Monitoring Brocade SAN Switch

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Brocade SAN Switch is a 16-port embedded switch. It supports link speeds up to 2 Gbit/sec. The Brocade SAN Switch is based on the Brocade Fabric Operating System™ (Fabric OS) version 4.x, and is compatible with the entire Brocade SilkWorm product family. To ensure the health and performance of the Brocade SAN Switch, it is imperative that the operations of the Brocade SAN switch should be monitored 24 x 7. The eG Enterprise helps administrator in this task.

This document deals with how to manage and monitor the Brocade SAN Switch servers.

Chapter 2: How does eG Enterprise monitor Brocade SAN Switch?

The eG Enterprise is capable of monitoring the Brocade SAN Switch in an *agentless* manner using the using SNMP. The eG external agent periodically checks the SNMP MIB of the Brocade SAN Switch for fetching metrics related to the performance of the Brocade SAN Switch. This sections that follow describes how to manage and monitor the Brocade SAN Switch.

2.1 Managing the Brocade SAN Switch

The eG Enterprise cannot automatically discover a Brocade SAN Switch so that you need to manually add the component for monitoring. To manage a Brocade SAN 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 **COMPONENT** page that appears next, select *Brocade SAN Switch* as the **Component type**. Then, click the **Add New Component** button. This will invoke Chapter 2.

