Monitoring Riverbed SteelHead

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction to Riverbed SteelHead Monitoring

Riverbed SteelHead appliance is used to improve the performance of distributed client-server systems. SteelHead appliances can be deployed in minutes. They are completely transparent and can be installed in the data path or out-of-path, without interfering with your applications. Whether you have a hub-and-spoke or mesh topology, you can begin by installing just two appliances, and then roll out additional boxes to key sites in your enterprise, as required. You can also deploy SteelHead appliances all at once at every site. Traffic is automatically optimized when another SteelHead appliance is installed on the other side of the WAN.

SteelHead appliance is ideal for organizations that want to improve application performance and data transfers served over a wide area network. The series is engineered for seamless network integration into remote sites and data centers, with scalable performance designed to support a growing number of users, devices, and data.

You can use this appliance as an application-performance barrier. For instance, if you are an international Navy needing to optimize communication with a distributed fleet or an enterprise building out your private cloud, the SteelHead appliance delivers the performance and ROI necessary to ensure your project's success.

This means that even the slightest dip in the performance of Riverbed SteelHead can adversely impact user experience with the application. To avoid this, administrators should continuously measure the performance of the appliance, instantly detect anomalies, and fix them before users notice. This is where eG Enterprise helps. eG Enterprise notifies administrators of abnormalities in appliance performance, so that they can promptly intervene and do the needful to resolve them.

Chapter 2: How Does eG Enterprise Monitor Riverbed SteelHead?

eG Enterprise monitors Riverbed SteelHead using an agent- based approach. For this purpose, you need to install an eG agent on your host system.

The broad steps for monitoring the Riverbed SteelHead using eG Enterprise are as follows:

1. Manage the Riverbed SteelHead using the eG admin interface
2. Configure the tests for the component.

The sections to come will discuss about the tests mapped to Riverbed SteelHead.

2.1 Managing Riverbed SteelHead

To manage the Riverbed SteelHead , do the following:

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

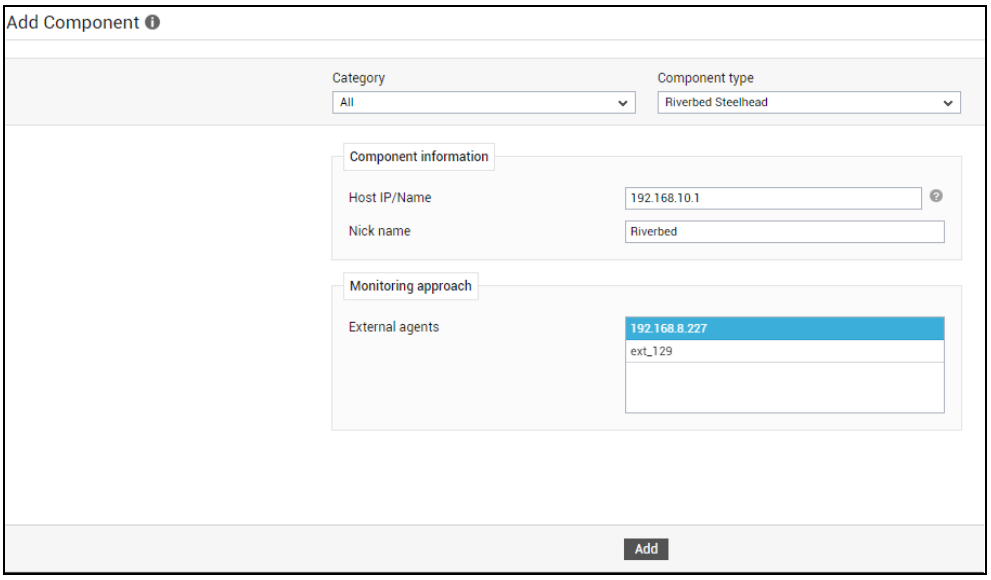

Figure 2.1: Adding the Riverbed SteelHead

4. Specify the **Host Name** and **Nick name** for the Riverbed SteelHead .
5. Next, assign a **External Agent** to the component.
6. Finally, click the **Add** button to add the Riverbed SteelHead to the eG Enterprise system. Components manually added will be automatically managed by eG Enterprise.

