Monitoring BlueCoat ProxySG

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Blue Coat ProxySG appliance securely isolates general-purpose servers from direct access, acting as an intermediary between web applications and the external clients who attempt to access them. To ensure clients uninterrupted access to critical web applications, eG Enterprise offers a dedicated Bluecoat ProxySG monitoring model (Figure 3.1) to serve complete monitoring support to the Bluecoat ProxySG appliance. To pull out the key performance metrics, this model enables running variety of tests, that are mapped to different layers, on the appliance. The metrics reported by these tests enable administrators to instantly find out the answers for the following performance quiries:

- How well the CPU is utilized on the appliance?
- What is the current state of each fan sensor and the speed of each fan?
- How well the memory of each memory module is utilized?
- What is the current state of each voltage sensor available in the modules of the target ProxySG?
- How well the resources are utilized?
- What is the current operational status of each fan?

This document will discuss about this specialied model in detail.

Chapter 2: How to Monitor Bluecoat ProxySG using eG Enterprise?

eG Enterprise uses a single eG external agent to monitor the BlueCoat ProxySG appliance. The external agent can be deployed on any remote host in the environment. This agent periodically tracks the SNMP traps and polls the SNMP MIB of the appliance to collect critical statistics pertaining to its performance. To enable the eG agent to communicate with the appliance, a set of pre-requisites needs to be kept in place. These requirements have been explained in the following section.

2.1 Pre-requisites for Monitoring the BlueCoat ProxySG

To ensure that the eG agent is able to use both the SNMP traps and the SNMP MIB of the BlueCoat ProxySG, the following pre-requisites should be fulfilled:

1. The SNMP service should be enabled on the ProxySG appliance;
2. The eG SNMP trap receiver service should be installed on the external agent host;
3. SNMP traps should be enabled on the ProxySG appliance and configured to send traps to the external agent host;

Once the above-said pre-requisites are fulfilled, proceed monitoring the ProxySG appliance. The broad steps for monitoring the ProxySG using eG Enterprise are as follows:

- Managing the BluCoat ProxySG
- Configuring the tests

These steps have been discussed in following sections.

2.2 Managing the BlueCoat ProxySG

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

1. Log into the eG administrative interface.
2. eG Enterprise cannot automatically discover the Bluecoat ProxySG. You need to manually add

the server using the **COMPONENTS** page (see Figure 2.1) that appears when the Infrastructure -> Components -> Add/Modify menu sequence is followed. Remember that components manually added are managed automatically.

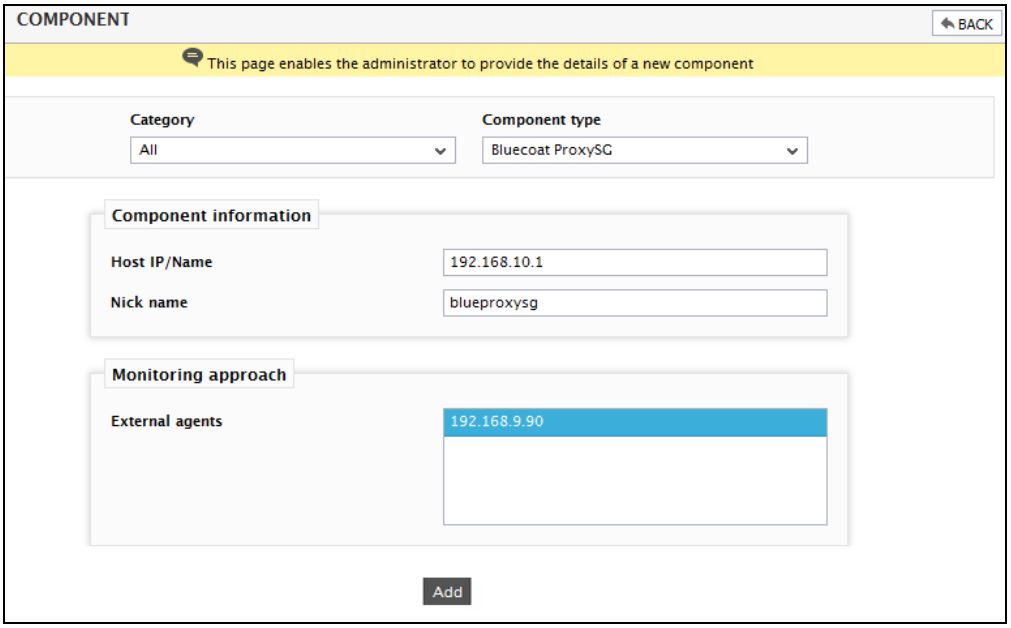

Figure 2.1: Adding the Bluecoat ProxySG

3. Specify the **Host IP/Name** and **Nick name** for the Bluecoat ProxySG in Figure 2.1. Then, click the **Add** button to register the changes.

