Monitoring EMC Isilon Storage System

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Dell EMC Isilon scale -out storage system contains the hardware base on which OneFS operating system executes. OneFS works exclusively with the Isilon scale-out storage system, referred to as a “cluster”. The cluster is architected with a wide variety of node styles and capacities, in order to meet the needs of a varied data set and wide spectrum of workloads. OneFS automatically divides the content and allocates the content to different storage nodes in parallel via the private Ethernet or InfiniBand network, which eliminates unnecessary network traffic. The Isilon cluster is managed as a single file system and the coordination and data distribution are completely transparent to end- user clients. This ability to automatically distribute data across multiple nodes in a transparent manner is fundamental for the ability of OneFS to enable growth, next -generation data protection, and extreme performance.

With the Isilon storage system, organizations can optimally scale-up their environment based on the growing needs, and administrators can easily manage the resource allocation to the environment without any glitch and down time. Therefore, insufficient resources in cluster, unavailability of nodes or failure detected in the hardware such as power sensor, fan, etc. may result in the loss of huge amount of data. Anything that renders the data inaccessible or delays access to data, such as a disk failure, a low throughput or an I/O overload, can be disastrous to these mission- critical IT environments. This is why, it is important that the storage system should be continuously monitored for performance flaws – both small or big! This is where eG Enterprise helps storage administrators.

Chapter 2: How to Monitor EMC Isilon Storage System Using eG Enterprise ?

eG Enterprise monitors the EMC Isilon Storage System using a remote agent on any Windows host in the environment. This agent is capable of monitoring the performance of the storage system in the following ways:

- By polling the SNMP MIB of the target storage system;
- By connecting to the storage system via SSH and running CLI commands;

To enable the eG agent to use the aforesaid methodologies, a set of pre-requisites should be fulfilled. These requirements have been discussed in the following section.

2.1 Pre-requisites for Monitoring the EMC Isilon Storage System

To enable the eG external agent to collect performance metrics from the target storage system, the following pre-requisites should be fulfilled:

1. The target storage system should be SNMP-enabled.
2. The eG agent should be able to access the target storage system over the network.
3. The eG agent should be able to communicate with the target storage system via SSH. For this, specify the SSH port (default port: 22) while configuring the *EMC Isilon Storage* component for monitoring and ensure that the SSH port is opened on the firewall (if any) between the agent and the target storage system.
4. Configure the credentials of a root user who can access the target storage system via SSH. In high security environments, administrators may not want to expose the credentials of the root user. In such cases, you can create a sudo user with the privileges of accessing the target storage system and then, execute the CLI commands via SSH. To achieve this, do the following:
   - Edit the **SUDOERS** file on the target storage system and append an entry of the following format:

     <eG_agent_install_user> ALL=(ALL) NOPASSWD:<Command_with_path>

   - For instance, if the eG agent install user is EG_Monitor, then the entries in the **SUDOERS** file should be:

     EG_Monitor ALL=(ALL) NOPASSWD: /usr/bin/isi ALL

The above-mentioned entry indicates that the eG install user will have permissions to run all the commands on the storage system like the root user.

- Sometimes, administrators may want to restrict the privileges of the sudo user to run the commands specific to monitor the target storage system. In this case, specify the commands mentioned below:

  *EG_Monitor ALL=(ALL) NOPASSWD: /usr/bin/isi status**

  *EG_Monitor ALL=(ALL) NOPASSWD: /usr/bin/isi statistics**

  EG_Monitor ALL=(ALL) NOPASSWD: /usr/bin/isi dedupe stats

  *EG_Monitor ALL=(ALL) NOPASSWD: /usr/bin/isi storagepool**

  EG_Monitor ALL=(ALL) NOPASSWD: /usr/bin/isi version

  For example, if you specify the following command alone, then, you will be allowed to run the commands that retrieve the status of the hardware/logical components of the storage system.

  *EG_Monitor ALL=(ALL) NOPASSWD: /usr/bin/isi status**

  Similarly specifying the other commands mentioned above will help you to run the commands that retrieve the relevant statistics of your interest.

- Finally, save the file.

Now, provide the credentials of the sudo user while configuring the *EMC Isilon Storage* component for monitoring. To enable the eG agent to use the sudo user to run the CLI commands, set the **Use Sudo** flag to **'Yes'** in the test configuration page.

Once the above-said pre-requisites are fulfilled, manage the EMC Isilon Storage component using the eG admin interface. The steps for achieving this are discussed in the Section **2.2**.

2.2 Managing the EMC Isilon Storage System

eG Enterprise can automatically discover the EMC Isilon storage system, and also lets you to manually add the component for monitoring. To manage an EMC Isilon Storage component, do the following:

1. Log into the eG administrative interface.
2. If the EMC Isilon storage system is already discovered, then directly proceed towards managing it using the **COMPONENTS – MANAGE/UNMANAGE** page.
3. However, if it is yet to be discovered, then run discovery (Infrastructure -> Components -> Discover) to get it discovered or follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu to manually add the component using the **COMPONENTS** page. Remember that components manually added are managed automatically.
4. In the **COMPONENT** page that appears next, select *EMC Isilon Storage* as the **Component type**. Then, click the **Add New Component** button. This will invoke 2.2.

