Monitoring Fibre Channel SAN Switch

eG Innovations Product Documentation

www.eginnovations.com

eG
Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

In the computer storage field, a Fibre Channel switch is a network switch compatible with the Fibre Channel (FC) protocol. It allows the creation of a Fibre Channel fabric, that is currently the core component of most storage area networks. The fabric is a network of Fibre Channel devices which allows many-to-many communication, device name lookup, security, and redundancy. FC switches implement zoning, a mechanism that disables unwanted traffic between certain fabric nodes.

A defective FC switch can wreak havoc in a SAN environment, as it may cause serious security glitches, severe communication lapses, or prolonged breaks in the availability of the SAN environment. By continuously monitoring the state and operations of the switch, you can ensure that you are promptly notified of performance issues with the switch, so as to avoid such outcomes. This is where the eG Enterprise helps big time.

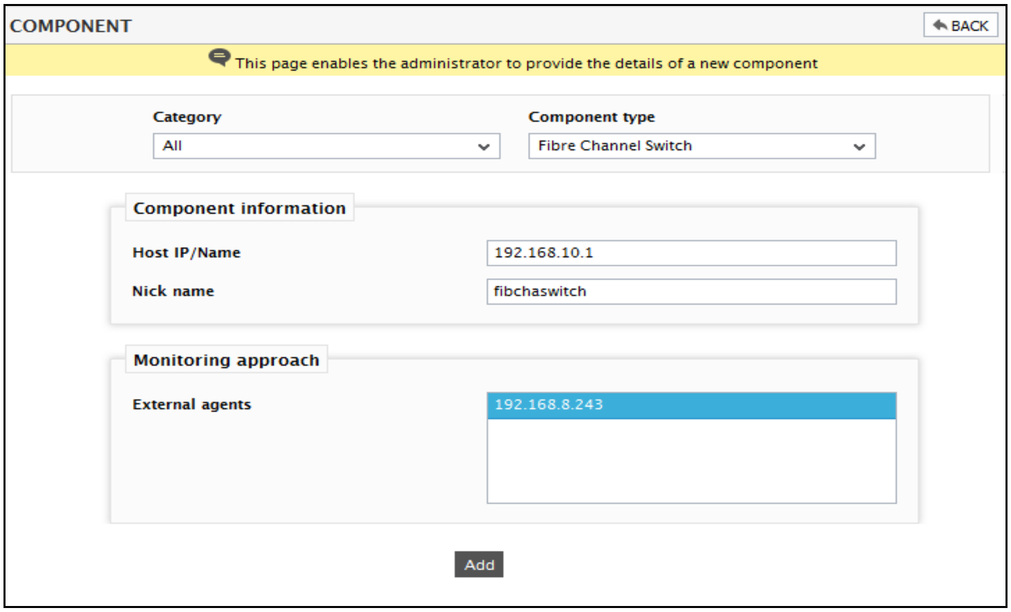
Chapter 2: How to Monitor Fibre Channel Switch Using eG Enterprise?

eG Enterprise monitors the Fibre Channel Switch in an *agentless* manner. For this purpose, the eG Enterprise employs an eG external agent on a remote Windows host. This agent polls the SNMP MIB of the switch to gather the statistics of interest at configured intervals. Before attempting to monitor the Fibre Channel Switch, ensure that the Fibre Channel Switch is SNMP-enabled.

2.1 Managing the Fibre Channel Switch

The eG Enterprise cannot automatically discover a Fibre Channel Switch. This implies that you need to manually add the component for monitoring. To manage a Fibre Channel Switch component, do the following:

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



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

Category: All

Component type: Fibre Channel Switch

Component information

Host IP/Name: 192.168.10.1

Nick name: fibchaswitch

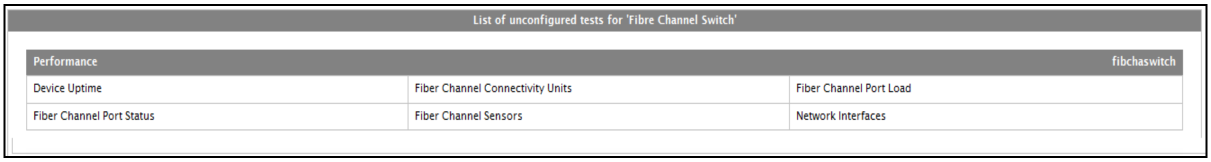
Monitoring approach

External agents: 192.168.8.243

Figure 2.1: Adding a Fibre Channel Switch

4. Specify **Host IP/Name** and **Nick name** for the Fibre Channel Switch component (see Figure 2.1). Then, click on the **Add** button to register the changes.

5. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).

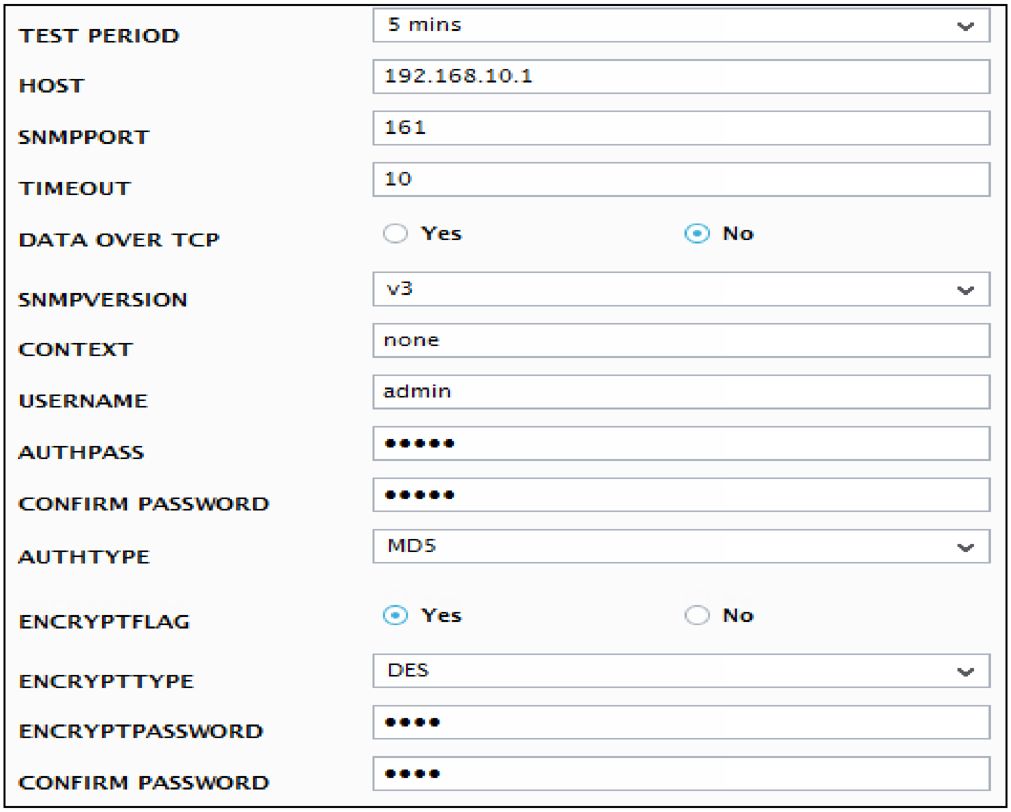


List of unconfigured tests for 'Fibre Channel Switch'

Performance		fibchaswitch
Device Uptime	Fiber Channel Connectivity Units	Fiber Channel Port Load
Fiber Channel Port Status	Fiber Channel Sensors	Network Interfaces

Figure 2.2: A list of unconfigured tests

6. Click on any test in the list of unconfigured tests. For instance, click on the **Fiber Channel Connectivity** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.



TEST PERIOD	5 mins	
HOST	192.168.10.1	
SNMPPORT	161	
TIMEOUT	10	
DATA OVER TCP	○ Yes	● No
SNMPVERSION	v3	
CONTEXT	none	
USERNAME	admin	
AUTHPASS	•••••	
CONFIRM PASSWORD	•••••	
AUTHTYPE	MD5	
ENCRYPTFLAG	● Yes	○ No
ENCRYPTTYPE	DES	
ENCRYPTPASSWORD	••••	
CONFIRM PASSWORD	••••	

Figure 2.3: Configuring the Fiber Channel Connectivity test

7. To know how to configure these parameters, refer to **Monitoring the Fibre Channel Switch** chapter.

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

Chapter 3: Monitoring the Fibre Channel Switch

eG Enterprise provides a specialized Fibre Channel Switch monitoring model that periodically monitors the state of the critical switch components and the load on the switch, so as to proactively alert administrators to unexpected state changes or a sudden/steady increase in the load to the switch.