2.3 Configuring the tests

1. When you attempt to sign out of eG administrative interface, a list of unconfigured tests will appear as shown in Chapter 2. This list reveals the unconfigured tests that require manual configuration.

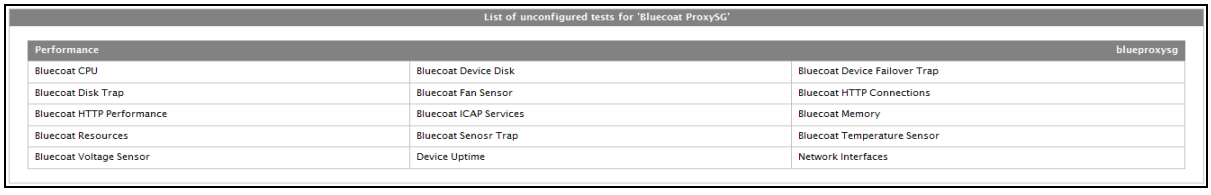

Figure 2.2: List of tests to be configured for Bluecoat ProxySG

2. To configure the tests, click on the test names in the list of unconfigured tests. For the details on configuring the tests, refer to **Monitoring the Bluecoat ProxySG** chapter.
3. Once all the tests are configured, signout of the eG administrative interface.

Chapter 3: Monitoring the Bluecoat ProxySG

Figure 3.1 shows the dedicated Bluecoat ProxySG monitoring model developed by eG Enterprise .

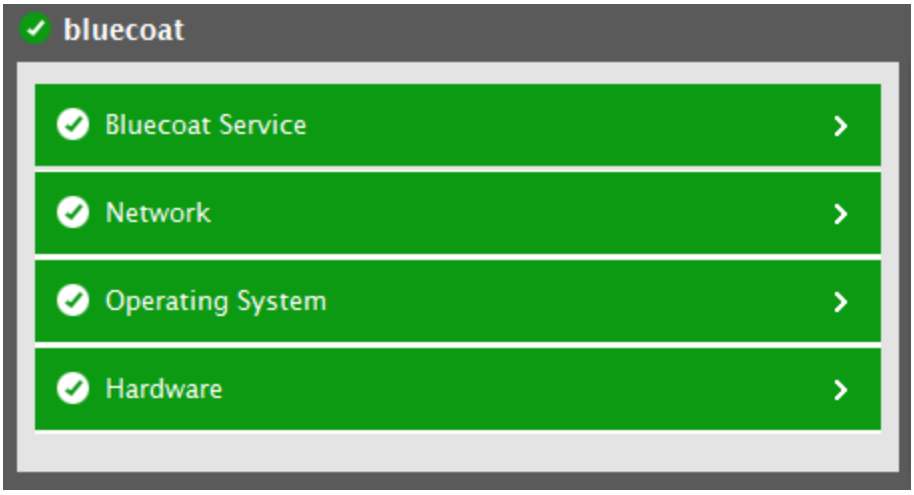

Figure 3.1: The layer model of the Bluecoat ProxySG

Every layer of Figure 3.1 is mapped to a variety of tests which connect to the SNMP MIB and the SNMP traps of the target Bluecoat ProxySG appliance to collect critical statistics pertaining to its performance. The sections to come will discuss each layer of Figure 3.1 in detail.

3.1 The Bluecoat Service layer

The tests pertaining to this layer tracks various statistics pertaining to the HTTP connections and ICAP services established between the target Bluecoat ProxySG and the clients. The details of these tests are discussed in the sections below.

