Monitoring Lefthand SAN Storage Cluster

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

HP LeftHand P4000 SAN Solutions deliver enterprise functionality that enhances virtual environments, simplifies management, and reduces costs. Easy to deploy, scale and maintain, HP P4000 SANs ensure that crucial business data remains available. The innovative approach to storage provides unique double fault protection across the entire SAN, reducing vulnerability without driving up costs the way traditional SANs can.

Failure of hardware components crucial to the functioning of the storage node of the storage cluster (such as voltage sensors, fans, power supply units etc.), abnormal state of the storage RAID, RAID controllers, and RAID Controller cache etc, minimal I/O processing capability of the volumes and drives, can significantly impact the performance of the storage system, thereby affecting the quality of the mission-critical services supported by the storage system. 24x7 monitoring of the storage system can greatly help in proactively identifying potential anomalies, and promptly averting them. This is where eG Enterprise helps administrators with two specialized monitoring models for *Lefthand SAN Node* and *Lefthand SAN Cluster*!

Chapter 2: How to Monitor Lefthand SAN Cluster Using eG Enterprise?

eG Enterprise monitors the Lefthand SAN Cluster in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. To start Lefthand SAN Cluster monitoring, first set the pre-requisites explained in the Pre-requisites for monitoring Lefthand SAN Storage Cluster, and then manage the Lefthand SAN Cluster component using the eG admin interface. The following sections explain how to set the pre-requisites and manage Lefthand SAN Cluster component.

2.1 Pre-requisites for monitoring Lefthand SAN Cluster

Before attempting to start monitoring the Lefthand SAN Cluster, you need to fulfill a set of pre-requisites to enable the eG agent to collect metrics from the target storage cluster. The eG agent uses the command-line interface (CLI), CLIQ, to communicate with the SAN cluster. CLIQ is the command-line interface (CLI) for the HP P4000 Storage Solution. To enable the communication between the eG agent and the cluster, do the following:

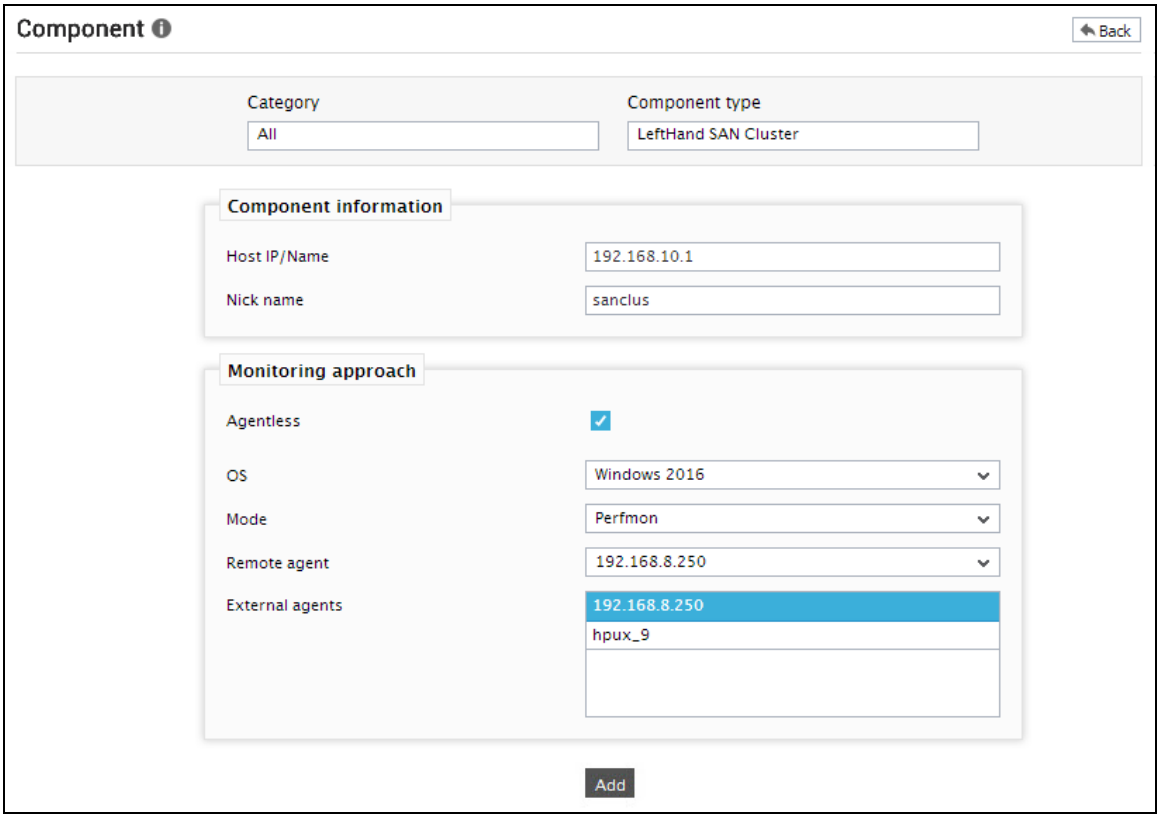
- Ensure that the CLIQ (**CLIQ.exe**) is installed on the host that communicates with the SAN cluster.
- Deploy the eG agent on the same host on which the CLIQ (**CLIQ.exe**) is installed.
- Then, configure the tests that use the CLIQ with the full path to the **CLIQ.exe** and the credentials of a user who can access the HP p4000 centralized management console and run the **CLIQ.exe**.

Once the above-said pre-requisites are fulfilled, manage the Lefthand SAN Cluster component using the steps provided in the section below.

2.2 Managing the Lefthand SAN Cluster

The eG Enterprise cannot automatically discover the Lefthand SAN Storage Cluster. 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 add a Lefthand SAN Node, 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 *LeftHand SAN Cluster* as the **Component type**. Then, click the **Add New Component** button. This will invoke Chapter 2.