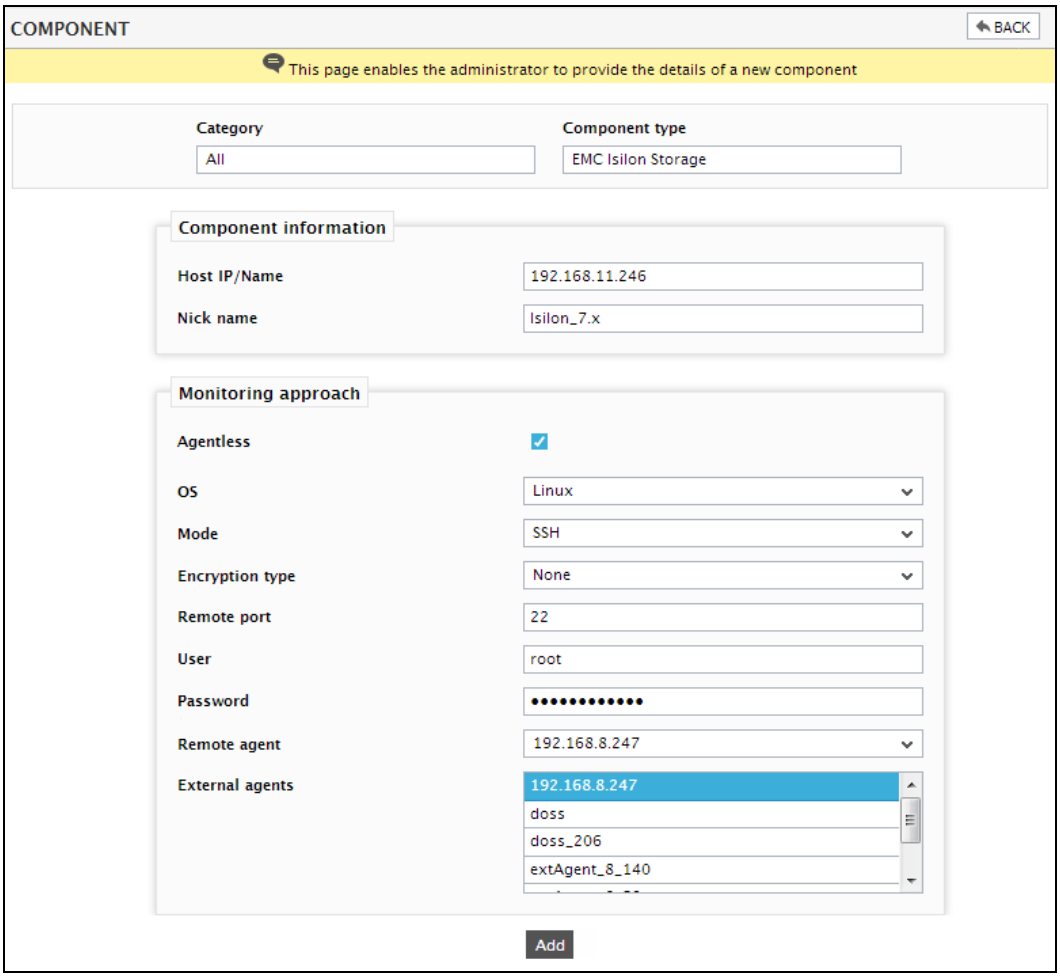

Figure 2.1: Adding the EMC Isilon Storage component

5. Specify the **Host IP/Name** and the **Nick name** for the *EMC Isilon Storage* component. Since the *EMC Isilon Storage* component is by default monitored in an agentless manner, the **Agentless**

check box will be selected by default.

6. Next, select **Linux** as the **OS** and **SSH** as the **Mode**. The SSH Remote port will be set as 22 by default. Change the remote port if the target storage system is listening on a different SSH port.
7. Specify the credentials of a root user or sudo user in the User and Password text boxes. The steps for creating the sudo user are explained in the Section **2.1**.
8. Select the **Remote agent** that will be monitoring the target storage system.
9. Choose an external agent for the target storage system by picking an option from the **External agents** list box.
10. Then, click the **Add** button to register the changes (see Figure 2.1).
11. The EMC Isilon Storage component so added will be managed automatically by eG Enterprise. Now, try to sign out of the user interface. Doing so, will invoke Figure 2.2 prompting you to configure a list of unconfigured tests for the new EMC Isilon Storage component.

List of unconfigured tests for 'EMC Isilon Storage'

Performance		isilon
Cluster Capacity	Cluster Status	Device Uptime
Network Interfaces	Node Disk Drive Throughputs	Node Disk Status
Node Fan	Node Power Sensor	Node Temperature Sensor

Figure 2.2: The list of unconfigured tests that need to be configured for the EMC Isilon Storage

12. Click on any test in the list of unconfigured tests.To know how to configure the tests, refer to **Monitoring the EMC Isilon Storage System**.
13. Finally, signout of the eG admin interface.

Chapter 3: Monitoring the EMC Isilon Storage System

eG Enterprise offers a specialized EMC Isilon Storage monitoring model that monitors the core functions and components of the Isilon storage system, and proactively alerts administrators to issues in its overall performance and its critical operations, so that the holes are plugged before any data loss occurs.

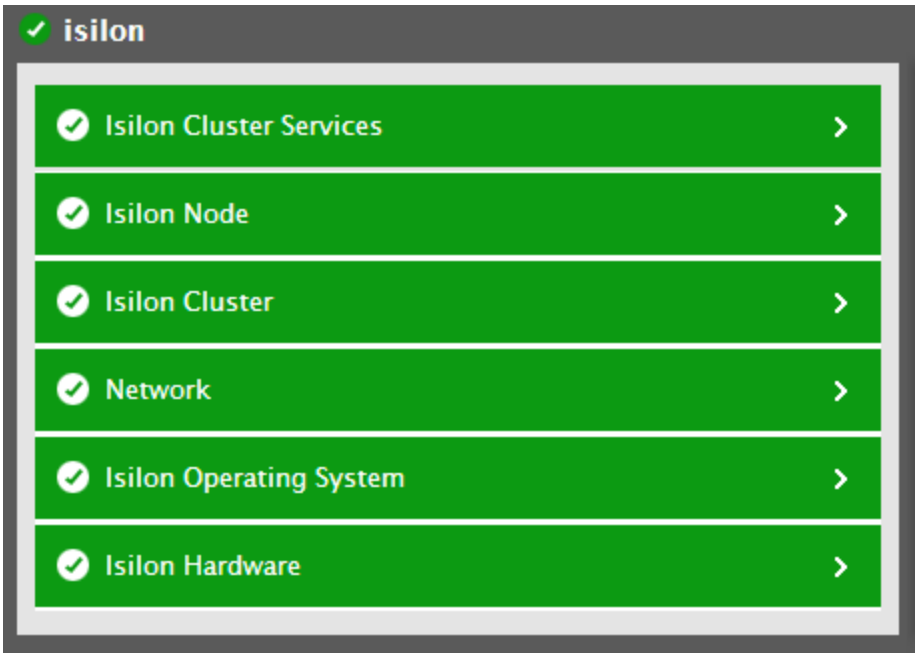

Figure 3.1: The layer model of the EMC Isilon storage system

Every layer of the layer model is mapped to a wide variety of tests that monitor critical performance parameters such as processing ability, load, and state, of the core components of the storage system. To pull out such useful performance data from the storage system, the eG agent needs to be deployed on a remote Windows host in the environment and configured to poll the SNMP MIB and run CLI commands via SSH port of the storage system at set intervals. To know how to configure the eG agent to collect performance metrics from the storage system, refer to **How to Monitor EMC Isilon Storage System Using eG Enterprise ?**. Once the pre-requisites discussed are fulfilled, the eG agent will extract useful statistics from the storage system and report it to the eG manager.

Using these metrics, the following critical performance queries can be answered:

- What is the status of storage cluster and nodes?
- What is the total capacity and space utilization of nodes and cluster?