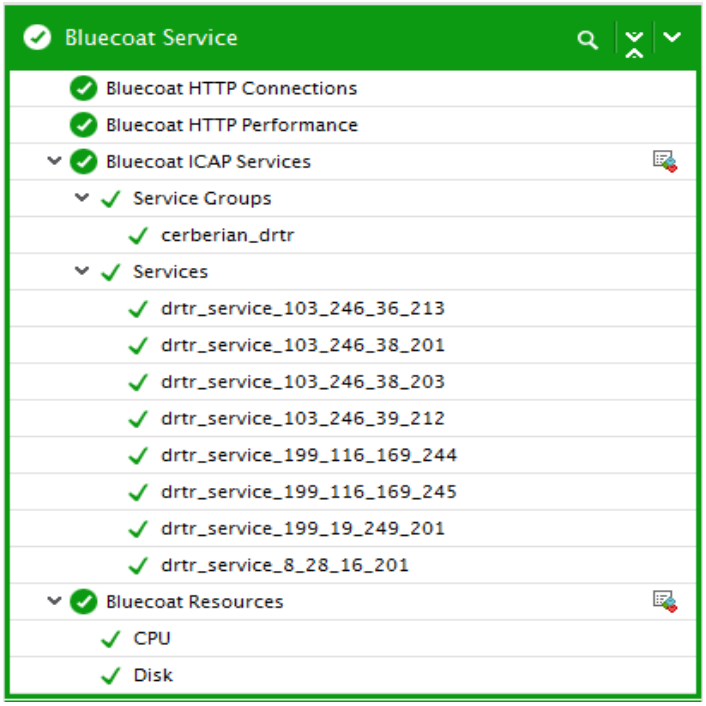

Figure 3.2: The tests associated with the Bluecoat Service layer

3.1.1 Bluecoat HTTP Connections Test

The Blucoat ProxySG appliance supports HTTP streaming. The HTTP connections are established through port 80 that allows you to send streaming data from the origin server to the clients. The HTTP connections established should be closely monitored over time to identify the HTTP connection load pattern on the appliance so that unusual traffic spikes can be spotted at ease. This can be achieved using the **Blucoat HTTP Connections** test!

This test continuously tracks the HTTP connections, and reports the total number of HTTP connections that are made to the appliance from the server and the clients. In addition, this test also reveals the count of HTTP connections that are currently active and are idle in the server side/client side.

Target of the test : A Bluecoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan sensor available in each module of the target Bluecoat ProxySG that is being monitored

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total client connections	Indicates the total number of HTTP connections that were established by the clients on the ProxySG appliance.	Number	
Active client	Indicates the number of	Number	The value of this measure should not

Measurement	Description	Measurement Unit	Interpretation
connections	currently active HTTP connections that were established by the clients on the ProxySG appliance.		exceed the value of *Total client connections* measure. If the value of this measure exceeds the *Total client connections* measure, then, the appliance begins to terminate idle persistent connections to allow the processing of new incoming requests. If the value of this measure exceeds the *Total client connections* measure when all connections are active, then, processing of incoming requests would be delayed until the processing of existing requests is complete.
Idle client connections	Indicates the number of HTTP connections (established by the clients) that were currently idle.	Number	
Total server connections	Indicates the total number of HTTP connections that were established on the ProxySG appliance from the sever.	Number	
Active server connections	Indicates the number of currently active HTTP connections that were established on the ProxySG appliance from the server.	Number	
Idle server connections	Indicates the number of HTTP connections (established from the server) that were currently idle.	Number	

3.1.2 Bluecoat HTTP Performance Test

This test tracks the performance of the HTTP connections established between the clients and the Bluecoat ProxySG appliance.

Target of the test : A Bluecoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Blue Coat ProxySG that is being monitored

Configurable parameters for the test

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

Parameters	Description
	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 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
Http request rate	Indicates the rate at which the HTTP requests were received from the client during the last measurement period.	Requests/sec	
Http hit rate	Indicates the rate at which the HTTP hits were produced by the client during the last measurement period.	Hits/Sec	
Http partial hit rate		Hits/Sec	
Http miss rate	Indicates the rate at which the HTTP hits were missed during the last measurement period.	Misses/Sec	
Http errors	Indicates the total number of errors occurred when the Http requests were established by the ProxySG during the last measurement period.	Errors	
Average http request	Indicates the average number of Http client requests received by the ProxySG per second during the last measurement period.	Requests/sec	
Http hit ratio	Indicates the percentage of hits generated by the client during the last measurement period.	Percent	
Data transmitted from client	Indicates the rate at which the amount of data was transmitted from the client to the ProxySG during the	MB/sec	

Measurement	Description	Measurement Unit	Interpretation
	last measurement period.		
Data received from proxy	Indicates the rate at which the amount of data was received by the client from the ProxySG during the last measurement period.	MB/sec	
Http request issued by proxy	Indicates the total number of Http requests made by the ProxySG during the last measurement period.	Requests/sec	
Http errors while fetching objects	Indicates the total number of errors occurred while fetching the objects from the remote server during the last measurement period	Errors	
Data transmitted from proxy	Indicates the rate at which the amount of data was transmitted to the remote servers during the last measurement period.	MB/sec	
Data received from remote server	Indicates the rate at which the amount of data was received from the remote server during the last measurement period.	MB/sec	
Average service time for all Http requests	Indicates the average time taken by the ProxySG to service for all the requests during the last measurement period.	Seconds	
Average service time for all Http hits	Indicates the average time taken by the ProxySG to service for the Http hits during the last measurement period.	Seconds	