2.2 Configuring Tests

Once the Riverbed SteelHead is managed, try to do the following:

1. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
2. Select the **Show managed component types** only check box and then select the *Riverbed SteelHead* component under **Component Type** list box. Then, the record appears in the grid as shown in Figure 2.2.

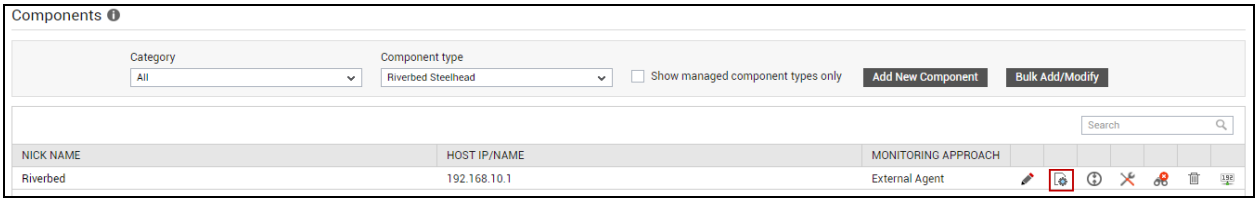

Figure 2.2: Managed Riverbed SteelHead record

3. Select the Configure Tests icon as shown in Figure 2.2 in the grid to configure the tests mapped

for the component. This will invoke Figure 2.3 listing all the configured tests for the Riverbed SteelHead.

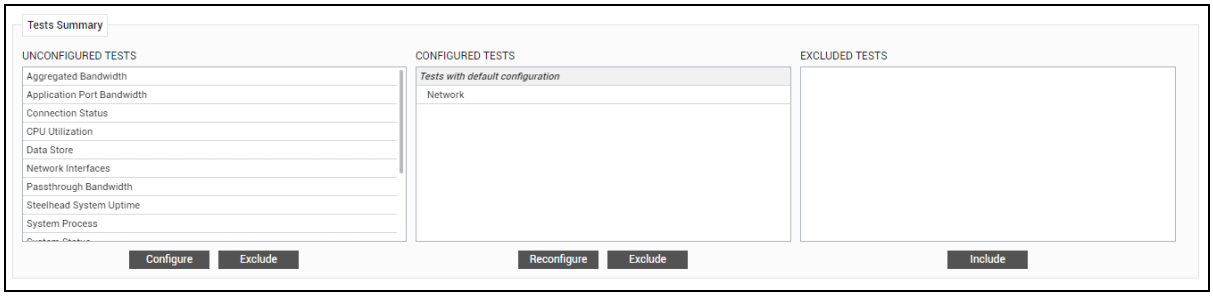

Figure 2.3: The list of unconfigured tests for the Riverbed SteelHead

Click on any test to configure it and sign out of the eG admin interface.

Chapter 3: Monitoring Riverbed SteelHead

eG Enterprise offers a dedicated monitoring model for Riverbed SteelHead which periodically monitors the system status, connection status, application traffic, CPU usage, Data Store and uptime of the appliance.

Figure 3.1: Riverbed SteelHead Layer

Using the metrics reported by the tests mapped to this layer, administrators can find quick and accurate answers to certain persistent performance queries, such as the following:

- Is Riverbed SteelHead appliance available?
- How long the appliance has been up since the last reboot?
- How well the CPU is utilized by the SteelHead appliance?
- Is the Data Store running without space?
- How much network traffic has been generated by the Source and Destination IPs? Which IP address is responsible for generating the maximum load?
- How much network traffic has generated by the application? Which application port is consuming maximum bandwidth?
- What is the current status of the processes running on the Riverbed SteelHead appliance?

3.1 The SteelHead Services Layer

Using the tests mapped to this layer, administrators can closely monitor the connection status, system status and processes that are running on the system.