- How much data was utilized for performing read/write operations on the disk?
- Is any disk on the node overloaded with I/O requests?
- What is the current temperature and voltage of each node?
- What is the current speed of the fans on each node?
- How well I/O operations were performed through each protocol?
- Which protocol was transferring maximum data?
- What is the throughput of the cluster and nodes?
- Is any node overloaded with I/O requests?
- Is load uniformly distributed across disks?
- Is any storage processor in a faulty state now?
- Is any storage processor overloaded?
- What is the current status of the storage pool?
- How well the storage pool was utilized?

The sections that will follow discuss each of the layers of Figure 3.1 in great detail.

3.1 The Isilon Hardware Layer

This layer is mapped with the various tests to monitor the hardware components (disks, fans, power sensors and temperature sensors) of the target storage system.

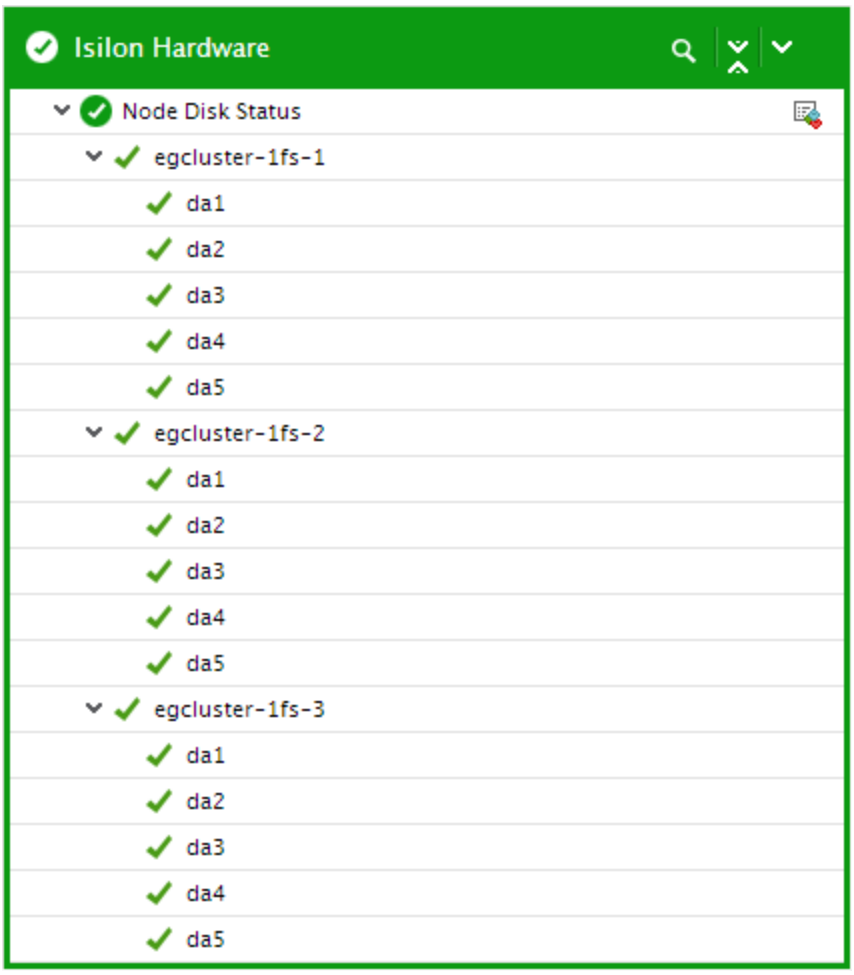

Figure 3.2: The tests mapped to the Isilon Hardware layer

3.1.1 Node Disk Status Test

If one/more disks in an Isilon node experience errors or are faulty or have failed, then users will be unable to access the data stored in those disks. In such cases, users may have to wait till the administrators identify the faulty or failed disks and repair those disks. For a better user experience, it is important for the administrators to rapidly identify the disks that are in an abnormal state and determine the reason for the abnormality, so that the problems are resolved quickly before end users complain! For this purpose, administrators can use the **Node Disk Status** test. This test reports the current status of each disk on each node of the target storage system.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameters	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 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 target storage system. 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.

Parameters	Description
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**.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1** . Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page.

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this disk on this node.		The table below summarizes the **State** values that this measure can report and their corresponding numeric equivalents: State: Value Other: 0 Healthy: 1 Journal: 2 Preparing: 3

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>State</th><th>Value</th></tr><tr><td>Empty</td><td>4</td></tr><tr><td>Smartfail</td><td>5</td></tr><tr><td>Replace</td><td>6</td></tr></table> **Note:** By default, this measure reports the above-mentioned **State**s while indicating the current status of each disk on every node. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only. The detailed diagnosis of this measure if enabled, lists the name of the disk bay at which the disk is located, and the size of the disk.

3.1.2 Node Fan Test

To maintain optimal temperature, each node comprises of multiple fans. If the fans are not running within the permissible range, the temperature of the nodes may soar/drop causing permanent damage to the components of the nodes. To avoid such heavy duty damage to the node, it is necessary to monitor the speed of the fans at regular intervals. This is where the **Node Fan** test helps! This test auto discovers the fans in the each node and reports the speed at which each fan operates. This way, administrators can instantly detect the fan speed, initiate remedial measures if any irregularities are detected so that damage to the components of the node can be prevented proactively.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each *node:fan* pair 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.
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. If the sudo user is Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Speed	Indicates the current speed of this fan.	RPM	The speed of the fan should be well within operable limit. A sudden/significant rise/fall in the value of this measure could be a cause for concern which warrants an investigation.

3.1.3 Node Power Sensor Test

This test auto-discovers the power sensors at each node of the storage system, and reports the voltage at which each power sensor is operating. Using this test, administrators are proactively alerted to fluctuations in the voltage of the nodes before any severe damage occurs.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameters	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 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 target storage system. 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.

Parameters	Description
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**.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1** section. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page.

Parameters	Description
	Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current Voltage	Indicates the current voltage of this power sensor.	Volts	The value of this measure should b e in the permissible range. A sudden increase or decrease in the value of this measure is a cause for concern.

3.1.4 Node Temperature Sensor Test

Abnormal temperature of the nodes in the storage system may often lead to the malfunctioning of the target storage system. If the abnormality condition is left unnoticed, the overall health of the storage system may get affected. To avert such adversities, administrators should monitor temperature of the nodes at regular intervals. This is where the **Node Temperature Sensor** test helps!

This test auto-discovers the nodes of the target storage system and for each node, this test reports the current temperature. Using this test, administrators can figure out the node that is not within the admissible temperature range and is malfunctioning.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameters	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 is *161*.