Measurement	Description	Measurement Unit	Interpretation
Average service time for all Http partial hits	Indicates the average time taken by the ProxySG to service for the Http partial hits during the last measurement period.	Seconds	
Average service time for all Http misses	Indicates the average time taken by the ProxySG to service for the Http misses during the last measurement period.	Seconds	

3.1.3 Bluecoat ICAP Services Test

The ProxySG appliance utilizes the Internet Content Adaptation Protocol (ICAP) to hand off HTTP requests and/or responses to an external server for configured processing and transformation. When integrated with a supported ICAP server, the ProxySG appliance provides content scanning, filtering, and repair service for Internet-based malicious code. ICAP is an evolving architecture that allows an enterprise to dynamically scan and change Web content. To eliminate threats to the network and to maintain caching performance, the ProxySG sends objects to the integrated ICAP server for checking and saves the scanned objects in its object store. With subsequent content requests, the ProxySG serves the scanned object rather than rescan the same object for each request. This ability to immediately serve scanned content to users provides a considerable performance enhancement for networks that require content scanning. To ensure the continuous and secure content transactions, administrator need to constantly track the incoming and outgoing traffic between the ProxySG and the ICAP server. This way, administrator can promptly detect performance issues, so that the issues can be fixed before they prove fatal to the critical business networks. This is where the **Bluecoat ICAP Services** test helps administrator!

This test auto-discovers the ICAP services/service groups, and reports the metrics related to unecrypted and secured transactions for each ICAP service/service group. This test also reveals the requests that were serviced successfully and failed. Besides, this test sheds light on the amount of data that were transmitted and received between the ProxySG and the ICAP server.

Target of the test : A Bluecoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for the every ICAP service/service group that is being monitored

Configurable parameters for the test

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

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
Plain transaction	Indicates the rate at which the unencrypted ICAP	Transactions/sec	

Measurement	Description	Measurement Unit	Interpretation
	scanning transactions are made between ProxySG and ICAP server.		
Secure transaction	Indicates the rate at which encrypted ICAP scanning transactions are made between the ProxySG and the ICAP server.	Transactions/sec	
Plain request	Indicates the rate at which unencrypted requests were transferred between ProxySG and ICAP server during the last measurement period.	Requests/sec	
Secured request	Indicates the rate at which encrypted requests were transferred between ProxySG and ICAP server during the last measurement period.	Requests/sec	
Queued request	Indicates the total number of ICAP scanning transactions that are waiting for an available connection during the last measurement period	Requests/sec	
Deferred request	Indicates the rate at which the ICAP scanning requests that were deferred until full object received during the last measurement period.	Requests/sec	
Data transmitted	This measure defines the amount of data that has been transmitted from ICAP services or service groups during the last	MB/sec	

Measurement	Description	Measurement Unit	Interpretation
	measurement period.		
Data received	Indicates the rate at which the data was received from ICAP services or service groups during the last measurement period.	MB/sec	
Successful request	Indicates the total number ICAP transactions completed successfully during the last measurement period.	Requests/sec	
Failed request	Indicates the rate at which the ICAP transactions failed during the last measurement period.	Requests/sec	Ideally, the value of this measure should be zero.

3.1.4 Bluecoat Resources Test

Some of the few key resource dimensions that establish the health and performance characteristics of the Bluecoat ProxySG appliance include CPU, disk, memory, and network. These resources should be monitored at regular intervals to ensure uninterrupted operation of the ProxySG appliance. The **Bluecoat Resources** test helps administrators in this regard!

This test auto-discovers the resources such as disk, CPU, etc, available in the ProxySG appliance and enables administrators to figure out how resource hungry the ProxySG appliance is. For each resource, this test measures current status and the utilization percentage of the resource. If the ProxySG appliance is found to consume the resources excessively, then, this test helps administrators to take remedial actions swiftly to avoid performance bottlenecks of the ProxySG appliance.

Target of the test : A Bluecoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for each resource of the target Bluecoat ProxySG that is being monitored

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Resource status	Indicates the current state of this resource.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>OK</td><td>0</td></tr><tr><td>High</td><td>1</td></tr></table> **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current state of the resource. The graph of this measure however, represents the status of a resource using the numeric equivalents only - 0 and 1.
Resource usage	Indicates the utilization percentage of this resource.	Percent	If the value of this measure is close to 100%, it indicates that the resources in the appliance are depleting fast. Therefore, administrators may need to allocate additional resources to the appliance.

3.2 The Operating System layer

This layer tracks the CPU and memory utilization of the Bluecoat ProxySG, current status of the hardware elements etc. The tests of this layer are discussed in the forthcoming sections.