Category: All

Component type: LeftHand SAN Cluster

Host IP/Name: 192.168.10.1

Nick name: sanclus

Agentless: ☑

OS: Windows 2016

Mode: Perfmon

Remote agent: 192.168.8.250

External agents: 192.168.8.250
hpux_9

Figure 2.1: Adding the LeftHand SAN Cluster component

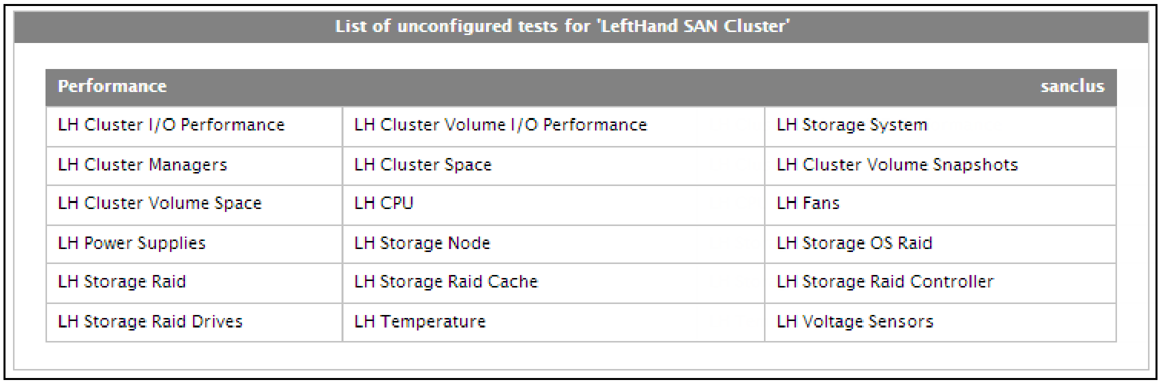
4. Specify the **Host IP/Name** and the **Nick name** for the LeftHand SAN Cluster component. Since the LeftHand SAN Cluster component is by default monitored in an agentless manner, the **Agentless** check box is selected by default.

5. Next, select the **OS** based on the operating system of the host on which the HP p4000 centralized management console is installed.
6. Choose the **Mode** for the selected OS.
7. Select the **Remote agent** that will be monitoring the target storage cluster.

8. Choose an external agent for the target storage system by picking an option from the **External agents** list box.

9. Then, click the **Add** button to register the changes (see Figure 2.1).

10. When you attempt to sign out, a list of unconfigured tests will be appear as shown in the below figure.



List of unconfigured tests for 'LeftHand SAN Cluster'

Performance		sanclus
LH Cluster I/O Performance	LH Cluster Volume I/O Performance	LH Storage System
LH Cluster Managers	LH Cluster Space	LH Cluster Volume Snapshots
LH Cluster Volume Space	LH CPU	LH Fans
LH Power Supplies	LH Storage Node	LH Storage OS Raid
LH Storage Raid	LH Storage Raid Cache	LH Storage Raid Controller
LH Storage Raid Drives	LH Temperature	LH Voltage Sensors

Figure 2.2: A list of unconfigured tests for Lefthand SAN Node

11. Click on the tests to configure. To know how to configure these tests, refer to the **Monitoring Lefthand SAN Cluster** chapter.

12. Finally, signout of the eG admin interface.

Chapter 3: Monitoring Lefthand SAN Cluster

eG Enterprise provides you with extensive monitoring capabilities for the Lefthand SAN Storage Cluster. A single eG agent is capable of monitoring the Lefthand SAN Storage Cluster. Every layer of the monitoring model is mapped to a wide variety of tests that a single agent executes and extracts loads of performance metrics from the Lefthand SAN Storage Cluster.

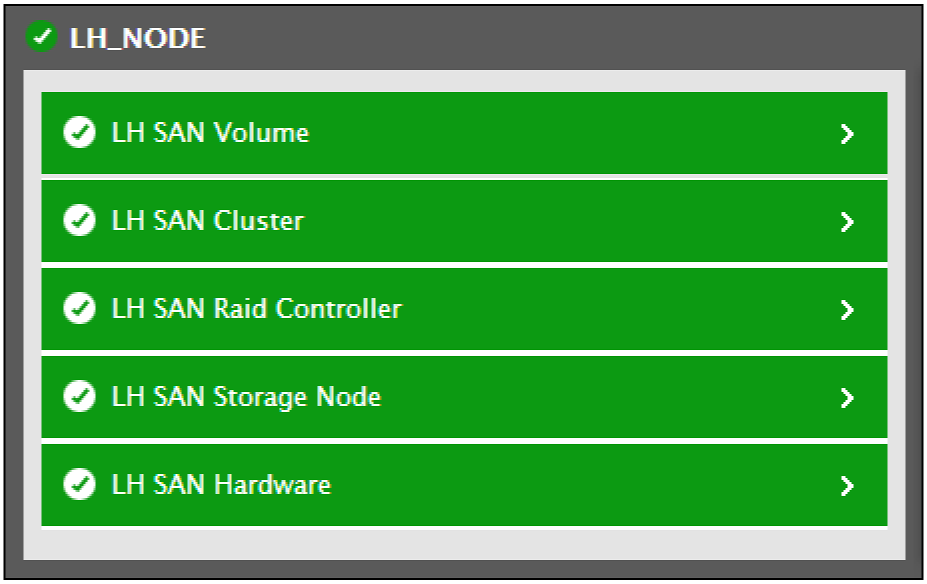


Figure 3.1: The layer model of Lefthand SAN Storage Cluster

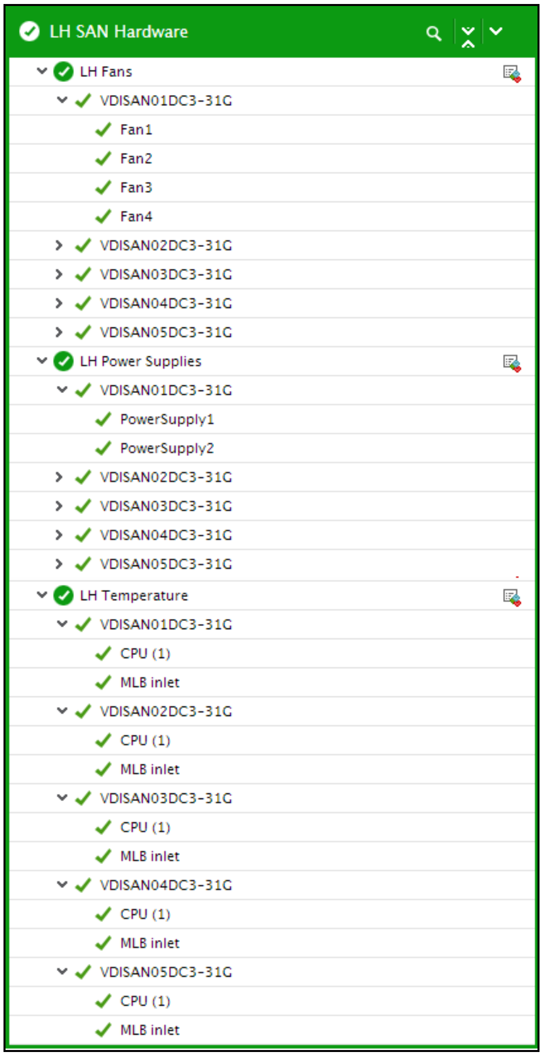
The metrics thus collected would be useful to figure out accurate answers to the following performance queries:

- What is the current status of cluster manager, storage node, Raid controller etc?
- Is the temperature of all the hardware components in admissible range?
- Are the fans in the storage system operating at normal speeds? Is any fan in an abnormal state?
- Are all power supply units in the storage cluster functioning smoothly, or has any unit in an abnormal state?
- What is the current temperature and fan speed of the CPU in each node?
- Is any storage cluster running out of space?
- How well the space on the storage node was utilized?
- Is there any node that is experiencing significant latencies during processing I/O operations?