Figure 3.2: The tests mapped to the SteelHead Services layer

3.1.1 Connection Status Test

This test displays the number of connection types (such as optimized, pass through, active, half-opened, half-closed, established, etc.) that pass through this device and alert administrators to promptly capture abnormalities in the device.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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

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

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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Optimized connection	Indicates the number of optimized connections.	Number	Optimized connections are connections that process request quickly by first searching in local cache i.e. datastore. If the request is available in datastore, data is fetched from the datastore. The request goes to the WAN, only on unavailability of that request in datastore. An optimized connection includes Half-closed, Half-opened, Active, Idle and Established connections in it.
Passthrough connection	Indicates the number of unoptimized connections that pass through.	Number	Passthrough connections are connections that process request directly to WAN instead of searching in datastore i.e. local cache. Since the search request happens in WAN, which is time consuming, the passthrough connection will be an unoptimized one.
Half-Opened connection	Indicates the number of half opened active connections.	Number	Half-opened connection is nothing but a TCP connection in which the connection has not been fully established. If you are experiencing a large number of half-opened

Measurement	Description	Measurement Unit	Interpretation
			connections, consider a more appropriately sized SteelHead.
Half-Closed connection	Indicates the number of half closed active connections.	Number	Half-closed connections are connections that the SteelHead has intercepted and optimized but are in the process of being disconnected. If you are experiencing a large number of half-closed connections, consider a more appropriately sized SteelHead. **Note:** Half-closed connections might remain if the client or server doesn't close its connections cleanly.
Established connection	Indicates the number of established connections.	Number	Established connection is nothing but a newly forming, initiating connections available in the Riverbed SteelHead device. The connection is being established but doesn't yet have an inner channel.
Active connection	Indicates the number of active connections.	Number	An abnormally high value for this measure could indicate a probable virus or spam attack to this device.
Total connection	Indicates the total number of connections that pass through this device.	Number	This measure is a sum total of all optimized connections.

3.1.2 System Status Test

Abnormal temperature of the device often lead to the malfunctioning of the device, which when left unnoticed may affect the overall health of the system. In addition, intermittent breaks in the service indicates that the service has been running without reboot for a long time. The **System Status** test helps administrators to tackle these issues!.

This test reports the overall health of the device, service status, uptime and temperature of the device.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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.

Parameter	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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current health status of the		The values that this measure reports and their corresponding numeric values

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td>device.</td><td></td><td>are listed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Healthy</td><td>10000</td></tr><tr><td>Degraded</td><td>30000</td></tr><tr><td>Admission Control</td><td>31000</td></tr></table>
Note:
By default, this measure reports the Measure Values discussed in the table above to indicate the health status of the Riverbed SteelHead device. In the graph of the measure however, the health status is indicated using the corresponding numeric equivalents only.</td></tr>
<tr><td>Service status</td><td>Indicates the current service status of the device.</td><td></td><td>The values that this measure reports and their corresponding numeric values are listed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>None</td><td>0</td></tr><tr><td>Unmanaged</td><td>1</td></tr><tr><td>Running</td><td>2</td></tr><tr><td>SentCom1</td><td>3</td></tr><tr><td>SentTerm1</td><td>4</td></tr><tr><td>SentTerm2</td><td>5</td></tr><tr><td>SentTerm3</td><td>6</td></tr><tr><td>Pending</td><td>7</td></tr><tr><td>Stopped</td><td>8</td></tr></table>
Note:</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure reports the **Measure Value**s discussed in the table above to indicate the service status of the Riverbed SteelHead device. In the graph of the measure however, the device service status is indicated using the corresponding numeric equivalents only.
Temperature	Indicates the current temperature of the target device.	Celsius	A sudden increase in temperature can impact the functioning of a device and must be immediately attended to.
Service uptime	Indicates the time at which the service was started for optimization.	Minutes	A low value is indicative of intermittent breaks in the availability of a service. Administrators may wish to be alerted if a particular service has been running without a reboot for a very long period.

3.1.3 System Process Test

For each critical system resource that is monitored (CPU, memory, disk space, disk activity, and bandwidth), this test promptly detects and reports the resource usage bottlenecks and the severity of these bottlenecks. Using this test, administrators can figure out how effectively the resources are utilized and the overall status of the processes that are running on the Riverbed SteelHead device.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for each process of the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.