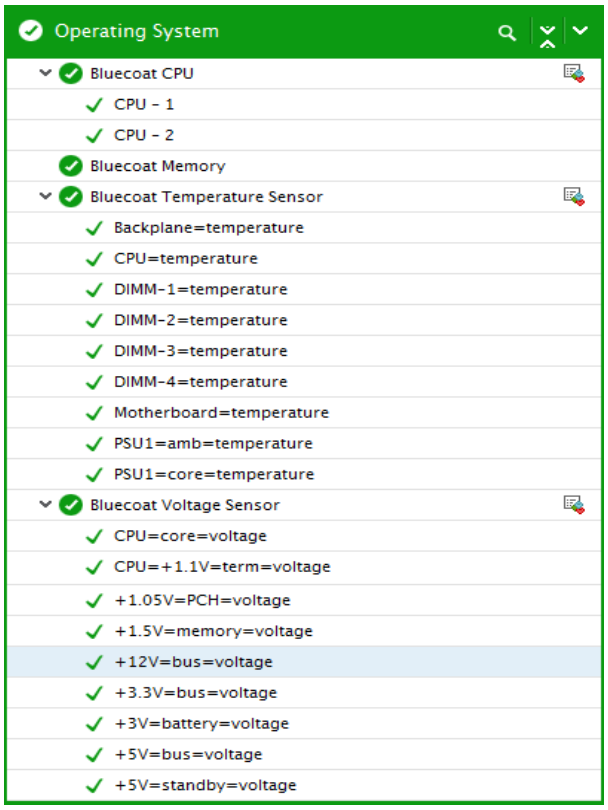

Figure 3.3: The tests associated with the Operating System layer

3.2.1 Bluecoat CPU Test

This test auto-discovers the CPUs available in the Bluecoat ProxySG and reports the utilization of each CPU. Using this test, administrators can figure out the CPUs that are highly utilized and can warrant further investigation to figure out the real reason behind the high utilization percentage of the CPUs.

Target of the test : A Bluecoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for each CPU of the target Bluecoat ProxySG that is being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed

Parameters	Description
Host	The host for which the 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 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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the utilization percentage of this CPU.	Percent	A value close to 100% indicates excessive usage of CPU. Compare the value of this measure across the CPUs to know which CPU is resource-intensive.

3.2.2 Bluecoat Memory Test

This test monitors the memory utilization of the Bluecoat ProxySG appliance and proactively alerts administrators to potential resource contention, if any.

Target of the test : A Bluecoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Bluecoat ProxySG that is being monitored.

Configurable parameters for the test

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

Parameters	Description
	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 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 memory	Indicates the total amount of memory allocated for the Bluecoat ProxySG appliance.	GB	
Memory used for system and other process	Indicates the amount of memory that is currently utilized by the appliance.	GB	A value close to the *Total memory* measure indicates that the memory resources are depleting rapidly.
Memory used for object caching	Indicates the amount of memory utilized for object caching in the appliance .	GB	
Memory utilization	Indicates the percentage of memory that is utilized by the appliance.	Percentage	If the value of this measure is close to 100%, it indicates that the memory utilization of the appliance is at its peak. Therefore, the administrator may need to allocate additional memory resources to the appliance.

3.2.3 Bluecoat Temperature Sensors Test

The Bluecoat ProxySG appliance is provided with built-in temperature sensors for each of the hardware modules such as CPU, power supply unit, motherboard and memory module. Whenever a temperature sensor detects abnormal temperature, then the hardware module corresponding to that temperature sensor is shutdown. If the hardware modules are shutdown frequently, then the performance of the appliance may degrade gradually. To avoid this, it is essential to monitor the operational state and the temperature of each module at regular intervals. The **Bluecoat Temperature Sensors** test helps administrators in this regard.

This test auto-discovers the temperature sensors of the appliance and reports the current status of each temperature sensor and the current temperature of each module detected by its corresponding temperature sensors.

Target of the test : A Blucoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for each temperature sensor available in each module of the target Bluecoat ProxySG appliance that is being monitored

Configurable parameters for the test

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

Parameters	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
Sensor status	Indicates the current state		The values reported by this measure

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>of this temperature sensor.</td><td></td><td>and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>OK</td><td>1</td></tr><tr><td>Unavailable</td><td>2</td></tr><tr><td>Non operational</td><td>3</td></tr></table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current state of the temperature sensor. The graph of this measure however, represents the status of a sensor using the numeric equivalents only - 1 to 3.</td></tr>
<tr><td>Temperature</td><td>Indicates the current temperature detected by this temperature sensor.</td><td>Celsius</td><td>Ideally, the value of this measure should be within the admissible temperature range.</td></tr>
</table>

3.2.4 Bluecoat Voltage Sensors Test

For a Bluecoat ProxySG appliance to function without a glitch, it is essential for the hardware modules to function properly. If any of the hardware modules do not function as expected due to abnormal voltage fluctuations, then that particular module will shutdown automatically. If the modules are frequently shutdown, then the overall performance of the Bluecoat ProxySG appliance may degrade drastically. To avoid this performance degradation, administrators should constantly keep a vigil on the voltage passing through each module. The **Bluecoat Voltage Sensors** test helps administrators in this regard. This test auto-discovers the voltage sensors in the modules of the appliance and reports the current status of each voltage sensor and the current voltage passing through each module.