- What is the total capacity of each volume on the cluster?
- What is the level of I/O traffic on each volume?
- Is the volume experiencing any read/write latencies?
- How well data was read from and written to each volume per second?
- Is the cache of any controller in abnormal state?
- What is the health of each raid controller?
- What is the operational status of the raid drive?
- What is the space utilization of snapshots on the storage cluster?
- What is the CPU and memory utilization of the cluster?
- How many I/O operations are in pending state on the cluster?
- How long the cluster took to complete the I/O operations?

3.1 The LH SAN Hardware Layer

The tests mapped to this layer measure the temperature of the CPU, status and operating speed of the fans, the status of the power supplies, the status and temperature of each hardware component, the status of the voltage sensor etc.



LH SAN Hardware

- ✓ LH Fans
  - ✓ VDISAN01DC3-31G
    - ✓ Fan1
    - ✓ Fan2
    - ✓ Fan3
    - ✓ Fan4
  - ✓ VDISAN02DC3-31G
  - ✓ VDISAN03DC3-31G
  - ✓ VDISAN04DC3-31G
  - ✓ VDISAN05DC3-31G
- ✓ LH Power Supplies
  - ✓ VDISAN01DC3-31G
    - ✓ PowerSupply1
    - ✓ PowerSupply2
  - ✓ VDISAN02DC3-31G
  - ✓ VDISAN03DC3-31G
  - ✓ VDISAN04DC3-31G
  - ✓ VDISAN05DC3-31G
- ✓ LH Temperature
  - ✓ VDISAN01DC3-31G
    - ✓ CPU (1)
    - ✓ MLB inlet
  - ✓ VDISAN02DC3-31G
    - ✓ CPU (1)
    - ✓ MLB inlet
  - ✓ VDISAN03DC3-31G
    - ✓ CPU (1)
    - ✓ MLB inlet
  - ✓ VDISAN04DC3-31G
    - ✓ CPU (1)
    - ✓ MLB inlet
  - ✓ VDISAN05DC3-31G
    - ✓ CPU (1)
    - ✓ MLB inlet

Figure 3.2: The tests mapped to the LH SAN Hardware layer

3.1.1 LH CPU Test

Optimal temperature of the CPU is key smooth functioning of the storage node. In other words, if the CPU of the storage node runs abnormally, then, it could cause I/O processing delays, abrupt shutdowns, etc which in turn could scar the user experience with the storage system. This is why, administrators should keep an eye on the temperature of the CPU and the fan speed of each CPU, so that abnormal temperature patterns can be detected proactively and treated, before end-users complain. This is where the **LH CPU** test helps. This test auto-discovers the CPUs of the target storage system and reports the current temperature and the speed of the fan on each CPU. In the process, the test points to those CPUs on which temperature and fan speed are abnormal.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *storage node:CPU* of the target storage system being monitored .

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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	Description
	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 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
Temperature	Indicates the current temperature of this CPU.	Celsius	Ideally, the value of this measure should be in permissible range. A sudden increase/decrease in the value of this measure may indicate an abnormal condition of the CPU.
Fan Speed	Indicates the current fan speed of this CPU.	Rpm	Ideally, the value of this measure should be within permissible range. A significant increase/decrease in the value of this measure may indicate severe damage to the fan.

3.1.2 LH Fans Test

If any of the fans in the storage node suddenly stops running, then, the temperature of the storage system hardware may soar, causing serious damage to the core components of the device. To avoid this, it is imperative to keep a vigil on the speed of the fan round the clock. The **LH Fans** test helps administrators achieve this!

This test auto-discovers the fans on the target storage system, and for each fan, reports the current status and speed. Using this test, administrators can identify the fan that is down and rectify the same well before the stack unit starts malfunctioning.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *storage node:fan* combination of the target storage cluster.

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.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this fan.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Abnormal</td><td>2</td></tr>
</table>
<b>Note:</b></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			This measure reports the **Measure Values** listed in the table above to indicate the current state of each fan. However, in the graph of this measure, the state is indicated using the **Numeric Values** listed in the above table.
Speed	Indicates that current operating speed of this fan.	Rpm	Ideally, the value of this measure should be within permissible range. A significant increase/decrease in the value of this measure may indicate severe damage to the fan.

3.1.3 LH Power Supplies Test

Often, sudden failure of the power supplies of storage nodes can cause the storage system to crash, leading to critical loss of data. To avoid this, you need to keep an eye on the state of each power supply unit. This can be achieved using the **LH Power supplies** test. This test auto-discovers the power supplies on the target storage system and reports the current state of each power supply. using this test, power supplies that are running abnormally can be detected with ease.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for every *storage node:power supply* of the target storage cluster.

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.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection

Parameter	Description
	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 node. 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

Parameter	Description
	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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this power supply.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Abnormal</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure</b></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			Values listed in the table above to indicate the current state of each power supply. However, in the graph of this measure, the state is indicated using the **Numeric Value**s listed in the above table.

3.1.4 LH Temperature Test

Abnormal temperature of the hardware components often lead to the malfunctioning of the storage system which when left unnoticed may affect the overall health. This test auto-discovers the hardware components in each storage node and for each hardware component, this test reports the current status and temperature. Using this test, administrators can determine the hardware components that were damaged.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *storage node: hardware component* combination on the storage cluster being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this hardware component.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Abnormal</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each hardware component. However, in the graph of this measure, the state is indicated using the <b>Numeric Value</b>s listed in the above table.</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Temperature	Indicates that current temperature of this hardware component.	Celsius	Ideally, the temperature should be well within admissible range. A sudden / gradual increase /decrease in the temperature is a cause of concern and warrants immediate attention of the administrator.