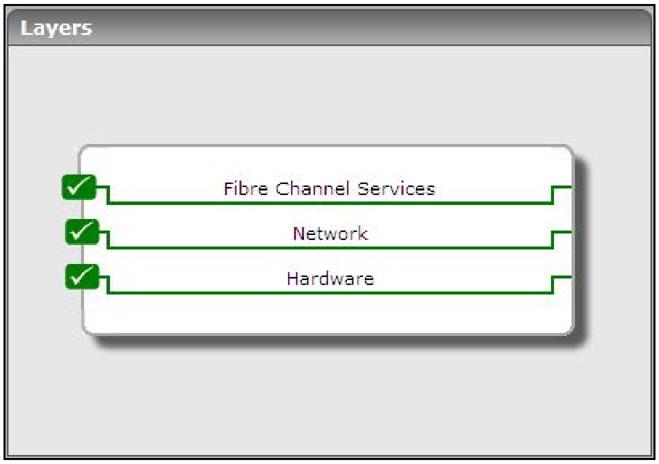


Figure 3.1: Layer model of the Fibre Channel switch

Each layer of Figure 3.1 is mapped to a series of tests that report a wealth of performance data that reveal the health of the fibre channel switch. Using these tests, you can accurately figure out the following:

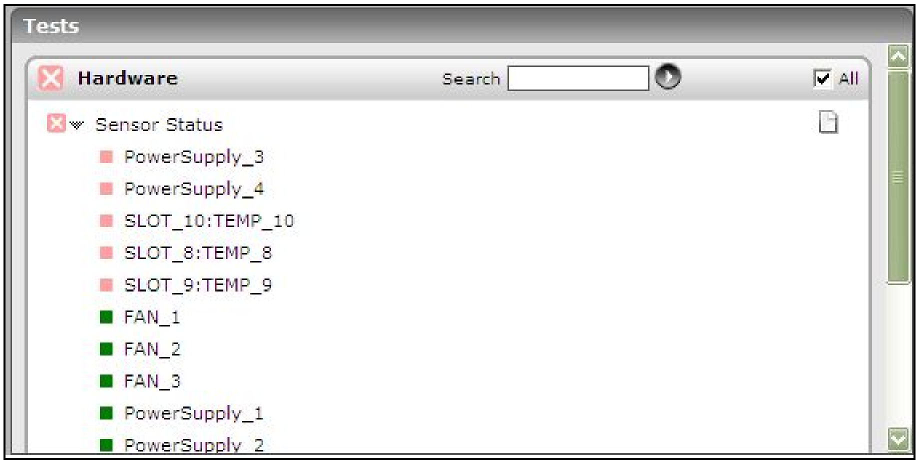
- Are all critical sensors of the switch in good health? Has any sensor failed? If so, which one is it?
- Is the switch available over the network?
- Are all the network interfaces supported by the switch using bandwidth optimally?
- Is any network interface operating at an abnormal speed?
- Which connection units are currently offline?
- Are there any unused connection units on the switch?
- How is the load on the ports? Is any port overloaded?
- Are all ports in the 'ready' state? Has any port failed?
- Are there 'invalid' ports on the switch?
- Has any port experienced a hardware failure?

- Is any port operating slowly?
- Is any port experiencing too many errors?
- Are link failures/invalid transmissions high on any port?
- Has any port encountered a signal loss/synchronization loss? Is it owing to a poor physical link?

The sections that follow will discuss each of these layers in great detail.

3.1 The Hardware Layer

Using the Sensor Status test mapped to this layer, you can be instantly updated with the current status of the power supply, fan, and temperature sensors of the switch.



☒ Sensor Status
- 🟥 PowerSupply_3
- 🟥 PowerSupply_4
- 🟥 SLOT_10:TEMP_10
- 🟥 SLOT_8:TEMP_8
- 🟥 SLOT_9:TEMP_9
- 🟩 FAN_1
- 🟩 FAN_2
- 🟩 FAN_3
- 🟩 PowerSupply_1
- 🟩 PowerSupply_2

Figure 3.2: The test mapped to the Hardware layer

3.1.1 Fiber Channel Sensors Test

This test reports the current status of each of the sensors on the FC switch.