Parameter	Description
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 • **SHA** – Secure Hash Algorithm

Parameter	Description
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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of the process that are running on the device.		The values that this measure reports and their corresponding numeric values are listed in the table below: Measure Value: Unknown — Numeric Value: 0 Measure Value: Running — Numeric Value: 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>Unmanaged</td><td>2</td></tr>
<tr><td>Stopped</td><td>3</td></tr>
</table>
Note:
By default, this measure reports the Measure Values discussed in the table above to indicate the status of the process. The graph of this measure however, is represented using the numeric equivalents only.
</td></tr>
<tr><td>Number of failure</td><td>Indicates the total number of times the process has crashed or exited unexpectedly.</td><td>Number</td><td>Ideally this value should be zero. A high value indicates that the server is being overloaded or there has been a network performance degradation.</td></tr>
</table>

3.2 The SteelHead Statistics Layer

Using the tests mapped to this layer, administrators can closely monitor the bandwdith of the Application, Port and Data Store related information.

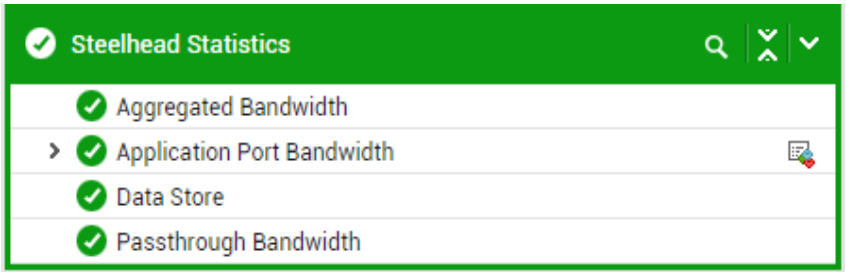

Figure 3.3: The tests mapped to the SteelHead Statistics layer

3.2.1 Aggregated Bandwidth Test

Aggregate bandwidth is the total data transfer rate of both device ports. Using this test, administrators can report the consolidated values obtained from multiple application ports during

receiving and transmission process over WAN to LAN and LAN to WAN.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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*.

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

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Optimized data received in WAN to LAN	Indicates the amount of aggregated data which has been received through device over WAN to LAN.	MB/sec	Comparing these values across device, helps you to identify the IPs that are used for receiving the data's and are bandwidth-intensive.
Optimized data received in LAN to WAN	Indicates the amount of aggregated data which has been received through device over LAN to WAN.	MB/sec	
Optimized data transmitted in WAN to LAN	Indicates the amount of aggregated data which has been transmitted through device over WAN to LAN.	MB/sec	Comparing these values across device, helps you to identify the IPs that are used for transmitting the data's and are bandwidth-intensive.
Optimized data transmitted in LAN to WAN	Indicates the amount of aggregated data which has been transmitted through device over LAN to WAN.	MB/sec	

3.2.2 Application Port Bandwidth Test

Monitoring bandwidth is one of the most critical aspects of network management and traffic monitoring software. Without comprehensive insight into traffic type and bandwidth utilization, it is not possible to ensure proper availability of bandwidth.

This test reports the following information:

- Determine the applications and hosts taking up critical bandwidth.
- Assist with identifying unauthorized applications.
- Ensure critical applications receive enough bandwidth.

Using this test, administrators can plan for spikes in usage, identify bandwidth-hogging applications and ensure critical applications get the requisite amount of bandwidth.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for each application port of the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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.

Parameter	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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Optimized data received in WAN to	Indicates the amount of data that has been	MB/sec	Comparing these values across the device to identify the inbound traffic

Measurement	Description	Measurement Unit	Interpretation
LAN	received through application port over WAN to LAN.		flowing from the WAN to the LAN.
Optimized data received in LAN to WAN	Indicates the amount of data that has been transmitted through application port over WAN to LAN.	MB/sec	
Optimized data transmitted in WAN to LAN	Indicates the amount of data that has been received through application port over LAN to WAN.	MB/sec	Comparing these values across the device to identify the outbound traffic flowing from the LAN to the WAN.
Optimized data transmitted in LAN to WAN	Indicates the amount of data that has been transmitted through application port over LAN to WAN.	MB/sec	

3.2.3 Data Store Test

SteelHeads transparently intercept and analyze all of your WAN traffic. TCP traffic is segmented, indexed, and stored as segments of data, and the references representing that data are stored on the **RiOS data store** within SteelHeads on both sides of your WAN. After the data has been indexed, it is compared to data already on the disk. Segments of data that have been seen before aren't transferred across the WAN again; instead a reference is sent in its place that can index arbitrarily large amounts of data, thereby massively reducing the amount of data that needs to be transmitted. One small reference can refer to megabytes of existing data that has been transferred over the WAN before. This is what Data store does in Riverbed SteelHead device!