3.1.5 LH Voltage Sensors Test

For the target storage system to function without a glitch, it is essential for the hardware modules to function properly. If any of the hardware modules do not function as expected due to abnormal voltage fluctuations, then that particular module will shutdown automatically. If the modules shutdown frequently, then, the overall performance of the cluster may degrade drastically. To avoid this performance degradation, administrators should constantly keep a vigil on the voltage passing through each module. The **LH Voltage Sensors** test helps administrators in this regard!

This test auto-discovers the voltage sensors in the modules of the storage system and reports the current status of each voltage sensor.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *storage node:voltage sensor* combination of the storage cluster being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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.

Parameter	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage node. 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 **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

Parameter	Description
	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**.

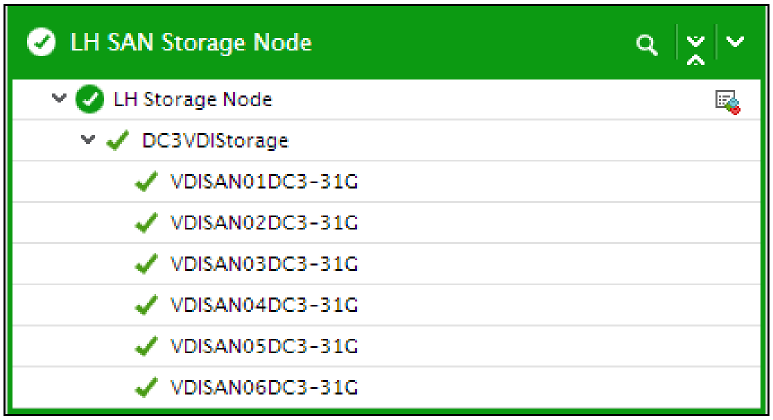
Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this voltage sensor.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Abnormal</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each voltage sensor. However, in the graph of this measure, the state is indicated</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			using only the **Numeric Value**s listed in the above table.

3.2 The LH SAN Storage Node Layer

Using the tests mapped to this layer, administrators can figure out the the current health, overall size, and the load- balancing capability of each storage node in the storage cluster. In addition, administrators can also figure out the idle CPU on the storage cluster and the memory utilized on the storage cluster.



LH SAN Storage Node
LH Storage Node
DC3VDIStorage
VDISAN01DC3-31G
VDISAN02DC3-31G
VDISAN03DC3-31G
VDISAN04DC3-31G
VDISAN05DC3-31G
VDISAN06DC3-31G

Figure 3.3: The tests mapped to the LH SAN Storage layer

3.2.1 LH Storage Node Test

This test auto-discovers the storage nodes on the storage cluster, and for each storage node, this test reports the current health, overall size, and the load-balancing capability of each storage node. With the help of this test, administrators can not only identify overloaded nodes, but can also predict the potential failure of the node, so that efforts can be undertaken to avert the same. In addition, the test also points administrators to the nodes that are handling more I/O requests than the rest, thus shedding light on irregularities in the distribution of I/O load across disks and prompting administrators to fine-tune the load-balancing algorithm.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for *storage node* on the target storage cluster.

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.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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

Parameter	Description
	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
Status	Indicates the current health of this storage node.		The values that this measure can report and the numeric values that correspond to them are listed 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>Up</td><td>1</td></tr><tr><td>Down</td><td>2</td></tr></table><b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current health of this storage node. However, in the graph of this measure, the state is indicated using only the <b>Numeric Values</b> listed in the above table.</td></tr>
<tr><td>Storage condition</td><td>Indicates the current storage condition of this storage node.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>NotReady</td><td>1</td></tr><tr><td>Unoperable</td><td>2</td></tr><tr><td>Overloaded</td><td>3</td></tr><tr><td>Ready</td><td>4</td></tr></table><b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current storage condition of this storage node. However, in the graph of this measure, the state is indicated using only the <b>Numeric Values</b> listed in the above table.</td></tr>
<tr><td>Total space</td><td>Indicates the total size of this storage node.</td><td>GB</td><td></td></tr>
<tr><td>Provisioned space</td><td>Indicates the space</td><td>GB</td><td></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	(allocated) provisioned for this storage node.		
Used space	Indicates the space that was already utilized in this storage node.	GB	A low value is desired for this measure. If the value of this measure is close to the Total space measure, then, it indicates that the storage node is running out of space. Administrators should therefore, free up the space in the storage node or allocate additional resources to the storage node.
Free space	Indicates the space that is currently available for use in this storage node.	GB	A high value is desired for this measure.
Space utilization	Indicates the space utilized in this storage node.	Percent	A low value is desired for this measure.
Allocated space used	Indicates the percentage of space that is utilized from the provisioned space of this storage node.	Percent	
Free space pct	Indicates the percentage of space that is available for use in this storage node.	Percent	
Allocated free space	Indicates the percentage of space that is available for use from the provisioned space of this storage node.	Percent	
I/O read rate	Indicates the rate at which read operations were performed on this storage node during the last measurement period.	Operations/Sec	Compare the value of this measure across storage nodes to know which node handled the maximum number of I/O read operations and which handled the least. If the gap

Measurement	Description	Measurement Unit	Interpretation
			between the two is very high, then it indicates serious irregularities in loadbalancing across storage nodes.
I/O write rate	Indicates the rate at which write operations were performed on this storage node during the last measurement period.	Operations/Sec	Compare the value of this measure across storage nodes to know which node handled the maximum number of I/O write operations and which handled the least. If the gap between the two is very high, then it indicates serious irregularities in loadbalancing across storage nodes.
Data read rate	Indicates the rate at which data was read from this storage node during the last measurement period.	MB/sec	Compare the value of these measures across storage nodes to identify the slowest node in terms of servicing read and write requests (respectively).
Data write rate	Indicates the rate at which data was written to this storage nod during the last measurement period.	MB/sec	
Pending I/O operations	Indicates the I/O operations that were pending on this storage node during the last measurement period.	Operations/Sec	A consistent increase in this value indicates a potential processing bottleneck with the storage node.
Read latency	Indicates the time taken to complete the read operations from this storage node during the last measurement period.	Millisecs	
Write latency	Indicates the time taken to complete the write operations on this storage node during the last	Millisecs	

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
I/O latency	Indicates the time taken to complete the read and write operations on this storage node during the last measurement period.	Millisecs	Ideally, this value should be low. If not, it implies that the storage node is slow.

3.2.2 LH Storage System Test

This test reveals the following critical statistics for the cluster:

- CPU and memory utilization;
- the rate at which the read and write operations were performed on the cluster;
- the rate at which the I/O operations were in pending state;
- the time taken by the cluster to complete I/O operations.