Target of the test : A Fibre Channel SAN Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each sensor on the SAN switch 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*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:

Parameter	Description
	• **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Sensor status</td><td>Indicates the current status of this sensor.</td><td></td><td>The table below summarizes the **State** values reported by this measure and their corresponding numeric equivalents:
<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Warning</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Other</td><td>3</td></tr>
<tr><td>ok</td><td>4</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned **State**s while indicating the current status of a sensor. However, the in graph of this measure, states will be represented using their corresponding numeric equivalents only.
Use the detailed diagnosis of this measure to determine the exact state of the sensor.</td></tr>
</table>

3.2 The Network Layer

To know the health of network connections to and from the switch, to measure the responsiveness of the switch, and to assess the bandwidth usage and speed of the network interfaces supported by the switch, use the tests mapped to the **Network** layer.

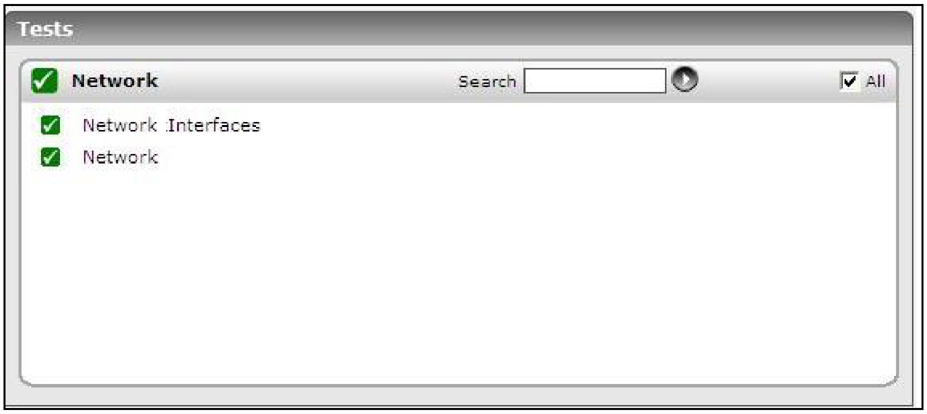


Figure 3.3: Figure 16.3: The tests associated with the Network layer

The tests mapped to this later have been discussed in the Monitoring Cisco Router document, let us proceed to the next layer.

3.3 The Fibre Channel Services Layer

The tests mapped to this layer enable network administrators to do the following:

- Promptly detect sudden changes in the operational state or overall health of one/more ports on the switch;
- Be alerted to errors/invalid transmissions at the port-level
- Isolate connection units that have failed;
- Identify overloaded ports or ports that are abnormally slow.

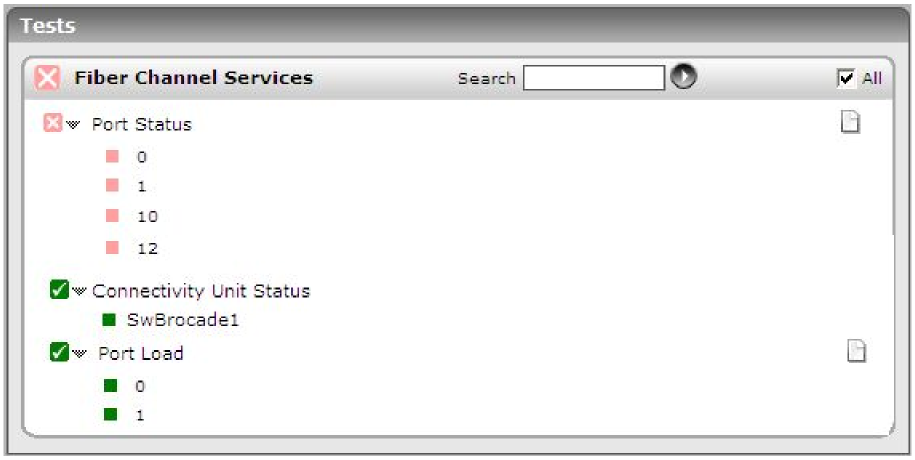


Figure 3.4: The tests mapped to the Fibre Channel Services layer

3.3.1 Fiber Channel Connectivity Units Test

This test reports the current operational state of the connection unit of the switch, and provides periodic updates on the current health of the unit.