Parameters	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 target storage system. 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

Parameters	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**.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Current temperature	Indicates the current temperature of this node.	Celsius	The value of this measure should be in the permissible range. A sudden

Measurement	Description	Measurement Unit	Interpretation
			increase or decrease in the value of this measure is a cause for concern.

3.2 The Isilon Operating System Layer

The tests mapped to this layer report CPU utilization of the cluster and the nodes, and the capacity of the cluster and the nodes on the target storage system.

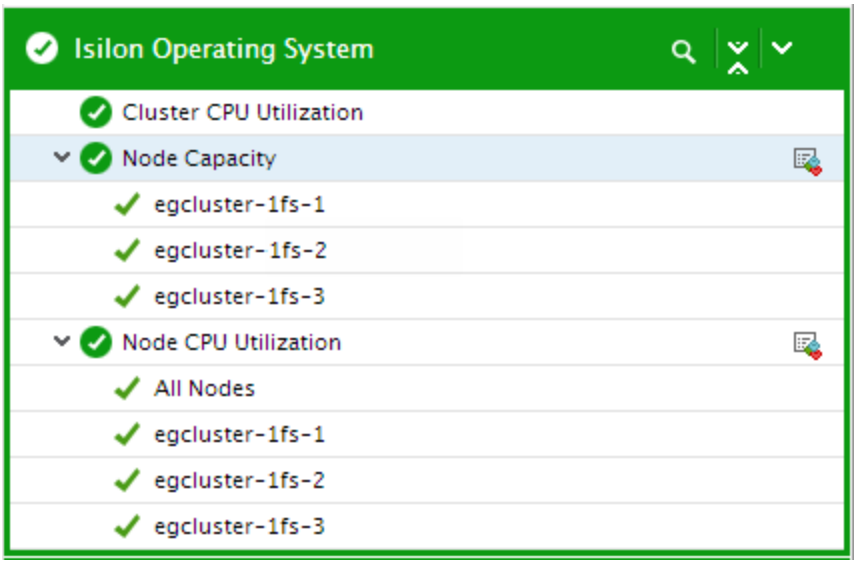

Figure 3.3: The tests mapped to the Isilon Operating System layer

3.2.1 Cluster Capacity Test

An Isilon cluster consists of three or more hardware nodes, which can be scaled up to 144 nodes. Cluster's storage capacity ranges from a minimum of 18 TB to a maximum of 15.5 PB. If the cluster lacks space, the data cannot be stored in the target storage system which may lead to critical data loss. To avoid this and to ensure peak performance of the cluster, it is mandatory to monitor the space utilization of the cluster periodically. The **Cluster Capacity** test helps administrators in this regard!

This test reports the space available for use in the cluster and space that is utilized in the cluster. By closely monitoring the space utilization of the cluster, administrators may be alerted to potential space crunch at the earliest before the users complain.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameters	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 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 target storage system. 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.

Parameters	Description
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 capacity	Indicates the total amount of space in the cluster.	TB	

Measurement	Description	Measurement Unit	Interpretation
Used space	Indicates the amount of space utilized on the cluster.	TB	Ideally, the value of this measure should be low. A high value of this measure indicates that the cluster is running out of space.
Free space	Indicates the amount of space that is available for use in the cluster.	TB	Ideally, the value of this measure should be high.
Space usage	Indicates the percentage of space utilized on the cluster.	Percent	
Space free	Indicates the percentage of space that is available for use in the cluster.	Percent	

3.2.2 Cluster CPU Utilization Test

Without adequate processing power, the storage cluster may abruptly stop functioning. This is why, it is imperative that administrators keep an eye on the CPU usage of the storage cluster, so that if CPU usage exceeds permissible limits, it can be quickly detected and treated to ensure optimal performance of the storage cluster. This is where the **Cluster CPU Utilization** test helps. This test monitors the overall CPU utilization of the storage cluster and reveals where the maximum CPU time is spent – in serving user requests? in system-level processing? or being idle? This way, the test not only points administrators to the excessive CPU usage by the storage cluster, but also indicates the reason for the same, so that administrators can initiate the correct remedial measures.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for 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.

Parameter	Description
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1** section. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
System CPU usage	Indicates the percentage of CPU time the storage cluster spent in system-level processing.	Percent	Compare the value of this measure with the value of the *User CPU* usage and *Idle CPU* measures to understand where storage cluster spent the maximum CPU time - in serving user requests? in system-level processing? or being idle? In the event of a slowdown, you can use the results of this comparative analysis to determine what caused the CPU contention.
User CPU usage	Indicates the percentage of CPU time that the storage cluster spent in user-level processing.	Percent	Compare the value of this measure with the value of the *System CPU* usage and *Idle CPU* measures to understand where storage cluster spent the maximum CPU time - in serving user requests? in system-level processing? or being idle? In the event of a slowdown, you can use the results of this comparative analysis to determine what caused the CPU contention.

Measurement	Description	Measurement Unit	Interpretation
Idle CPU	Indicates the percentage of time the CPU was idle on the storage cluster.	Percent	Compare the value of this measure with the value of the *System CPU usage* and *User CPU usage* measures to understand where storage cluster spent the maximum CPU time - in serving user requests? in system-level processing? or being idle? In the event of a slowdown, you can use the results of this comparative analysis to determine what caused the CPU contention.

3.2.3 Node Capacity Test

Nodes are the fundamental building blocks of an Isilon cluster that is built on a highly redundant architecture. As a rack - mountable appliance, each node includes the following components in a 2U or 4U rack - mountable chassis with an LCD front panel:

- memory
- CPUs
- RAM
- NVRAM to protect write operations from power failures
- network interfaces
- InfiniBand adapters that provide the distributed system bus that connects all the nodes
- disk controllers
- storage media

Each node in a distributed cluster has compute as well as storage or capacity capabilities. If any of the nodes is running out of storage space, the node will not be able to service the user requests received, resulting in poor performance of the node. This in turn will degrade overall performance of the target storage system. To avoid this, space utilization of each node should be tracked continuously. To achieve this, administrators can use the **Node Capacity** test.