This test auto-discovers the data store and reports the details about the hits and misses that happened in Riverbed SteelHead device. It also alerts the administrators about the data stores that are running without space.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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

Parameter	Description
	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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Total hits	Indicates the total number of hits measured on the data store per second during last measurement	Hits/sec	A high value is desired for this measure. A very low value is a cause for concern, as it indicates that cache usage is very poor; this in turn implies

Measurement	Description	Measurement Unit	Interpretation
	period.		that direct disk accesses, which are expensive operations, are high.
Total miss	Indicates the total number of misses measured on the data store per second during last measurement period.	Misses/sec	A high value of this measure can cause performance degradation of the system and increases latency, because you need to read the cache first instead of disc for data.
Disk utilization	Indicates the percentage of disk utilized for the data store operations.	Percent	A value of 100% is a cause of concern, as it indicates that the disk is running out of space.

3.2.4 Passthrough BandwidthTest

This test reports the amount of data that were passed unoptimized and reports the bandwidth utilized for passing those data. Using this test, administrators can identify those resources for which traffic has been consistently bandwidth-intensive

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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.

Parameter	Description
Username	This parameter appears only when **v3** is selected as the SNMPversion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types:

Parameter	Description
	• **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmission over WAN to LAN	Indicates the amount of data that has been passed through the device over WAN to LAN.	MB/sec	This measure indicates the amount of bandwidth utilized during inbound traffic flowing from the WAN to the LAN. A higher value is a cause of concern as it affects the system performance.
Data transmission over LAN to WAN	Indicates the amount of data that has been passed through the device over LAN to WAN	MB/sec	This measure indicates the amount of bandwidth utilized during outbound traffic flowing from the LAN to the WAN. A higher value is a cause of concern as it affects the system performance.
Total data transmission	Indicates the total amount of data transmission done without optimization.	MB/sec	This measure is a sum total of bandwidth utilized by both inbound and outbound traffic.

3.3 The Flow StatisticsLayer

Using the tests mapped to this layer, administrators can closely monitor the inbound and outbound traffic of the appliance.

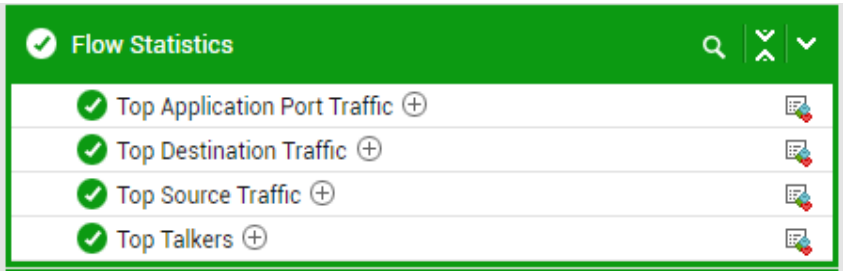

Figure 3.4: The tests mapped to the Flow Statistics layer

3.3.1 Top Application Port Traffic Test

One of the key challenges that network administrators face every day is identifying the application ports that are bandwidth- intensive and the root- cause for traffic congestion. The **RbtSteelTopPortTest** test helps administrators tackle this challenge!

This test auto-discovers the top-n application ports (in terms of volume of traffic they generate) and reports those application ports that are consuming maximum bandwidth and those that could probably be choking the network link.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for each port for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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.

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.
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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Generated traffic	Indicates the amount of traffic generated on the specified application port.	GB	Compare the value of this measure across application ports to identify which application ports is contributing to the high level of network traffic.

3.3.2 Top Destination Traffic Test

This test auto-discovers the destination's (in terms of volume of traffic) and reports the data traffic leading to or coming from that destination. This way, the test points you to the destinations that generate the maximum traffic. The bandwidth used by each destination when receiving / transmitting data is also reported, so that you can quickly identify those destinations for which traffic has been consistently bandwidth-intensive.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for each destination IP for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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**.

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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Received traffic	Indicates the amount of traffic received on the destination configured on the SteelHead device.	GB	Compare the value of this measure across destinations to identify which destination host is contributing to the high level of network traffic.