Target of the test : A Fibre Channel SAN Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Fibre Channel Switch 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*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. 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

Parameter	Description
	SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
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

Parameter	Description
	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**.
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Operational state of connection unit</td><td>Indicates the current operational state of the connection unit.</td><td></td><td>The table below summarizes the <b>State</b> values that this measure can report and their corresponding numeric equivalents:
<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>Offline</td><td>0</td></tr>
<tr><td>Unknown</td><td>1</td></tr>
<tr><td>Online</td><td>100</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the above-mentioned <b>States</b> while indicating the current operational state of the connection unit. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>Use the detailed diagnosis of this measure to know the exact state of the connection unit, the number of sensors, and number of ports.</td></tr>
<tr><td>Current health of connection unit</td><td>Indicates the current health of the connection unit.</td><td></td><td>The table below summarizes the State values that this measure can report and their corresponding numeric equivalents:
<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>Failed</td><td>0</td></tr>
<tr><td>Warning</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Other</td><td>3</td></tr>
<tr><td>ok</td><td>100</td></tr>
</table>

Note:
By default, this measure reports the above-mentioned **State**s while indicating the current health of the connection unit. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.
Use the detailed diagnosis of this measure to know the exact state of the connection unit, the number of sensors, and number of ports.</td></tr>
</table>

3.3.2 Fiber Channel Port Load Test

To proactively capture sporadic or consistent increases in the load on a switch, it is imperative to monitor the traffic handled by each of the ports on the switch. Using the Port Load test, you can study the data, frames, and line resets sent and received by each port on the switch, and thus analyze the load on the switch.

Target of the test : A Fibre Channel SAN Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each port on the SAN switch 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*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.

Parameter	Description
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Frames transmitted	Indicates the number of frames / packets / IOs / etc that have been transmitted by this port.	Number	These measures serves as effective indicators of the I/O load on the ports. Comparing the value of these measures across ports will reveal the I/O-intensive ports.
Frames received	Indicates the number of frames / packets / IOs / etc that have been received by this port.	Number	
Data transmitted	Indicates the number of octets or bytes that have been transmitted by this port per second.	KB/Sec	These measures serve as good indicators of the data traffic handled by a port. Comparing the value of these measures across ports will reveal the busiest ports on the switch.
Data received	Indicates the number of octets or bytes that have been transmitted by this port per second.	Number	
Link resets transmitted	Indicates the number of link resets transmitted by this port.	Number	A link reset is a primitive sequence used during link initialization between ports. Besides indicating the load on a port, these measures also help determine how many ports have tried to establish a link with a particular port, and whether any link initialization attempt has failed.
Link resets received	Indicates the number of link resets received by this port.	Number	

3.3.3 Fiber Channel Port Status Test

Instantly detect changes in the port state, isolate ports that are operating at abnormal speeds, and be immediately notified of errors/problem conditions experienced by the ports with the help of the Port Status test mapped to this layer.

Target of the test : A Fibre Channel SAN Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each port on the SAN switch 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*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned UserName. This parameter once again appears only if the SNMPversion selected is **v3**.

Parameter	Description
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
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.