This test auto-discovers the nodes in the cluster, and for each node, reports the space available for use and space that is utilized. By closely monitoring the space utilization of each node,

administrators may be alerted to investigate the reasons for the space crunch, and resolve the issue, before the overall performance of the storage system gets affected.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameters	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 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 target storage system. 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

Parameters	Description
	Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related 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 capacity	Indicates the total amount of space allocated to this node.	TB	
Used space	Indicates the amount of space utilized in this node.	TB	Ideally, the value of this measure should be low. A high value of this measure indicates that the cluster is running out of space.
Free space	Indicates the amount of space that is available for use in this node.	TB	Ideally, the value of this measure should be high.
Space usage	Indicates the percentage of space utilized in this node.	Percent	
Space free	Indicates the percentage of space that is available for use in this node.	Percent	

3.2.4 Node CPU Utilization Test

This test auto-discovers the nodes on the target storage system, and monitors the CPU utilization of each node. This way, the test points administrators to figure out how CPU hungry each node is.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each node 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.
Port	The port at which the host listens. By default, this will be *NULL*.

Parameter	Description
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU usage	Indicates the percentage of CPU utilized by this node.	Percent	Compare the value of this measure across the nodes to identify the node which consumes the maximum CPU.

3.3 The Network Layer

The **Network** layer reflects the status of network connectivity to and from the storage system. The tests that map to this layer are as follows.

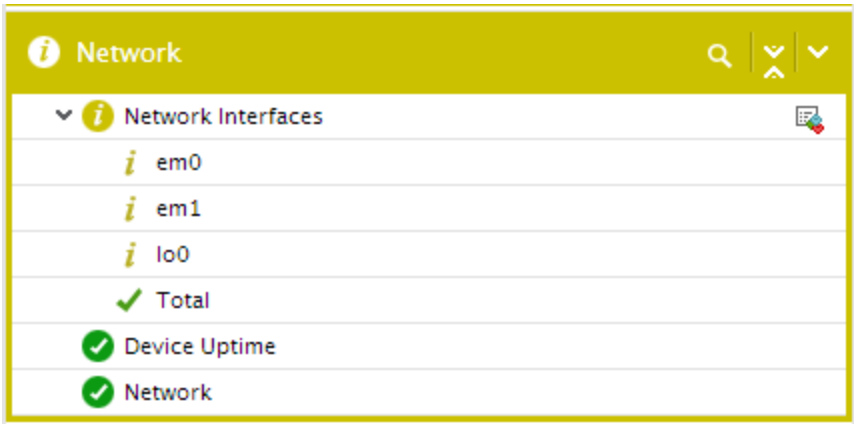

Figure 3.4: List of tests associated with the Network layer

To know the details on the *Device Uptime* and *Network interfaces* tests refer to the *Monitoring Cisco Router* document, and for the details on the *Network test*, refer to *Monitoring Unix and Windows Servers* document.

3.4 The Isilon Cluster Layer

The tests mapped to this layer monitor the current status and utilization of each storage pool on the target storage system. In addition, the disk activities and throughput of the cluster are also monitored, and its usage and effectiveness is determined.

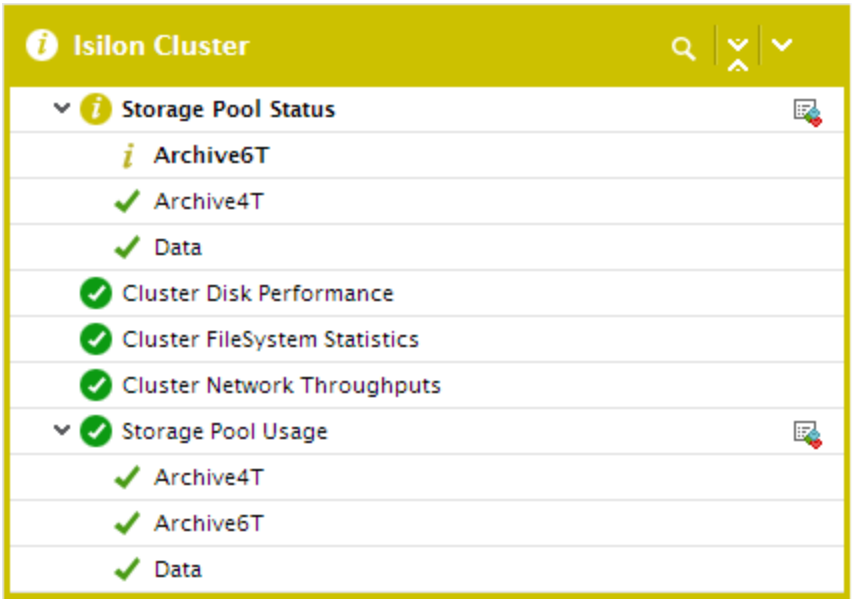

Figure 3.5: The tests mapped to the Isilon Cluster layer

3.4.1 Storage Pool Status Test

Storage pools provide the ability to define subsets of physical resources within a single cluster, allowing the file layout to be aligned with specific sets of nodes through the configuration of storage pool policies. The storage pools include disk pools, node pools, and user-defined tiers. Monitoring the status of storage pools enables administrators to find out the following:

- Does any storage pool consist of few nodes?
- Is any drive missing?
- Is there any node/drive in the pool smartfailed/down? or
- Is there any node/drive that needs to be repaired?

With the help of the **Storage Pool Status** test, administrators can accurately find out the answers for the above questions. This test auto-discovers the storage pools on the target storage system, and reports the current status of each pool.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the each storage pool 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.
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis

Parameter	Description
	measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this storage pool.		The table below summarizes the **State** values that this measure can report and their corresponding numeric equivalents: **State** / **Numeric Value** Ok: 0 Too few nodes: 1 Nodes or drives are smartfailed: 2 Missing drives: 3 Nodes or drives need repair: 4 Nodes or drives are down: 5 **Note:** By default, this measure reports the above-mentioned **State**s while indicating the current status of each storage pool. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only. The detailed diagnosis of this measure reveals the name, status and type of each node in the storage pools.

3.4.2 Cluster Disk Performance Test

Processing bottlenecks in disks can significantly delay reading from and/or writing to the disks, affecting user experience with the storage cluster as a whole. To prevent this, administrators need to keep a close watch on the I/O activity on the disks of the storage cluster, detect a slowdown well before the users notice the slowdown, and take pre- emptive actions. The **Cluster Disk Performance** test can help administrators to achieve this. This test monitors the read and write operations on the disks, using which any abnormalities can be detected before users start complaining of slowdowns.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for 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.
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data reads	Indicates the amount of data utilized for performing the read operations on the disk.	MB/Sec	
Data writes	Indicates the amount of data utilized for performing the write operations on the disk.	MB/Sec	
Disk IOPS	Indicates the rate at which the I/O operations are performed on this disk.	IOPS	

3.4.3 Cluster Filesystem Statistics Test

The EMC Isilon storage system is a fully distributed storage system with the ability to manage your entire environment under an intelligent light-weight file system. The file system spans across all nodes in the cluster, and protects data by distributing it across all nodes. This way, the load on the cluster is distributed and managed by the file system. If any load-balancing irregularity on the file system is not addressed in time, then, this will make the data protection questionable and adversely impact the performance of the entire storage system. To avoid such eventualities, the workload on the file system should be continuously monitored. This can be easily done using the **Cluster Filesystem Statistics** test.