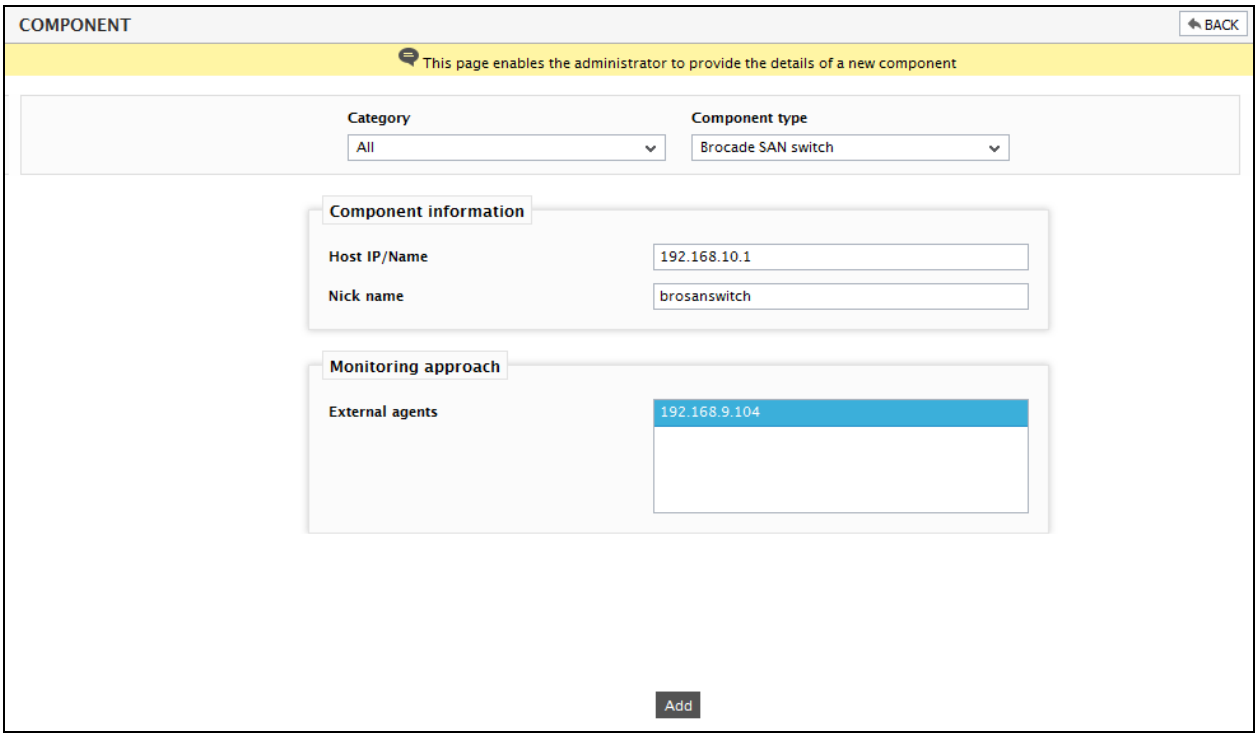

Figure 2.1: Adding a Brocade SAN Switch component

4. When you attempt to sign out, a list of unconfigured tests appears.

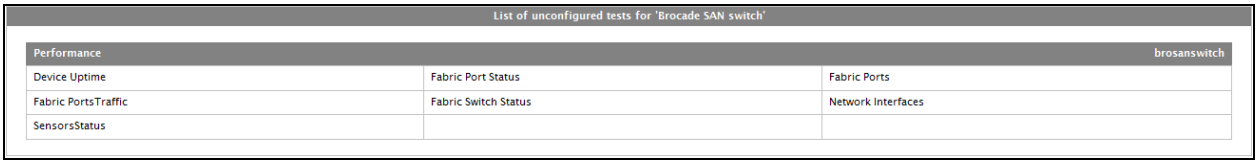

Figure 2.2: List of unconfigured tests to be configured for the Brocade SAN Switch

5. Click on any test in the list of unconfigured tests. For instance, click on the **Fibre Port Status** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.