Using these metrics, administrators can find out any abnormalities, if any, on the cluster at early stage and prevent the occurrence of processing bottlenecks before anything untoward happens.

Target of the test : A Lefthand SAN Cluster

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the storage cluster being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the host is listening.
CLI Path	The eG agent uses the command-line interface, **CLIQ.exe**, to communicate with and monitor the storage cluster. To enable the eG agent to invoke the CLI, configure the full path to the CLI in the CLI Path text box.
Username and	Specify the credentials of a user who can execute the CLIQ.exe on the host that is

Parameter	Description
Password	connected with the storage cluster in the Username and Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Timeout	Specify the duration (in seconds) beyond which the test will timeout in the Timeout text box. The default value is 60 seconds.

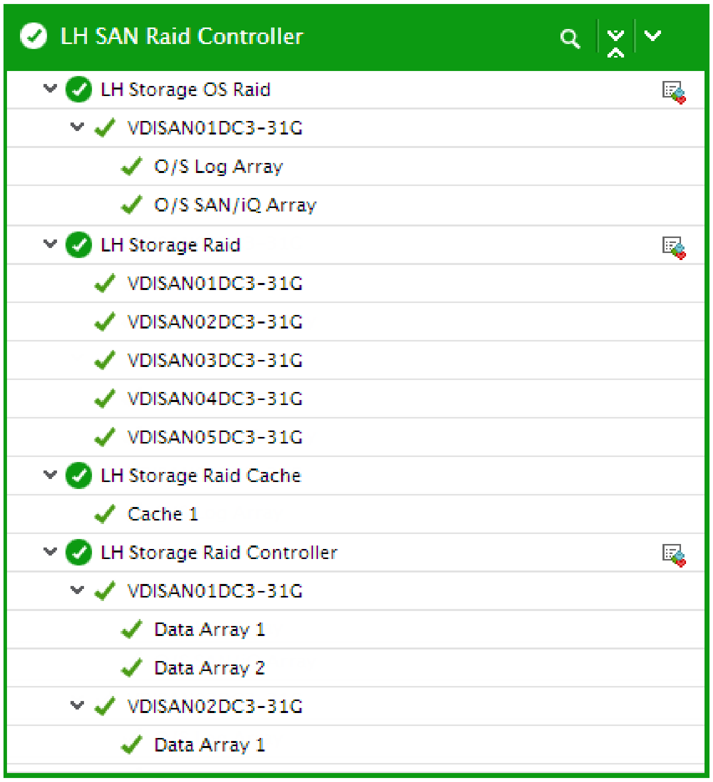
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU busy	Indicates the percentage of CPU utilized by the storage cluster.	Percent	
CPU idle	Indicates the percentage of CPU that is idle on the storage cluster.	Percent	
Memory utilization	Indicates the percentage of memory utilized for the storage cluster.	Percent	A low value is preferred for this measure. A high value of this measure indicates a potential space crunch on the cluster.
I/O read rate	Indicates the rate at which read I/O operations were performed on the storage cluster during the last measurement period.	Operations/sec	
I/O write rate	Indicates the rate at which write I/O operations were performed on the storage cluster during the last measurement period.	Operations/sec	
Total I/O	Indicates the total read and write I/O operations that were performed on the storage cluster during the last measurement period.	Operations/sec	
Data read rate	Indicates the rate at which data was read from the	MB/sec	

Measurement	Description	Measurement Unit	Interpretation
	storage cluster.		
Data write rate	Indicates the rate at which data was written to the storage cluster.	MB/sec	
Data processed	Indicates the rate at which data was read from and written to the storage cluster.	MB/sec	
Pending I/O operations	Indicates the rate at which I/O operations were pending on the storage cluster during the last measurement period.	Operations/sec	A low value of preferred for this measure. A high value indicates the processing bottle neck on the cluster.
Read latency	Indicates the time taken to complete read I/O operations on the storage cluster.	Millisec	The values of these measure should be very low. High values indicate that the cluster is taking more time to complete the I/O operations, which may degrade the performance of the cluster.
Write latency	Indicates the time taken to complete write I/O operations on the storage cluster.	Millisec	

3.3 The LH SAN Raid Controller Layer

This layer helps administrators track the current status and size of each OS Raid, the status of each storage RAID and the size of the RAID, the current status of the controller cache, the number of disks in each storage RAID, the status and size of each drive etc.



LH SAN Raid Controller

- ✓ LH Storage OS Raid
  - ✓ VDISAN01DC3-31G
    - ✓ O/S Log Array
    - ✓ O/S SAN/iQ Array
- ✓ LH Storage Raid
  - ✓ VDISAN01DC3-31G
  - ✓ VDISAN02DC3-31G
  - ✓ VDISAN03DC3-31G
  - ✓ VDISAN04DC3-31G
  - ✓ VDISAN05DC3-31G
- ✓ LH Storage Raid Cache
  - ✓ Cache 1
- ✓ LH Storage Raid Controller
  - ✓ VDISAN01DC3-31G
    - ✓ Data Array 1
    - ✓ Data Array 2
  - ✓ VDISAN02DC3-31G
    - ✓ Data Array 1

Figure 3.4: The tests mapped to the LH SAN Raid Controller layer

3.3.1 LH Storage OS Raid Test

The disks in Lefthand SAN Storage are automatically protected with RAID (RAID 10, RAID 5, or RAID 0). This test monitors this protective shield by periodically checking the status of the RAID on each storage node, and promptly reporting RAID failures. This test also reports the current size of each RAID.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for the *storage node:OS Raid* of the target storage cluster being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.

Parameter	Description
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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

Parameter	Description
	- **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
OS raid status	Indicates the current status of this OS Raid.		The values that this measure can report and the numeric values that correspond to them are listed 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>Normal</td><td>100</td></tr><tr><td>Rebuilding</td><td>1</td></tr><tr><td>Degraded</td><td>0</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each OS Raid array. However, in the graph of this measure, the state is indicated using only the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td>OS raid capacity</td><td>Indicates the total size of this OS Raid.</td><td>KB</td><td></td></tr>
</table>

3.3.2 LH Storage Raid Test

RAID is critical to the operation of the storage system. If RAID has not been configured, the storage system cannot be used. The disks in Lefthand SAN Storage are automatically protected with RAID (RAID 10, RAID 5, or RAID 0). This test monitors this protective shield by periodically checking the status of the RAID on each storage node, and promptly reporting RAID failures. This test also reports the current size of each RAID.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each storage node on the target storage system being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.