Target of the test : A Blucoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for each voltage sensor available in each module of the target Bluecoat ProxySG that is being monitored

Configurable parameters for the test

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

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
Sensor status	Indicates the current state of this voltage sensor.		The values reported by this measure and its numeric equivalents are

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>mentioned in the table below:
<table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>OK</td><td>1</td></tr><tr><td>Unavailable</td><td>2</td></tr><tr><td>Non operational</td><td>3</td></tr></table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current state of the voltage sensor. The graph of this measure however, represents the status of a sensor using the numeric equivalents only - 1 to 3.</td></tr>
<tr><td>Voltage</td><td>Indicates the current voltage detected by this voltage sensor.</td><td>Volts</td><td></td></tr>
</table>

3.3 The Hardware Layer

This layer monitors the hardware components of the Bluecoat ProxySG such as disks and fans, and proactively alerts administrators to hardware failures.

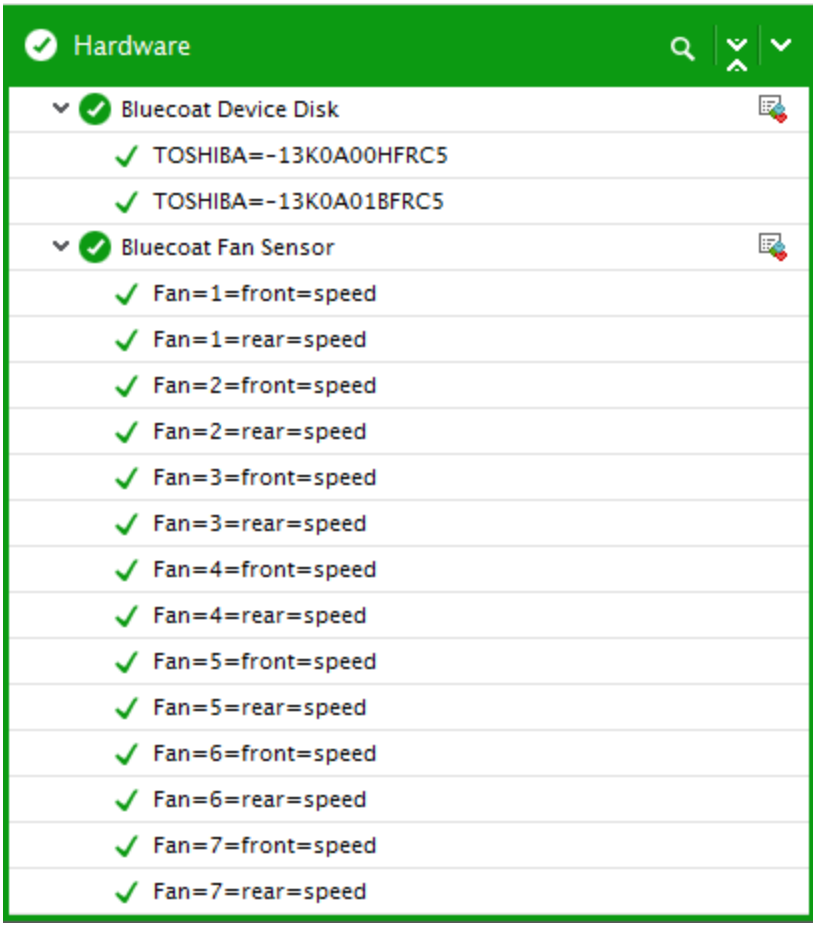

Figure 3.4: The tests mapped to the Hardware layer

3.3.1 Bluecoat Device Disk Test

This test auto-discovers the disks available in the target Bluecoat ProxySG appliance and reports the current operational status of each disk.