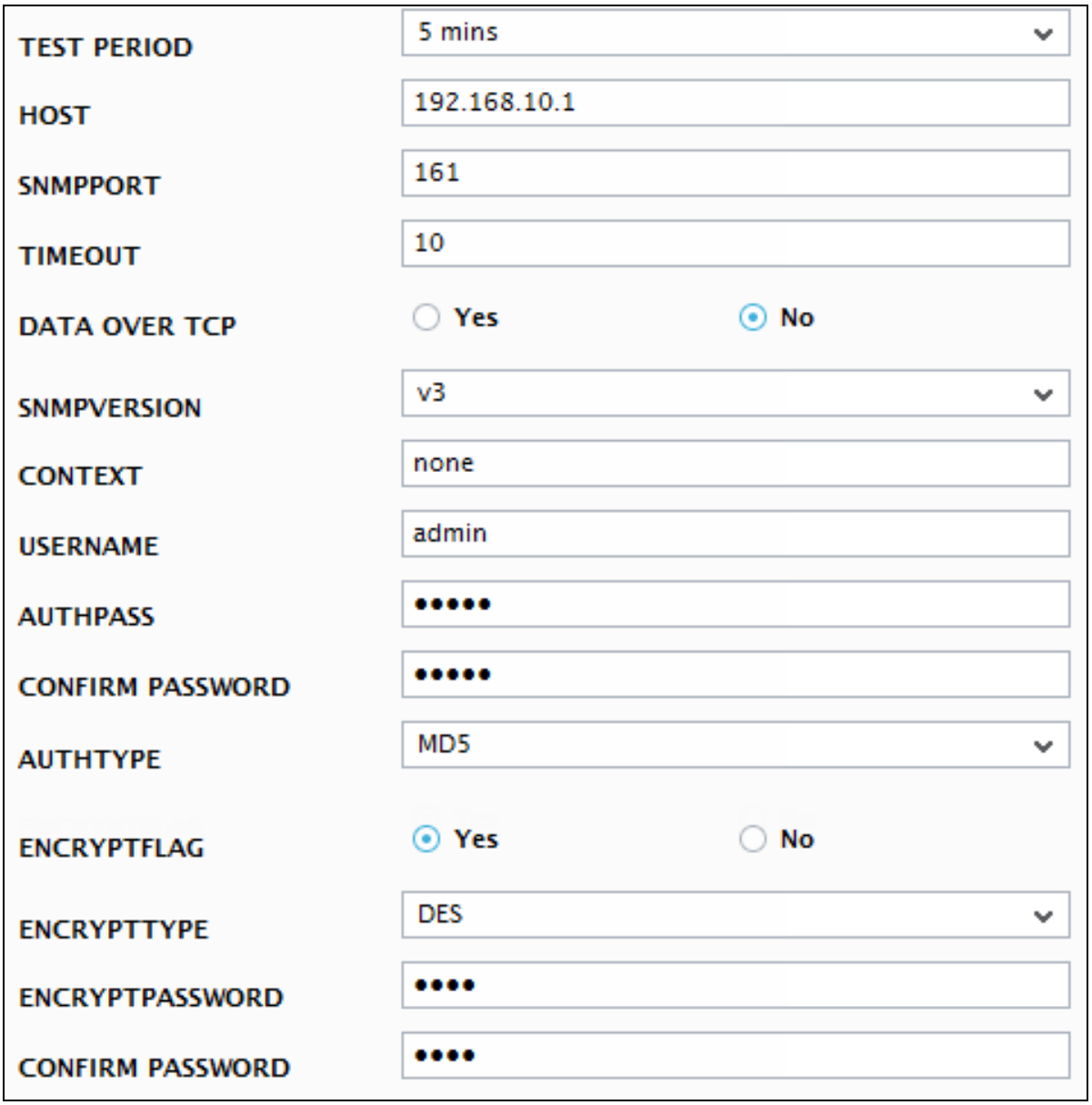

Figure 2.3: Configuring the Fibre Port Status test

To know how to configure the tests, refer to the **Monitoring Brocade SAN Switches** chapter. To know how to configure the **Device Uptime** test and **Network Interfaces** test, refer to *Monitoring Cisco Router* document.

6. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring Brocade SAN Switches

eG Enterprise embeds a specialized *Brocade SAN switch* monitoring model (see Figure 3.1), which enables users to run periodic status checks on the availability, hardware, and the fabric switches at the heart of the Brocade SAN switch, and reports problems (if any) with those components.

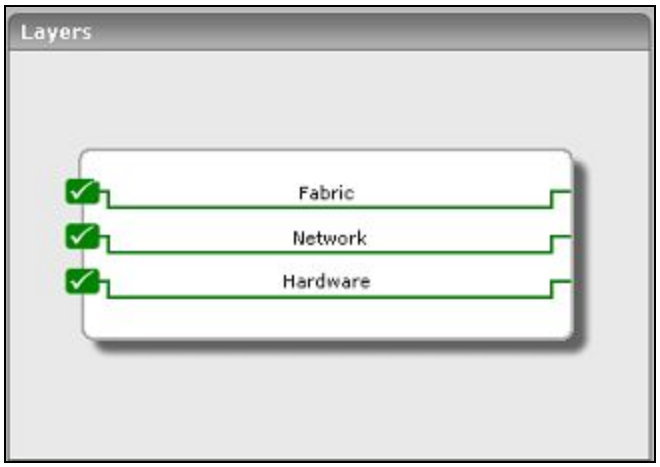

Figure 3.1: The layer model of the Brocade SAN switch

The sections to come discuss each layer of Figure 3.1 in great detail.

3.1 The Hardware Layer

This layer tracks the status of the different types of sensors on the switch (see Figure 3.2).