Parameter	Description
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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:

Parameter	Description
	- **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
Raid status	Indicates the current status of this storage node.		The values that this measure can report and the numeric values that correspond to them are listed 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>Normal</td><td>1</td></tr><tr><td>Abnormal</td><td>2</td></tr></table><b>Note:</b>
This measure reports the <b>Measure Values</b> listed in the table above to indicate the current state of each storage node. However, in the graph of this measure, the state is indicated using only the <b>Numeric Values</b> listed in the above table.</td></tr>
<tr><td>Raid capacity</td><td>Indicates the size of this storage node.</td><td>GB</td><td></td></tr>
</table>

3.3.3 LH Storage Raid Cache Test

Each SAN storage array is composed of disk/RAID controllers with caches. Cache memory in the disk/storage RAID controller enhances read and write performance, improving overall storage throughput. Streaming data can be queued into the cache to dramatically accelerate read performance. This test monitors each disk controller cache in the storage system and reports its size and status.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each cache of the storage controller on the target storage system.

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.

Parameter	Description
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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

Parameter	Description
	- **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
Controller cache status	Indicates the current status of this cache.		The values that this measure can report and the numeric values that correspond to them are listed below: **Measure Value** – **Numeric Value** Normal – 1 Abnormal – 2

Measurement	Description	Measurement Unit	Interpretation
			Note: This measure reports the **Measure Value**s listed in the table above to indicate the current state of each cache. However, in the graph of this measure, the state is indicated using only the **Numeric Value**s listed in the above table.
Controller cache size	Indicates the size of this cache.	KB	

3.3.4 LH Storage Raid Controller Test

This test auto-discovers the Raid Controllers and for each Raid controller, reports the current state, the size of the RAID controller and the number of disks. With the help of this test, administrators can be proactively alerted to potential controller failures / slowdowns.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *storage node:Raid Controller* combination on the target storage system.

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.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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.

Parameter	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage node. 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 **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

Parameter	Description
	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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Controller status</td><td>Indicates the current status of this raid controller.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Abnormal</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each raid controller. However, in the graph of this measure, the state is indicated using</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			only the **Numeric Value**s listed in the above table.
Controller capacity	Indicates the size of this raid controller.	GB	
Disks	Indicates the number of disks on this raid controller.	Number	

3.3.5 LH Storage Raid Drives Test

This test auto-discovers the drives on each storage node of the target storage cluster and for each drive, reports the current state, size and temperature. This test also reports the temperature status of each drive. With the help of this test, administrators can not only identify faulty drives, but can also predict the potential failure of a drive, so that efforts can be undertaken to avert the same.

Target of the test : A Lefthand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *storage node:Drive* combination on the target storage system being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion

Parameter	Description
	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 **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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Status</td><td>Indicates the current status of this drive.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Abnormal</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current state of each drive. However, in the graph of this measure, the state is indicated using only the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td>Mode</td><td>Indicates the current</td><td></td><td>The values that this measure can report</td></tr>
</table>

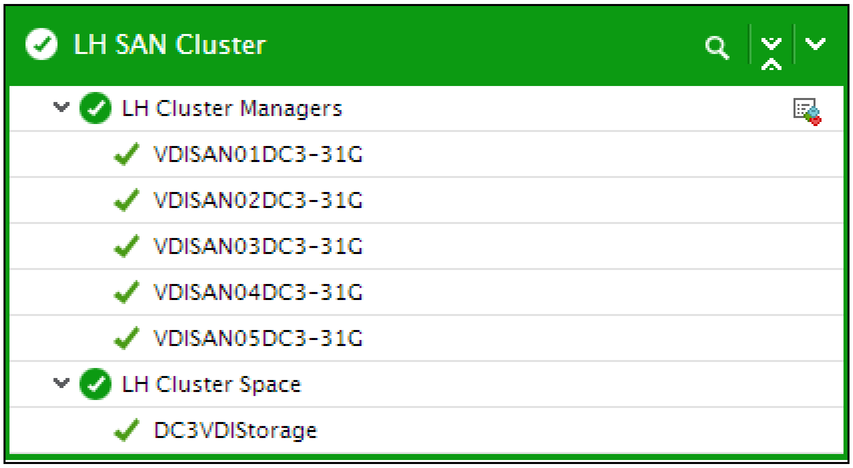
<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>operational state of this drive.</td><td></td><td>and the numeric values that correspond to them are listed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Active</td><td>100</td></tr><tr><td>Inactive</td><td>0</td></tr><tr><td>Hot Spare</td><td>1</td></tr><tr><td>Rebuilding</td><td>2</td></tr><tr><td>Uninitialized</td><td>3</td></tr><tr><td>Foreign</td><td>4</td></tr><tr><td>Off or removed</td><td>5</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current operational state of each drive. However, in the graph of this measure, the state is indicated using only the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td>Capacity</td><td>Indicates the total size of this drive.</td><td>GB</td><td></td></tr>
<tr><td>Temperature status</td><td>Indicates the current temperature state of this drive.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Normal</td><td>1</td></tr><tr><td>Abnormal</td><td>2</td></tr></table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current temperature state of each drive. However, in the graph of</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			this measure, the state is indicated using only the **Numeric Value**s listed in the above table.
Temperature	Indicates the current temperature of this drive.	Celsius	Ideally, the value of this measure should be well within admissible range. An abnormal temperature may result in the damage of the drive.

3.4 The LH SAN Cluster Layer

The tests mapped to this layer helps administrators to determine the following:

- the space utilization of each cluster;
- the current state of each cluster manager and whether the cluster manager is a failover manager or not;
- the cluster utilization;
- the I/O processing capability of the cluster manager etc;



LH SAN Cluster

LH Cluster Managers

✓ VDISAN01DC3-31G

✓ VDISAN02DC3-31G

✓ VDISAN03DC3-31G

✓ VDISAN04DC3-31G

✓ VDISAN05DC3-31G

LH Cluster Space

✓ DC3VDIStorage

Figure 3.5: The tests mapped to the LH SAN Cluster layer

3.4.1 LH Cluster Space Test

This test reports the space utilization of the storage cluster, and also reveals the number of the volumes and storage nodes on the storage cluster. This way, administrators are proactively alerted to potential space crunch on the storage cluster.

Target of the test : A LeftHand SAN Cluster

Agent deploying the test : An external agent

Outputs of the test : One set of results for the storage cluster being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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*.

