test

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>Test Period</td><td>How often should the test be executed.</td></tr>
<tr><td>Host</td><td>The host for which the test is to be configured.</td></tr>
<tr><td>Port</td><td>The port at which the specified Host listens. By default, this is <i>NULL</i>.</td></tr>
<tr><td>Source Address</td><td>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.</td></tr>
<tr><td>OID Value</td><td><p>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:</p>
<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>
<p>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.</p>
<p>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*.</p>
<p>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:</p></td></tr>
</table>

Parameters	Description
	Trap5: .1.3.6.1.4.1.9156.1.1.5-any. In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be: Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any. Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.
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.
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.
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
Controller 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 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.

3.2 The Nimble Volumes Layer

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

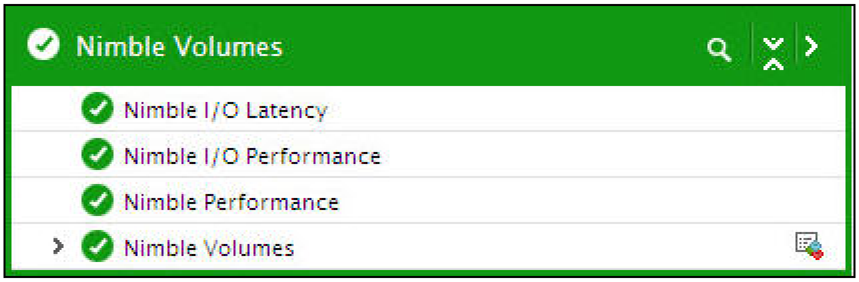


Figure 3.3: The tests mapped to the Nimble Volumes layer

3.2.1 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Nimble Storage that is to be 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 will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.

Parameter	Description
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Read latency	Indicates the average time taken to process the read operations during the last measurement period.	Secs	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.
Write latency	Indicates the average time taken to process the write operations during the last measurement period.	Secs	

3.2.2 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Nimble Storage that is to be 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 will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
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

Parameter	Description
	your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the

Parameter	Description
	Yes option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	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	IOPS	

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
Random write IOPS	Indicates the rate at which random I/O operations were written during the last measurement period.	IOPS	
Total IOPS	Indicates the total number of I/O operations performed per second.	IOPS	This measure is the total of *Sequential read IOPS, Sequential write IOPS, Random read IOPS* and *Random write IOPS* measures. The gradual increase in the value of this measure indicates a consistent rise of I/O load on the storage.
Total I/O reads	Indicates the total number of I/O operations that were read during the last measurement period.	Reads	
Total I/O writes	Indicates the total number of I/O operations that were written during the last measurement period.	Writes	Ideally, high value is desired for this measure.
Avg. I/O read latency	Indicates the average time taken to process each read operation during the last measurement period.	MilliSeconds	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.
Avg. I/O write latency	Indicates the average time taken to process each write operation during the last measurement period.	MilliSeconds	
Avg latency	Indicates the average time taken to process the total read and write operations	Milliseconds	This measure is the sum of *Avg. I/O read latency* and *Avg. I/O write latency* measures. Ideally, the value of this measure is preferred to be low. A high value of this measure indicates

Measurement	Description	Measurement Unit	Interpretation
			that the storage is taking more time to process the I/O operations.
Total IOPS	Indicates the total number of I/O operations performed per second.	IOPS	This measure is the total of Sequential read IOPS, Sequential write IOPS, Random read IOPS and Random write IOPS measures. The gradual increase in the value of this measure indicates a consistent rise of I/O load on the storage.

3.2.3 Nimble Throughput 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Nimble Storage that is to be 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 will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.

Parameter	Description
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 this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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:

Parameter	Description
	- **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	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	MB/Sec	

Measurement	Description	Measurement Unit	Interpretation
	random data is written during the last measurement period.		
Total throughputs	Indicates the total throughput of the Nimble storage.	MB/Sec	This measure is the sum of *Sequential read data, Sequential write data, Random read data* and *Random read data* measures. This measure is a good indicator of the I/O load on the storage.

3.2.4 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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for each volume of the Nimble Storage that is to be 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 will be *NULL*.

Parameter	Description
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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

Parameter	Description
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Is the volume online?	Indicates whether/not this volume is online.		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>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s 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</td><td>Indicates the total capacity of this volume.</td><td>TB</td><td></td></tr>
<tr><td>Used space</td><td>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>
<tr><td>Free space</td><td>Indicates the amount of spacec that is currently available for use in this volume.</td><td>TB</td><td>A high value is desired for this measure.</td></tr>
<tr><td>Space utilization</td><td>Indicates the percentage of space that is utilized in this volume.</td><td>Percent</td><td>A low value is desired for this measure.</td></tr>
<tr><td>Free space utilization</td><td>Indicates the percentage of space that is available for use in this volume.</td><td>Percent</td><td>A high value is desired for this measure.</td></tr>
<tr><td>iSCSI connections</td><td>Indicates the number of iSCSI connections established to this volume.</td><td>Number</td><td>This measure is a good indicator of the current workload on the volume.</td></tr>
</table>

3.2.5 Nimble Cache Test

Using this test, administrators can 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

Outputs of the test : One set of results for the target Nimble Storage that is to be 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 will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a

Parameter	Description
	contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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

Parameter	Description
	to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	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.

3.2.6 Nimble Disk Space Test

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

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Nimble Storage* as the desired **Component type**, set *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.

Target of the test : A Nimble Storage

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Nimble Storage that is to be 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 will be *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.

Parameter	**Description**
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.
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
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 this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3.**
Confirm Password	Confirm the AuthPass by retyping it here.
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
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG

Parameter	Description
	agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this 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
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
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 monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data used on disk for volumes	Indicates the amount of space used by the volumes on the storage array.	TB	
Data used on disk for snapshots	Indicates the amount of space used by the snapshots on the storage array.	TB	

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.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.