This test helps administrators to find out the data reception/transmission rates on the file system, and alerts them to take remedial actions immediately, if any irregularities are detected.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for 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.
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data received	Indicates the rate at which the data was received on the file system.	MB/sec	These measures are the indicators of how well the file system handles the load on the storage cluster.
Data transmitted	Indicates the rate at which the data was transmitted by the file system.	MB/sec	
Total data	Indicates the rate at which the data was received/ transmitted by the file system.	MB/sec	

3.4.4 Cluster Network Throughputs Test

When users complain of slowness of the storage cluster, administrators should first check the throughput of the storage cluster. Throughput reveals how well/badly the storage cluster handles network traffic. Low throughput is indicative of a traffic processing bottleneck, which can cause users to experience slowness when storing/retrieving data from the cluster. To receive insights into the throughput of the cluster, administrators can use the **Cluster Network Throughputs** test. This test

measures the rate at which the data is received/transmitted by the cluster, and also reports the number of packets received/transmitted per second. Additionally, the test also reveals the number of errors occurred per second during receiving/transmitting the data, if any.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for 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.
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data received	Indicates the rate at which the data is received by the cluster.	MB/Sec	These measures are the indicators of traffic handling ability of the cluster. A very high value of these measures points out that the cluster does not have adequate resources to process upcoming traffic.

Measurement	Description	Measurement Unit	Interpretation
Data transmitted	Indicates the rate at which the data is transmitted from the cluster.	MB/Sec	
Received packets	Indicates the rate at which the packets are received by the cluster.	Packets/Sec	
Transmitted packets	Indicates the number of packets that is transmitted from the cluster per second.	Packets/Sec	
Error in received data	Indicates the number of errors that is occurred per second when receiving data on the cluster.	Errors/Sec	Ideally, the value of this measure should be zero. A high value of this measure indicates a processing bottleneck requiring further investigation.
Error in transmitted data	Indicates the number of errors that is occurred per second when transmitting data from the cluster.	Errors/Sec	Ideally, the value of this measure should be zero. A high value of this measure indicates a processing bottleneck requiring further investigation.

3.4.5 Storage Pool Usage Test

This test auto-discovers the storage pools on the target storage system, and reports the space utilization on each storage pool. By closely monitoring the space utilization of the storage pools, administrators may be alerted to potential space crunch at the earliest before users complain.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameters	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 listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Storage capacity	Indicates the total amount of space in this storage pool.	TB	
Storage used space	Indicates the amount of space utilized on this storage pool.	TB	Ideally, the value of this measure should be low. A high value of this measure indicates that the storage pool. is running out of space.
Storage free space	Indicates the amount of space that is available for use in this storage pool.	TB	Ideally, the value of this measure should be high.
Storage utilization	Indicates the percentage of space utilized on this storage pool.	Percent	

3.5 The Isilon Node Layer

The tests mapped to this layer help administrators to find out the following useful metrics:

- the current status of the nodes;
- the load balancing capability of each disk on the node;
- the throughput of network and disk drives of the node;
- the load received by the nodes through each protocol;
- the rates at which the data was transmitted and received to perform the protocol operations.

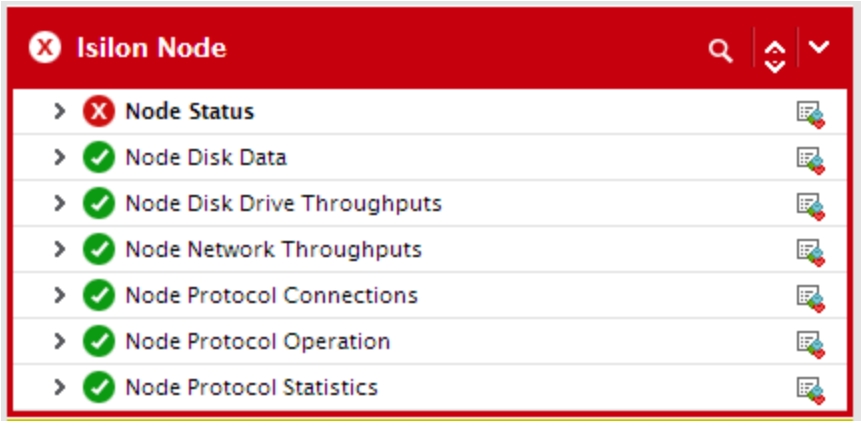

Figure 3.6: The tests mapped to the Isilon Cluster layer

3.5.1 Node Status Test

A single Isilon cluster consists of multiple nodes, which are rack-mountable enterprise appliances. Availability of the nodes is vital for proper functioning of the storage clusters and for servicing the user requests quickly. If the node is down or goes offline, the overall performance of the cluster will degrade. This will adversely slow down the request processing ability of the storage system. To avoid this, administrators can use the **Node Status** test to verify if the node is functioning properly. This test auto-discovers the nodes in the storage system, and reports the current status of each node.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each node 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.
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. If the sudo user is Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this node.		The table below summarizes the **State** values that this measure can report and their corresponding numeric equivalents: **State** / **Value** Ok / 0 Attention / 1 Down / 2 Invalid / 3 **Note:** By default, this measure reports the above-mentioned **State**s while indicating the current status of each

Measurement	Description	Measurement Unit	Interpretation
			node. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.

3.5.2 Node Disk Data Test

This test monitors the load balancing capability of each disk on each node of the target storage system. Using this test, administrators can pin point the disks that are handling more read and write operations than the rest. This way, irregularities in the distribution of I/O load across the disks can be detected at ease and in the process, administrators will be able to fine-tune the load-balancing algorithm.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Measures are also reported for *All* descriptor.

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 listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page.

Parameter	Description
	Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data reads	Indicates the rate at which the data was read from this disk.	MB/sec	For the *All* descriptor, these measures will report the total amount of data read and written across the nodes per second. Comparing the value of these measures across the disks will clearly indicate which disk drive 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 disks.
Data writes	Indicates the rate at which the data was written on this disk.	MB/sec	

3.5.3 Node Disk Drive Throughputs Test

The nodes in the storage system contain a number of disk drives that are held in drive bays. The drive bays facilitate easy removal of the failed drives and insertion of the replacement drives. If users complain about slowness of disk drives on the nodes, then administrators should first check the traffic flowing in and out of each disk drive. Tracking the traffic to the disk drives helps administrators to find out how well the read/write requests were performed on the disk drives and delays in I/O operations. This is what exactly the **Node Disk Drive Throughputs** test does.