Parameter	Description
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 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
Total space	Indicates the total size of the cluster.	GB	
Provisioned space	Indicates the space provisioned for the cluster while created.	GB	
Used space	Indicates the space that was already utilized on the cluster.	GB	
Free space	Indicates the space that is available for use in the cluster.	GB	
Space utilization	Indicates the percentage of space that is utilized in the cluster.	Percent	A high value for this measure indicates that the cluster is currently running out of space. Administrators can either clear unwanted data on the cluster or add additional resources.
Allocated space used	Indicates the percentage of space already utilized from this cluster against the allocated space for the cluster.	Percent	
Free space pct	Indicates the percentage of space that is available for use in this cluster.	Percent	
Allocated free space	Indicates the percentage of space that is available for use from the cluster against the allocated space.	Percent	
Volume count	Indicates the number of volumes created on the cluster.	Number	
Module count	Indicates the number of storage nodes in the cluster.	Number	

3.4.2 LH Cluster Managers Test

Within a management group, managers are storage systems that govern the activity of all of the storage systems in the group. The Failover Manager is a specialized version of the LeftHand OS software designed to operate as a manager and provide automated failover capability. In a cluster set up, administrators may often want to figure out the state of each manager and determine whether the manager is a failover manager or not. For this, administrators can use the **LH Cluster Managers** test.

This test auto-discovers the cluster managers in the target storage cluster and for each cluster manager, this test reports the current state. This test also helps administrators determine whether the cluster manager is a failover manager or not.

Target of the test : A LeftHand SAN Cluster

Agent deploying the test : An external agent

Outputs of the test : One set of results for each cluster manager on the target LeftHand SAN Cluster being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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

Parameter	Description
	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: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.

Parameter	Description
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Manager status</td><td>Indicates the current status of this cluster manager.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Up</td><td>1</td></tr>
<tr><td>Down</td><td>2</td></tr>
</table>
<b>Note:</b>
This measure reports the <b>Measure Value</b>s listed in the table above to indicate the current status of this cluster manager. However, in the graph of this measure, the state is indicated using only the <b>Numeric Value</b>s listed in the above table.</td></tr>
<tr><td>Is failover manager</td><td>Indicates whether/not this cluster manager is a failover manager.</td><td></td><td>The values that this measure can report and the numeric values that correspond to them are listed below:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Yes</td><td>1</td></tr><tr><td>No</td><td>0</td></tr></table><p><b>Note:</b></p><p>This measure reports the <b>Measure Values</b> listed in the table above to indicate whether/not this cluster manager is a failover manager. However, in the graph of this measure, the state is indicated using only the <b>Numeric Values</b> listed in the above table.</p></td></tr>
</table>

3.4.3 LH Cluster I/O Performance Test

This test auto-discovers the volumes in each storage cluster of the target storage system and reports how well each volume handles the I/O requests it receives. In addition, this test reveals the time taken to complete read and write operations on each volume. This way, the test turns the spotlight on volumes that are experiencing a slowdown and also reveals what is causing the slowdown – load-balancing irregularities across volumes or poor I/O processing capability?

Target of the test : A Lefthand SAN Cluster

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the *Storage cluster* being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the host is listening.
CLI Path	The eG agent uses the command-line interface, **CLIQ.exe**, to communicate with and

Parameter	Description
	monitor the storage cluster. To enable the eG agent to invoke the CLI, configure the full path to the CLI in the CLI Path text box.
Username and Password	Specify the credentials of a user who can execute the **CLIQ.exe** on the host that is connected with the storage cluster in the Username and Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Timeout	Specify the duration (in seconds) beyond which the test will timeout in the Timeout text box. The default value is 60 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
I/O read rate	Indicates the rate at which read I/O operations were performed on this cluster during the last measurement period.	Operations/sec	
I/O write rate	Indicates the rate at which write I/O operations were performed on this cluster during the last measurement period.	Operations/sec	
Total I/O	Indicates the total read and write I/O operations performed on this cluster during the last measurement period.	Operations/sec	This measure serves as a good indicator of the I/O processing ability of the cluster. A consistent drop in this value is hence a cause for concern, as it indicates a processing slowdown.
Data read rate	Indicates the rate at which data was read from this cluster.	MB/sec	Comparing the value of these measures across the clusters will clearly indicate which cluster is the busiest in terms of the rate at which data is read and written - it could also shed light on irregularities in load balancing across the clusters.
Data write rate	Indicates the rate at which data was written to this cluster.	MB/sec	

Measurement	Description	Measurement Unit	Interpretation
Data processed	Indicates the overall rate at which data was read from and written to this cluster.	MB/sec	
Pending read operations	Indicates the rate at which read I/O operations were pending on this cluster during the last measurement period.	Operations/sec	
Pending write operations	Indicates the rate at which write operations were pending on this cluster during the last measurement period.	Operations/sec	
Pending I/O operations	Indicates the overall rate at which read and write I/O operations were pending on this cluster during the last measurement period.	Operations/sec	
Read latency	Indicates the time taken to complete the read I/O operations on this cluster.	Millisec	
Write latency	Indicates the time taken to complete the write I/O operations on this cluster.	Millisec	
Read Cache hits	Indicates the rate which read operations were serviced from the cache of this cluster.	Operations/sec	Ideally, the value of this measure should be high. A consistent drop in cache hits and a steady increase in cache misses during the same time frame is indicative of ineffective read cache usage, which can lead to a slowness in read request servicing.

3.5 The LH SAN Volume Layer

This layer tracks the status of each volume, the space utilization of each volume snapshot, the I/O processing capability of each volume.

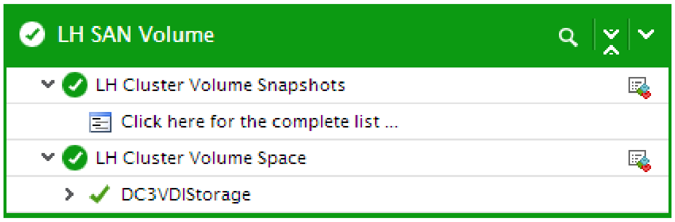

LH SAN Volume
LH Cluster Volume Snapshots
Click here for the complete list ...
LH Cluster Volume Space
DC3VDIStorage

Figure 3.6: The tests mapped to the LH SAN Volume layer

3.5.1 LH Cluster Volume Space Test

A volume is a logical subdivision in a storage cluster. If a single volume in the Lefthand storage cluster is running out of space, it can rupture the user experience with the entire storage cluster. Therefore, it is necessary to monitor the space utilization of the volumes round the clock! The **LH Cluster Volume Space** test helps you in this regard!

This test auto-discovers the volumes in the storage cluster and reports the space utilization of each volume. By closely monitoring the volumes, administrators can figure out whether/not any volume has been grossly over- utilized. This way, the test turns the spotlight on volumes that are experiencing potential space crunch.