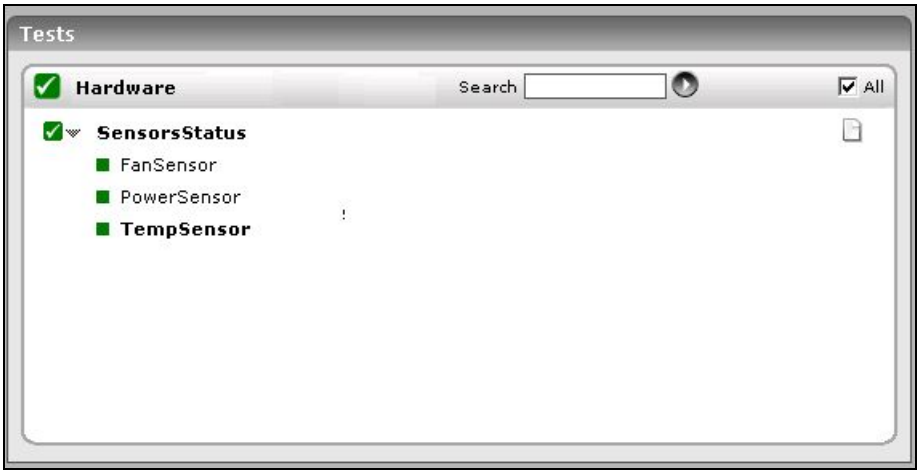

Figure 3.2: The tests mapped to the Hardware layer

3.1.1 Sensors Status Test

Sensors are of three types namely Fansensor, PowerSensor and TemperatureSensor. The SensorTest monitors each of the above-mentioned sensor types on the Brocade 48000 switch, and reports the number of sensors of every type that are in varying states of activity such as normal, faulty, unknown, or absent.

Target of the test : A Brocade 48000 switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for every type of sensor on the monitored Brocade 48000 switch

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the switch for which this test is to be configured.
Port	The port on which the switch is listening.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
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

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

Parameter	Description
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

Measurement	Description	Measurement Unit	Interpretation
Total sensors	The total number of sensors of this type currently available on the switch.	Number	The detailed diagnosis of this measure, if enabled, provides the complete details of sensors such as the Sensor ID, Sensor name, and the current state of the sensor.
Normal sensors	The number of sensors of this type that are currently in a normal state.	Number	
Unknown sensors	The number of sensors of this type that are currently in an unknown state.	Number	

Measurement	Description	Measurement Unit	Interpretation
Faulty sensors	The number of sensors of this type that are currently in a faulty state.	Number	Ideally, this value should be low.
Absent sensors	The number of sensors of this type that are currently absent.	Number	
New nomal sensors	The number of sensors of this type that were in the normal state during the last measurement period.	Number	
New unknown sensors	The number of sensors of this type that were in the unknown state during the last measurement period.	Number	
New faulty sensors	The number of sensors of this type that were faulty during the last measurement period.	Number	Ideally, this value should be low.
New absent sensors	The number of sensors of this type that were absent during the last measurement period.	Number	

3.2 The Network Layer

The tests mapped to this layer indicate whether the switch is available or not, how well the network interfaces supported by the switch are performing, and the uptime of the switch.

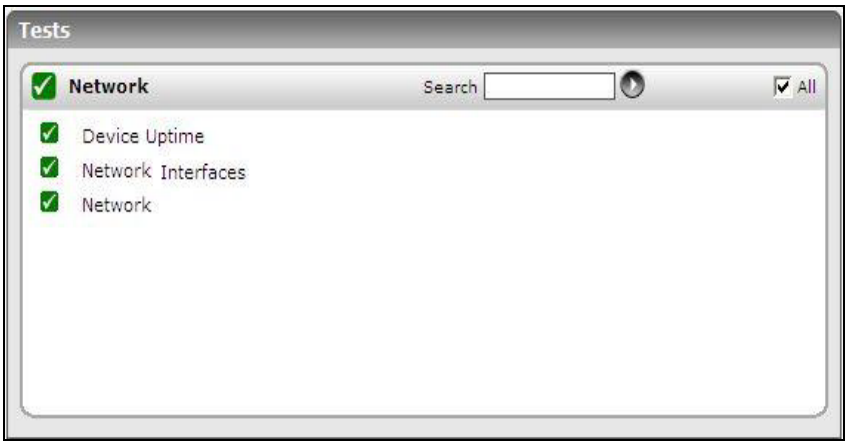

Figure 3.3: The test associated with the Network layer

The **Device Uptime** and **Network Interfaces** tests have been discussed in the *Monitoring Cisco Router* document. The details about the **Network** test is available in the *Monitoring Unix and Windows Servers* document.