This test auto-discovers the disk drives on the nodes, and reports the rate at which the data was read from/written on each disk drive, and the rate at which the read and write operations were performed on the disk drive. In the process, this test also reveals the time taken by each disk drive to perform read and write operations. This way, the test promptly alerts administrators to any abnormal increase in total traffic to the disk drives and the time delay (if any) in processing the I/O requests.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Configurable parameters for the test

Parameters	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 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 target storage system. 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.

Parameters	Description
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**.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page.

Parameters	Description
	Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.
Include Nodes	By default, this parameter is set to *all* indicating that the eG agent reports performance metrics for all nodes in the cluster by default. Sometimes, administrators may want to monitor performance of the nodes that are very critical. In such a case, the eG agent can be configured to include only those nodes for monitoring. To achieve this, provide a comma-separated list of nodes in the Include Nodes text box. The specification could be any of the following formats: • the list of node numbers - *2,4,6,8,10,12,14* • the list of node number ranges - *1-5,7-11,21-25,27-32,34-42* or • the combination node numbers and node number ranges - *2, 6, 8, 10-18, 24, 29, 40-48*. This way, administrators can make sure that the eG agent collects metrics only for a configured set of nodes.
Exclude Nodes	By default, this parameter is set to *none* indicating that the eG agent reports performance metrics for all nodes in the cluster by default. In some environments, administrators may not want to monitor some of the less-critical nodes. In such a case, the eG agent can be configured to exclude such nodes from monitoring. To achieve this, provide a comma-separated list of nodes in the Exclude Nodes text box. The specification could be any of the following formats: • the list of node numbers - *1,2,3,7,10,18* • the list of node number ranges - *6-9,12-15,21-29,47-52* or • the combination node numbers and node number ranges - *2,6,8,10-18,24,29,40-48*. This way, administrators can make sure the eG agent stops collecting metrics for a configured set of nodes.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data reads	Indicates the rate at which the data was read from this	MB/sec	Comparing the value of these measures across the disk drives will

Measurement	Description	Measurement Unit	Interpretation
	disk drive.		clearly indicate which disk drive 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 disk drives.
Data writes	Indicates the rate at which the data was written on this disk drive.	MB/sec	
Disk reads	Indicates the rate at which the read operations were performed on this disk drive during the last measurement period.	Reads/sec	Ideally, the value of this measure should be high. A steady dip in this measure value could indicate a potential reading bottleneck.
Disk writes	Indicates the rate at which the write operations were performed on this disk drive during the last measurement period.	Writes/sec	Ideally, the value of this measure should be high. A steady dip in this measure value could indicate a potential writing bottleneck.
Disk I/O operations	Indicates the total number of I/O operations that were performed on this disk drive per second.	IOPS	
Disk latency	Indicates the time taken by this disk drive to perform read and write operations.	Milliseconds	Ideally, this value should be low. A high value could indicate that read and operations are slowing down for some reason.
Disk busy	Indicates the percentage of time that this disk drive was busy processing the requests.	Percent	Compare the value of this measure across the disk drives to know which disk drive was the busiest and which disk drive was not. If the gap between the two is very high, then it indicates serious irregularities in load-balancing across disk drives.

3.5.4 Node Network Throughputs Test

Sometimes, administrators may want to closely watch the traffic flowing into each node in the storage system. To achieve this, administrators can use the **Node Network Throughputs** test. This test auto-discovers the nodes in the storage system, and reports the traffic flowing into and out

of each node. In the process, the test promptly alerts administrators to any abnormal increase in total traffic to the nodes.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

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

Measures are also reported for an additional **All** descriptor.

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 listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data received	Indicates the rate at which the data is received by this node.	MB/Sec	For the *All* descriptor, this measure will report the total amount of data received across the nodes per second. Compare the value of this measure across nodes to know which node is

Measurement	Description	Measurement Unit	Interpretation
			receiving maximum data.
Data transmitted	Indicates the rate at which the data is transmitted from this node.	MB/Sec	For the *All* descriptor, this measure will report the total amount of data transmitted across the nodes per second. Compare the value of this measure across nodes to know which node is transmitting maximum data.
Total data	Indicates the rate at which the data is received by/transmitted from this node.	MB/Sec	For the *All* descriptor, this measure will report the rate at which data is received/transmitted across the nodes. This is the sum of the *Data received* and *Data transmitted* measures and reveals the overall network throughput of the node. A consistent drop in the value of this measure could indicate that the node does not have adequate bandwidth resources for processing network traffic.

3.5.5 Node Protocol Connections Test

Users access the nodes on the target storage system via the communication protocols such as NFS, SMB/CIFS, HTTP/HTTPS, FTP, REST API, and SWIFT. These connections are a good indicator of the load on the storage system. If users complain about the poor connectivity to the storage system, administrators may want to check the protocol connections to figure out whether the storage system is stressed due to an overload condition. If so, administrators may also want to identify the protocol thorough which the maximum load is received by the storage system. This where the **Node Protocol Connections** test helps administrators!

This test not only reports the number of connections established through each protocol but also reveals the count of active connections. This way, the test measures the connection load on the storage system and points to those protocols that are responsible for overloading the storage system with numerous connections. In the process, this test also indicates to administrators the connections that are currently active on the storage system.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the each protocol connected to 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.
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.
Connected Protocol	By default, this text box is populated with a default set of protocols separated by semi colons. The protocols listed are: *cifs;ftp;hdfs;http;iscsi;ndmp;nfs;nlm;papi;siq;smb*. This implies that the eG agent monitors the protocols mentioned in this text box alone and reports metrics. **You can remove one/more protocols from this text box and add them back but will not be allowed to add a new protocol.**
Active Protocol	By default, this text box is populated with a semi-colon-separated list of protocols that are currently active on the target storage system. For instance, the protocols listed are: *cifs;ftp;hdfs;http;iscsi;ndmp;jobd;lsass_out;nfs;nfs3;nfs4;nlm;papi;siq;smb2*. This list will only include one or more protocols or the variants of the protocols mentioned in the *Connected Protocol* text box.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Connected	Indicates the number of connections established thorough this protocol.	Number	This measure is a good indicator of the load imposed through each protocol on the storage system.
Active	Indicates the number of connections that are currently active.	Number	

3.5.6 Node Protocol Statistics Test

The EMC Isilon storage system supports standard network communication protocols that enable users to access the storage system via the file system. The users with adequate credentials and privileges can create, modify, and read data from the cluster using one of the communication protocols. The communication protocols supported by the storage system are:

- NFS (Network File System)
- SMB/CIFS (Server Message Block/Common Internet File System)
- FTP (File Transfer Protocol)
- HTTP/HTTPs (Hypertext Transfer Protocol)
- HDFS (Hadoop Distributed File System)
- REST API (Representational State Transfer Application Programming Interface)
- OpenStack Swift (Object Storage API)

By periodically checking the data transferred via the protocols that connect the users to the storage system, administrators can identify the protocol through which the storage system receives high-level of traffic. Using the **Node Protocol Statistics** test, administrators can easily monitor the data traffic received through the protocols.