Target of the test : A LeftHand SAN Node

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *volume* on the target storage cluster.

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.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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
Total space	Indicates the total size of this volume.	GB	
Provisioned space	Indicates the space provisioned for this volume while created.	GB	
Used space	Indicates the space that was already utilized on this volume.	GB	A low value is desired for this measure. Compare the value of this measure across volumes to determine the volume that is utilizing the maximum space.
Free space	Indicates the space that is	GB	A high value is desired for this

Measurement	Description	Measurement Unit	Interpretation
	available for use in this volume.		measure.
Volume space utilization	Indicates the percentage of space that is utilized in this volume.	Percent	A high value for this measure indicates that the volume is currently running out of space. Administrators can either clear unwanted data on the volume or add additional resources.
Allocated space used	Indicates the percentage of space already utilized from this volume against the allocated space for this volume.	Percent	
Free space pct	Indicates the percentage of space that is available for use in this volume.	Percent	A high value is desired for this measure. A value close to *0* is a cause of concern.
Allocated free space	Indicates the percentage of space that is available for use from this volume against the allocated space.	Percent	
Cluster space used by volume	Indicates the percentage of space utilized by this volume on the storage cluster.	Percent	

3.5.2 LH Cluster Volume I/O Performance Test

This test auto-discovers the volumes in the target storage cluster and reports how well each volume handles the I/O requests it receives. In addition, this test reveals the time taken to complete read and write operations on each volume. This way, the test turns the spotlight on volumes that are experiencing a slowdown and also reveals what is causing the slowdown – load-balancing irregularities across volumes or poor I/O processing capability?

Target of the test : A LeftHand SAN Cluster

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the volume on the target storage cluster.

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 host is listening.
CLI Path	The eG agent uses the command-line interface, **CLIQ.exe**, to communicate with and monitor the storage cluster. To enable the eG agent to invoke the CLI, configure the full path to the CLI in the CLI Path text box.
Username and Password	Specify the credentials of a user who can execute the CLIQ.exe on the host that is connected with the storage cluster in the Username and Password text boxes.
Confirm Password	Confirm the password by retyping it here.
Timeout	Specify the duration (in seconds) beyond which the test will timeout in the Timeout text box. The default value is 60 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
I/O read rate	Indicates the rate at which read I/O operations were performed on this volume during the last measurement period.	Operations/sec	Ideally, the value of this measure should be high. A steady dip in this measure value could indicate a potential reading bottleneck.
I/O write rate	Indicates the rate at which write I/O operations were performed on this volume during the last measurement period.	Operations/sec	
Total I/O	Indicates the total read and write I/O operations performed on this volume during the last measurement period.	Operations/sec	This measure serves as a good indicator of the I/O processing ability of the volume. A consistent drop in this value is hence a cause for concern, as it indicates a processing slowdown.
Data read rate	Indicates the rate at which data was read from this	MB/sec	Comparing the value of these

Measurement	Description	Measurement Unit	Interpretation
	volume.		measures across the volumes will clearly indicate which volume is the busiest in terms of the rate at which data is read and written - it could also shed light on irregularities in load balancing across the volumes.
Data write rate	Indicates the rate at which data was written to this volume.	MB/sec	
Data processed	Indicates the overall rate at which data was read from and written to this volume.	MB/sec	
Pending read operations	Indicates the rate at which read I/O operations were pending on this volume during the last measurement period.	Operations/sec	
Pending write operations	Indicates the rate at which write operations were pending on this volume during the last measurement period.	Operations/sec	
Pending I/O operations	Indicates the overall rate at which read and write I/O operations were pending on this volume during the last measurement period.	Operations/sec	
Read latency	Indicates the time taken to complete the read I/O operations on this volume.	Millisec	
Write latency	Indicates the time taken to complete the write I/O operations on this volume.	Millisec	
Read Cache hits	Indicates the rate which read operations were serviced from the cache of this volume.	Operations/sec	Ideally, the value of this measure should be high. A consistent drop in cache hits and a steady increase in cache misses during the same time frame is indicative of ineffective read cache usage, which can lead to a slowness in read request servicing.

3.5.3 LH Cluster Volume Snapshots Test

This test auto-discovers the snapshots on each volume of the target storage cluster and helps administrators to figure out the snapshot that is busy processing I/O requests, detect irregularities in the distribution of I/O load across the snapshots. In addition, using this test, administrators can analyze the space utilization of each snapshot and thus figure out the snapshots that are running out of space.

Target of the test : A LeftHand SAN Cluster

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *volume:snapshot* combination on the target storage cluster.

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.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value 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 node. 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.

Parameter	Description
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, 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 the EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
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.

Parameter	Description
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
Total space	Indicates the total size of this snapshot.	GB	
Provisioned space	Indicates the space provisioned for this snapshot while created.	GB	
Used space	Indicates the space that was already utilized on this snapshot.	GB	
Free space	Indicates the space that is available for use in this snapshot.	GB	
Snapshot space utilization	Indicates the percentage of space that is utilized in this snapshot.	Percent	A high value for this measure indicates that the snapshot is currently running out of space. Administrators can either clear unwanted data on the snapshot or add additional resources.
Allocated space used	Indicates the percentage of space already utilized from this snapshot against the allocated space for this snapshot.	Percent	
Free space pct	Indicates the percentage of space that is available for use in this volume.	Percent	

Measurement	Description	Measurement Unit	Interpretation
Allocated free space	Indicates the percentage of space that is available for use from this snapshot against the allocated space.	Percent	
Cluster space used by snapshot	Indicates the percentage of space utilized by this snapshot on the storage cluster.	Percent	
I/O read rate	Indicates the rate at which read I/O operations were performed on this snapshot during the last measurement period.	Operations/sec	
I/O write rate	Indicates the rate at which write I/O operations were performed on this snapshot during the last measurement period.	Operations/sec	
Data read rate	Indicates the rate at which data was read from this snapshot during the last measurement period.	MB/sec	
Data Write rate	Indicates the rate at which data was written to this snapshot during the last measurement period.	MB/sec	
Pending read operations	Indicates the rate at which read operations were pending on this snapshot during the last measurement period.	Operations/sec	
Pending write operations	Indicates the rate at which write operations were pending on this snapshot during the last	Operations/sec	

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
Read latency	Indicates the time taken to complete read operations on this snapshot.	MilliSecs	
Write latency	Indicates the time taken to complete write operations on this snapshot.	MilliSecs	
Read cache hits	Indicates the rate at which cache of this snapshot was read during the last measurement period.	Operations/sec	

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.