3.3 The Fabric Layer

The heart of a SAN are Fibre Channel switches that provide any-to-any connectivity for servers and storage devices. Switch product lines range from entry- to enterprise-level to meet a wide range of changing business requirements. Two or more interconnected switches create a SAN fabric. Fabrics allow you to optimize your SAN for performance, scalability, and availability. Some switches include a high-value fabric operating system that provides intelligence, enabling advanced SAN fabric management, monitoring, and security. The tests associated with the **Fabric** layer report the health of the fabric switch (see Figure 3.4.

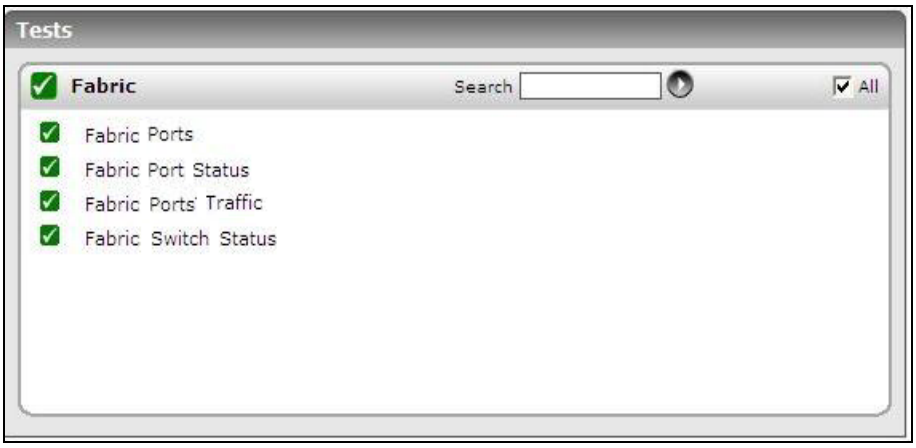

Figure 3.4: The tests associated with the Fabric layer

3.3.1 Fabric Ports Test

The FabricPorts test reports the current state of the ports available on the Fabric switch. Typically, a port on a Brocade 48000 switch can be in any of the following states:

- Online
- Offline
- Faulty
- Testing
- Unknown

Using this test, administrators can accurately determine how many ports are in a particular state of activity.

Target of the test : A Brocade 48000 switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Brocade 48000 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 switch for which this test is to be configured.
Port	The port on which the switch is listening.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
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

Parameter	Description
	SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVERSION. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard

Parameter	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Only Online Ports	By default, this flag is set to **No** . This implies that the test, by default, reports the count of online and offline ports. If you want the test to report the count of online ports alone (and not offline ports), set this flag to **Yes**. In this case, the test will report only the count of online ports and not offline ports.
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

Measurement	Description	Measurement Unit	Interpretation
Online ports	The total number of ports that are currently in the online state.	Number	
Offline ports	The number of ports that	Number	The detailed diagnosis of this

Measurement	Description	Measurement Unit	Interpretation
	are currently in the offline state.		measure, if enabled, lists the ports that are in an offline state.
Faulty ports	The number of ports that are currently faulty.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that are in a faulty state.
Ports under testing	The number of ports that are currently being tested.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that are in testing.
Unknown ports	The number of ports that are in the unknown state.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that are in an unknown state.
New online ports	The total number of ports that were online during the last measurement period.	Number	
New offline ports	The number of ports that were offline during the last measurement period.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that were in an offline state.
New faulty ports	The number of ports that were faulty during the last measurement period. .	Number	The detailed diagnosis of this measure, if enabled, lists the ports that were in a faulty state.
New testing ports	The number of ports that were in testing during the last measurement period.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that were in testing.
New unknown ports	The number of ports that were in the unknown state during the last measurement period.	Number	The detailed diagnosis of this measure, if enabled, lists the ports that were in an unknown state.