Parameter	Description
	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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Operational state of port</td><td>Indicates the current operational state of this port.</td><td></td><td>The table below summarizes the <b>State</b> values that this measure can report and their corresponding numeric equivalents:
<table>
<tr><th>State</th><th>Value</th></tr>
<tr><td>Offline</td><td>0</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Bypassed</td><td>4</td></tr>
<tr><td>Diagnostics</td><td>5</td></tr>
<tr><td>Online</td><td>100</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the above-mentioned <b>State</b>s while indicating the operational state of a port. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.
Use the detailed diagnosis of this measure to determine the exact state of the port.</td></tr>
<tr><td>Current health of port</td><td>Indicates the current health of this port.</td><td></td><td>The table below summarizes the State values that this measure can report and their corresponding numeric equivalents:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>State</th><th>Value</th></tr><tr><td>Warning</td><td>1</td></tr><tr><td>Failure</td><td>2</td></tr><tr><td>Unknown</td><td>3</td></tr><tr><td>Unused</td><td>4</td></tr><tr><td>Non participating</td><td>6</td></tr><tr><td>Initializing</td><td>7</td></tr><tr><td>Bypass</td><td>8</td></tr><tr><td>Ols</td><td>9</td></tr><tr><td>Ready</td><td>100</td></tr></table>
<b>Note:</b>
By default, this measure reports the above-mentioned <b>State</b>s while indicating the operational health of a port. However, in the graph of this measure, states will be represented using their corresponding numeric equivalents only.
Use the detailed diagnosis of this measure to determine the exact status of the port.
Moreover, if the detailed diagnosis of the Operational state measure reveals that a port is currently not in the online state, then the Current health of that port will be unknown.</td></tr>
<tr><td>Control status of port</td><td>Indicates the control status of this port.</td><td></td><td>The table below summarizes the <b>State</b> values that this measure can report and their corresponding numeric equivalents:</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>State</th><th>Value</th></tr><tr><td>Offline</td><td>0</td></tr><tr><td>Unknown</td><td>1</td></tr><tr><td>Invalid</td><td>2</td></tr><tr><td>Reset</td><td>3</td></tr><tr><td>Bypass</td><td>4</td></tr><tr><td>Unbypass</td><td>5</td></tr><tr><td>ResetCounters</td><td>8</td></tr><tr><td>Online</td><td>100</td></tr></table>
<b>Note:</b>
By default, this measure reports the above-mentioned <b>State</b>s while indicating the control status of a port. However, in the graph of this measure, control states will be represented using their corresponding numeric equivalents only.
Use the detailed diagnosis of this measure to determine the exact control status of the port.</td></tr>
<tr><td>Hardware status of port</td><td>Indicates the current status of the switch hardware.</td><td></td><td>The table below summarizes the State values that this measure can report and their corresponding numeric equivalents:
<table><tr><th>State</th><th>Value</th></tr><tr><td>TxFault</td><td>1</td></tr><tr><td>LinkDown</td><td>2</td></tr><tr><td>Failed</td><td>3</td></tr></table></td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><th>State</th><th>Value</th></tr><tr><td>Unknown</td><td>4</td></tr><tr><td>Bypass</td><td>5</td></tr><tr><td>Loopback</td><td>6</td></tr><tr><td>NoMedia</td><td>7</td></tr><tr><td>Active</td><td>100</td></tr><tr><td>Ready</td><td>100</td></tr></table>
Note:
By default, this measure reports the above-mentioned **State**s while indicating the hardware status of a port. However, in the graph of this measure, hardware states will be represented using their corresponding numeric equivalents only.
Use the detailed diagnosis of this measure to determine the exact hardware status of the port.</td></tr>
<tr><td>Port speed</td><td>Indicates the speed of the port.</td><td>KB/Sec</td><td>A sudden/consistent deteriorıation in speed could indicate a problem requiring further investigation.</td></tr>
<tr><td>Number of errors</td><td>Indicates the number of errors that have occurred on this port.</td><td>Number</td><td>Ideally, the value of this measure should be 0. A non-zero value indicates the existence of one/more problems with the port. A very high value is indicative of a problem-prone port.</td></tr>
<tr><td>Buffer full events</td><td>Indicates the number of times when all input buffers of this port were full.</td><td>Number</td><td></td></tr>
<tr><td>Link failures</td><td>Indicates the number of link failures experienced by this port.</td><td>Number</td><td>Ideally, the value of this measure should be 0.</td></tr>
<tr><td>Invalid frames received</td><td>Indicates the number of invalid frames that were</td><td>Number</td><td>Ideally, the value of this measure should be 0. A high value could indicate a bad</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	transmitted by this port.		physical link.
Invalid words transmitted	Indicates the number of invalid words that were transmitted by this port.	Number	Ideally, the value of this measure should be 0. A high value could indicate a bad physical link.
Signal loss count	Indicates the number of times a signal loss was detected at this port.	Number	
Synchronization loss count	Indicates the number of times a synchronization loss was detected at his port.	Number	Ideally, the value of this measure should be 0. If the value of this measure is high, then, you might want to take a look at the value reported by the Invalid words transmitted measure to check whether the physical link is really bad and if that caused the loss of synchronization.

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.