This test auto-discovers the protocols that connect the users with the target storage system, and for each protocol, reports the amount data transferred per second. This revelation helps administrators to figure out the throughput of each protocol and proactively detect potential abnormalities and/or processing bottlenecks (if the connection is not legitimate).

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each protocol used to access the target storage system being monitored.

This test also reports measures for **Total** descriptor.

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 listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transfer	Indicates the rate at which the data is transferred via this protocol.	MB/sec	For the *Total* descriptor, this measure will report the rate at which the data is transferred across the protocols. Compare the value of this measure across the protocols to identify the protocol that is transferring maximum amount of data to the storage system.

3.5.7 Node Protocol Operation Test

Users access the file system of the storage system using the access protocols, including NFS, SMB/CIFS, HTTP/HTTPS, FTP, REST API, and SWIFT. The users send I/O operation requests and receive responses from the storage nodes only through the access protocols. If any of the nodes are overloaded with too many I/O operations, the particular node will not be able to quickly serve the upcoming I/O requests. This will attribute the slowdowns in I/O request processing. When the administrators experience such slowdowns, they need to swiftly identify the following:

- Which nodes are over-loaded with operations?
- Which protocol is sending maximum number of requests to the node?
- What type of operations registered the maximum latency – CIFS, NFS, or iSCSI?

This test helps administrators to find out accurate answers for the above queries. This test reports the amount of data transmitted/received while performing each operation and also reveals the time delay (if any).

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every operation performed on each node of the target storage system.

First-level descriptor: Node

Second-level descriptor: Protocol

Third-level descriptor: Class:Operation

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 listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Connected Protocol	By default, this text box is populated with a default set of protocols separated by semi colons. The protocols listed are: *cifs;ftp;hdfs;http;iscsi;ndmp;nfs;nlm;papi;siq;smb*.

Parameter	Description
	This implies that the eG agent monitors the protocols mentioned in this text box alone and reports metrics. **You can remove one/more protocols from this text box and add them back but will not be allowed to add a new protocol.**
Active Protocol	By default, this text box is populated with a semi-colon-separated list of protocols that are currently active on the target storage system. For instance, the protocols listed are: *cifs;ftp;hdfs;http;iscsi;ndmp;jobd;lsass_out;nfs;nfs3;nfs4;nlm;papi;siq;smb2*. This list will only include one or more protocols or the variants of the protocols mentioned in the *Connected Protocol* text box.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total operations	Indicates the rate at which operations of this type were performed.	Operations/sec	The value of this measure reveals the workload received via each protocol to each node in the storage cluster.
Data received	Indicates the rate at which the data was received during performing this operation.	KB/sec	Compare the value of this measure across the operations to identify the operation during which the maximum amount of data was received.
Data transmitted	Indicates the rate at which the data was transmitted out during performing this operation.	KB/sec	Compare the value of this measure across the operations to identify the operation during which the maximum amount of data was transmitted.
Average time	Indicates the average time taken for performing this operation.	Milliseconds	A high value of this measure is a cause for concern, as it indicates a processing bottleneck.

Measurement	Description	Measurement Unit	Interpretation
Standard time deviation	Indicates the standard time deviation of this operation.	Milliseconds	

3.6 The Isilon Cluster Services Layer

To monitor the status of the storage cluster, use the test mapped to this layer.

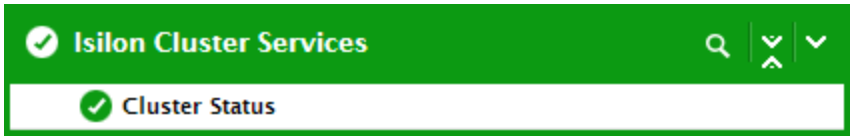

Figure 3.7: The tests mapped to the Isilon Cluster Services layer

3.6.1 Cluster Status Test

A single Isilon cluster consists of multiple nodes, which are rack-mountable enterprise appliances containing: memory, CPU, networking, Ethernet or low-latency InfiniBand interconnects, disk controllers and storage media. Whenever administrators encounter difficulties in accessing the cluster or nodes in the cluster, administrators can use this test to verify the availability and node capacity of the cluster.

This test enables administrators to determine the current status of the cluster and the number of nodes in the cluster. The detailed diagnosis of this test reveals the details on the offline and online nodes in the cluster. This helps administrators to instantly find out the offline nodes, and start investigating the reason behind offline status before it adversely affects overall performance of the storage system.

Target of the test : An EMC Isilon Storage System

Agent deploying the test : A remote agent

Outputs of the test : One set of results for 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.
Port	The port at which the host listens. By default, this will be *NULL*.
Timeout	Specify the time duration (in seconds) beyond which this test should time out in the Timeout text box. The default is 10 seconds.
Use SUDO	By default, this parameter is set to **No**. This indicates that, by default, the eG agent will not require any special permissions to execute the commands. However, in some highly secure environments, this command cannot be executed directly as the eG agent install user is different from the root user who has the privileges to run all commands on the target storage system. In such cases, create a sudo user using the steps discussed in the Section **2.1**. Credentials of such a user should be specified in the Username and Password text boxes in the **COMPONENTS** page. Set the Use Sudo parameter to **Yes**. This will enable the eG agent install user to execute the commands.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of the cluster.		The table below summarizes the **State** values that this measure can report and their corresponding numeric equivalents:

<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>State</th><th>Value</th></tr>
<tr><td>Ok</td><td>0</td></tr>
<tr><td>Attention</td><td>1</td></tr>
<tr><td>Down</td><td>2</td></tr>
<tr><td>Invalid</td><td>3</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned States while indicating the current status of the cluster. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.
</td></tr>
<tr><td>Number of nodes</td><td>Indicates the number of nodes in the cluster.</td><td>Number</td><td>The detailed diagnosis of this measure provides the name of the storage cluster, the number of nodes that are online and the number of nodes in the offline mode.</td></tr>
</table>

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.