3.3.2 Fabric Port Status Test

Using this test, administrators can determine the current status of the ports on a fabric switch. The ports on a Brocade 48000 switch can be in the enabled, disabled, or loop back state. This test looks for the number of ports on the switch that are in each of the listed states.

Target of the test : A Brocade 48000 switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Brocade SAN switch 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 on which the switch is listening.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
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

Measurement	Description	Measurement Unit	Interpretation
Ports	The total number of ports that are in this state currently.	Number	The detailed diagnosis of this measure, if enabled, reveals the current state of every port on the fabric switch.

3.3.3 Fabric Switch Status Test

This test reports the status of the Fabric switch that is being monitored.

Target of the test : A Brocade 48000 switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Brocade 48000 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 switch for which this test is to be configured.
Port	The port on which the switch is listening.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

Parameter	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the 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: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

Parameter	Description
	selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Only Online Ports	By default, this flag is set to **No** . This implies that the test, by default, reports the count of online and offline ports. If you want the test to report the count of online ports alone (and not offline ports), set this flag to **Yes**. In this case, the test will report only the count of online ports and not offline ports.
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
Switch status	The current status of the switch.	Boolean	This Boolean value will be either 1 or 0. If it reports a value of 1, it implies that the switch is active or in an online state. If it reports a value of 0, it indicates that the switch is in the offline state or inactive mode.

3.3.4 Fabric PortsTraffic Test

This test is used to provide the port traffic statistics for the ports available in the Fabric switch.

Target of the test : A Brocade 48000 switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Brocade 48000 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 switch for which this test is to be configured.
Port	The port on which the switch is listening.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
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.
Only Online Ports	By default, this flag is set to **No** . This implies that the test, by default, reports the count of online and offline ports. If you want the test to report the count of online ports alone (and not offline ports), set this flag to **Yes**. In this case, the test will report only the count of online ports and not offline ports.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmitted	Indicates the total count of the number of Fibre Channel data that the port has transmitted in KB/sec.	KB/Sec	
Data received	Indicates the total count of the number of Fibre Channel data that the port has received in KB/sec.	KB/Sec	
Error count	Indicates the total number of count of the number of CRC errors detected for frames received.	Number	
Short data received	Indicates the total number of count of the number of truncated frames that the port has received.	Number	
Long data received	Indicates the total number of count of the number of received frames that are too long.	Number	
EOF data received	Indicates the total number of count of the number of received frames that are too long.	Number	
C3 discards received	Indicates the total number of count of the number of Class 3 frames that the port has discarded.	Number	

3.3.5 Fabric Event Status Test

This test reports the number and type of events that have occurred on the fabric switch of the Brocade SAN switch.

This test is disabled by default. To enable the test, go to the **ENABLE / DISABLE TESTS** page using the menu sequence : Agents -> Tests -> Enable/Disable, pick *Brocade SAN Switch* as the **Component type**, *Performance* as the **Test type**, choose the test from the **DISABLED TESTS** list, and click on the **>>** button to move the test to the **ENABLED TESTS** list. Finally, click the **Update** button.

Target of the test : A Brocade 48000 switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Brocade SAN switch 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 on which the switch is listening.
SNMPPort	The port at which the monitored target exposes its SNMP MIB;
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

Parameters	Description
	contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related

Parameters	Description
	to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
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
Critical events	The number of critical events that occurred on the fabric switch.	Number	
Error events	The number of errors that occurred on the fabric switch.	Number	
Warnings	The number of warning events that occurred on the fabric switch.	Number	
Information events	The number of information events that occurred on the fabric switch.	Number	
Debug events	The number of debug events that occurred on the fabric switch.	Number	

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.