Target of the test : A Blucoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for each disk available in the target Bluecoat ProxySG that is being monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed

Parameters	Description
Host	The host for which the 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 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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Operation status	Indicates the current operational state of this disk.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** Present / 1

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure value</th><th>Numeric Value</th></tr>
<tr><td>Initializing</td><td>2</td></tr>
<tr><td>Inserted</td><td>3</td></tr>
<tr><td>Offline</td><td>4</td></tr>
<tr><td>Removed</td><td>5</td></tr>
<tr><td>Not present</td><td>6</td></tr>
<tr><td>Empty</td><td>7</td></tr>
<tr><td>IO error</td><td>8</td></tr>
<tr><td>Unused</td><td>9</td></tr>
<tr><td>Unknown</td><td>10</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current state of this disk. The graph of this measure however, represents the status of a disk using the numeric equivalents only - 1 to 10.
</td></tr>
</table>

3.3.2 Bluecoat Disk Trap Test

This test intercepts the disk failure traps sent by the Blue Coat ProxySG appliance, extracts relevant information related to the failure from the traps, and reports the count of disk failure events to the eG manager. This information enables administrators to detect the disk failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A Blue Coat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Blue Coat ProxySG that is to be monitored

Configurable parameters for the test

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>Test Period</td><td>How often should the test be executed</td></tr>
<tr><td>Host</td><td>The host for which the test is to be configured.</td></tr>
<tr><td>Port</td><td>The port at which the specified Host listens. By default, this is NULL.</td></tr>
<tr><td>Source Address</td><td>Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.</td></tr>
<tr><td>OID Value</td><td>Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.3417.2.2.2.0.1 and .1.3.6.1.4.1.3417.2.2.2.0.2. The values of these OIDs are as given hereunder:
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.3417.2.2.2.0.1</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.3417.2.2.2.0.2</td><td>NETWORK</td></tr>
</table>
In this case the oidvalue parameter can be configured as Trap1:.1.3.6.1.4.1.3417.2.2.2.0.1 -Host_system,Trap2:.1.3.6.1.4.1.3417.2.2.2.0.2-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.

An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.

Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.3417.2.2.2.0.1 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.3417.2.2.2.0.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID.1.3.6.1.4.1.3417.2.2.2.0.5, which in itself, say represents a failure condition, then your specification would be:</td></tr>
</table>

Parameters	Description
	Trap5: .1.3.6.1.4.1.3417.2.2.2.0.5-any. In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (.1.3.6.1.4.1.3417.2.2.2.0.4 and .1.3.6.1.4.1.3417.2.2.2.0.5) representing a failure condition needs to be monitored by the test, then, your specification should be: Trap6:..1.3.6.1.4.1.3417.2.2.2.0.4;.1.3.6.1.4.1.3417.2.2.2.0.5-any. Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.
ShowOID	Specifying **True** against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **False**, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
TrapOIDs	By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the Trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Disk failure count	Indicates the number of times the disk failure event was triggered during the last measurement period.	Number	The failure events may be generated due to the failure of disks of the ProxySG appliance. If the failure events are not rectified within a certain pre-defined timeperiod, the ProxySG appliance will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the ProxySG appliance.

3.3.3 Bluecoat Failover Trap Test

This test intercepts the failover failure traps sent by the Blue Coat ProxySG appliance, extracts relevant information related to the failure from the traps, and reports the count of failover failure events to the eG manager. This information enables administrators to detect the failover failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A Blue Coat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Blue Coat ProxySG that is to be monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
Port	The port at which the specified Host listens. By default, this is *NULL*.
Source Address	Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.

<table>
<tr><th>Parameters</th><th>Description</th></tr>
<tr><td>OID Value</td><td>Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: 1.3.6.1.4.1.3417.2.13.2.0.1 and 1.3.6.1.4.1.3417.2.13.2.0.2. The values of these OIDs are as given hereunder:

<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>1.3.6.1.4.1.3417.2.13.2.0.1</td><td>Host_system</td></tr>
<tr><td>1.3.6.1.4.1.3417.2.13.2.0.2</td><td>NETWORK</td></tr>
</table>

In this case the OIDvalue parameter can be configured as Trap1:.1.3.6.1.4.1.3417.2.13.2.0.1-Host_system,Trap2:1.3.6.1.4.1.3417.2.13.2.0.2-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.

An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.

Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID 1.3.6.1.4.1.3417.2.13.2.0.1 is found to be hostT and not Host_system, then the test ignores OID 1.3.6.1.4.1.3417.2.13.2.0.1 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID 1.3.6.1.4.1.3417.2.13.2.0.5, which in itself, say represents a failure condition, then your specification would be:

Trap5: 1.3.6.1.4.1.3417.2.13.2.0.5-any.

In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.3417.2.13.2.0.4 and 1.3.6.1.4.1.3417.2.13.2.0.5) representing a failure condition needs to be monitored by the test, then, your specification should be:

Trap6:.1.3.6.1.4.1.3417.2.13.2.0.4;1.3.6.1.4.1.3417.2.13.2.0.5-any.

Here, a semi-colon is used as a separator to separate the OIDs and the value should be specified after the last OID.</td></tr>
<tr><td>ShowOID</td><td>Specifying True against ShowOID will ensure that the detailed diagnosis of this test</td></tr>
</table>

Parameters	Description
	shows the OID strings along with their corresponding values. If you enter False, then the values alone will appear in the detailed diagnosis page, and not the OIDs.
TrapOIDs	By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified Source Addresses. To make sure that the agent considers only specific traps received from the Source Address, then provide a comma-separated list of OIDs in the TrapOIDs text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is 1:1. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Bluecoat device failover count	Indicates the number of times the failover failure event was triggered during the last measurement period.	Number	The failure events may be generated due to the failure of failover of the ProxySG appliance. If the failure events are not rectified within a certain pre-defined timeperiod, the ProxySG appliance will not be able to function

Measurement	Description	Measurement Unit	Interpretation
			continuously and will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the ProxySG appliance.

3.3.4 Bluecoat Fan Sensors Test

This test auto-discovers the fans of the target Bluecoat ProxySG appliance and reports the current status of the sensor available in each fan. In addition, this test also reports the speed at which each fan operates. Using this test, administrators can easily determine fan failures by identifying the fans that are currently running at abnormal speed.

Target of the test : A Blucoat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan sensor available in each module of the target Bluecoat ProxySG that is being monitored

Configurable parameters for the test

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

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

Parameters	Description
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
Sensor status	Indicates the current state of this fan sensor.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** OK – 1 Unavailable – 2 Non operational – 3 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current state of this fan sensor. The graph of this measure however, represents the status of a fan sensor using the numeric equivalents only - 1 to 3.
Speed	Indicates the current speed of this fan.	RPM	Ideally, the speed of the fan should be within admissible range. An abnormal speed is an indication of the

Measurement	Description	Measurement Unit	Interpretation
			malfunctioning of the fan and administrators should therefore replace the fans immediately for the smooth functioning of the appliance.

3.3.5 Bluecoat Sensor Trap Test

This test intercepts the sensor failure traps sent by the Blue Coat ProxySG appliance, extracts relevant information related to the failure from the traps, and reports the count of sensor failure events to the eG manager. This information enables administrators to detect the sensor failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A Blue Coat ProxySG

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Blue Coat ProxySG that is to be monitored

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
Port	The port at which the specified Host listens. By default, this is *NULL*.
Source Address	Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
OID Value	Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, DisplayName:OID-OIDValue. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.3417.2.13.2.0.1 and .1.3.6.1.4.1.3417.2.13.2.0.2. The values of these OIDs are as given hereunder:

Parameters	Description

OID	Value
.1.3.6.1.4.1.3417.2.13.2.0.1	Host_system
.1.3.6.1.4.1.3417.2.13.2.0.2	NETWORK

In this case the OIDvalue parameter can be configured as Trap1:.1.3.6.1.4.1.3417.2.13.2.0.1-Host_system,Trap2:.1.3.6.1.4.1.3417.2.13.2.0.2-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.

An * can be used in the OID/value patterns to denote any number of leading or trailing characters (as the case may be). For example, to monitor all the OIDs that return values which begin with the letter 'F', set this parameter to Failed:*-F*.

Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.3417.2.13.2.0.1 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.3417.2.13.2.0.1 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.3417.2.13.2.0.5, which in itself, say represents a failure condition, then your specification would be:

Trap5: .1.3.6.1.4.1.3417.2.13.2.0.5-any.

In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (.1.3.6.1.4.1.3417.2.13.2.0.4 and .1.3.6.1.4.1.3417.2.13.2.0.5) representing a failure condition needs to be monitored by the test, then, your specification should be:
Trap6:.1.3.6.1.4.1.3417.2.13.2.0.4;.1.3.6.1.4.1.3417.2.13.2.0.5-any.

Trap6:.1.3.6.1.4.1.3417.2.13.2.0.4;.1.3.6.1.4.1.3417.2.13.2.0.5-any.

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

ShowOID — Specifying **True** against ShowOID will ensure that the detailed diagnosis of this test shows the OID strings along with their corresponding values. If you enter **False**, then the values alone will appear in the detailed diagnosis page, and not the OIDs.

TrapOIDs — By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent

Parameters	Description
	considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the Trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, *94.2*,*.1.3.6.1.4.25*, where * indicates leading and/or trailing spaces.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Sensor failure count	Indicates the number of times the sensor failure event was triggered during the last measurement period.	Number	The failure events may be generated due to the failure of sensors of the ProxySG appliance. If the failure events are not rectified within a certain pre-defined timeperiod, the ProxySG appliance will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the ProxySG appliance.

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.