3.3.3 Top Source Traffic Test

This test auto-discovers the source hosts whose interactions with other hosts in the environment are resulting in large volumes of data being transmitted over a network interface. In the event of a network slowdown, you can use this test to isolate those hosts that are engaged in bandwidth-intensive transactions with other hosts, and could hence be contributing to the slowdown.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for each source IP for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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

Parameter	Description
	3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard

Parameter	Description
	• **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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Generated traffic	Indicates the amount of traffic generated from the source across SteelHead device.	GB	Compare the value of this measure across sources to identify which source host is contributing to the high level of network traffic.

3.3.4 Top Talkers Test

The traffic flows that generate the heaviest use of WAN bandwidth are known as the Top Talkers. A traffic flow consists of data sent and received from a first single IP address and port number to a second single IP address and port number over the same protocol.

This test reports the information about traffic flows that happens between source and destination IPs. Using this test, administrators can track down the top talking I P's that are generating most traffic in our network.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for each combination of source and destination for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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.

Parameter	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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Data transmission	Indicates the amount of data transmission flows	GB	Compare the value of this measure across all IPs to identify the IPs that

Measurement	Description	Measurement Unit	Interpretation
	measured on the top talkers.		are overutilizing WAN and creating traffic.

3.4 The Network Layer

Using the tests mapped to this layer, administrators can closely monitor the network related details such as the uptime of the system.

Figure 3.5: The tests mapped to the Network layer

3.4.1 SteelHead System Uptime Test

In most production environments, it is essential to monitor the uptime of critical network devices in the infrastructure. By tracking the uptime of each of the devices, administrators can determine what percentage of time a device has been up. Comparing this value with service level targets, administrators can determine the most trouble-prone areas of the infrastructure.

In some environments, administrators may schedule periodic reboots of their network devices. By knowing that a specific device has been up for an unusually long time, an administrator may come to know that the scheduled reboot task is not working on a device.

This **RbtSteelUptimeTest** test monitors the uptime of critical network devices.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Riverbed SteelHead device is being monitored.

Configurable parameters for the test

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

Parameter	Description
Host	The IP address of the target host to be monitored.
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

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

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Has the system been rebooted?	Indicates whether the device has been rebooted during the last measurement period or not.	Boolean	If this measure shows 1, it means that the device was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this SteelHead device was rebooted.
Total uptime of the	Indicates the total time that	Minutes	Administrators may wish to be alerted

Measurement	Description	Measurement Unit	Interpretation
system	the device has been up since its last reboot.		if the device has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.
Uptime during the last measure period	Indicates the time period that the device has been up since the last time this test ran.	Seconds	If the device has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the server was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the server was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period - the smaller the measurement period, greater the accuracy.

3.5 The Hardware Layer

Using the tests mapped to this layer, administrators can closely monitor the hardware related details such as the trap events that had occurred in the device and the CPU usage details.

Figure 3.6: The tests mapped to the Hardware layer

3.5.1 CPU Utilization Test

This test measures the CPU utilization of the target Riverbed SteelHead device. Using this test, administrators can figure out the average CPU utilization of the device thus helping them analyze CPU utilization patterns of the target device.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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

Parameter	Description
	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 to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Avg usage in the past minute	Indicates the average percentage of CPU utilized over the last minute.	Percent	A gradual/sudden increase in the value of this measure is a cause of concern which could eventually result in the failure of the CPU.

3.5.2 Trap Event Details Test

SNMP Traps are alert messages sent from a remote SNMP-enabled device to a central collector, the “SNMP manager”. Trap messages are the main form of communication between an SNMP Agent and an SNMP Manager. They are used to inform an SNMP manager when an important event happens at the Agent level. A benefit of using Traps for reporting alarms is that they trigger instantaneously, rather than waiting for a status request from the manager.

This test reports and captures the trap events occurring in the device. Using this test, administrators can capture the count and details of critical information, warning, and critical events that are generated on the Riverbed SteelHead device.

Target of the test : A Riverbed SteelHead

Agent deploying the test : An external agent

Outputs of the test : One set of results for each event that occurred on the Riverbed SteelHead device is being monitored.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the target host to be monitored.
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	Description
	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 selecting an option from the EncryptType list. SNMP v3 supports the following

Parameter	Description
	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**.

Measures made by the test

Measurement	Description	Measurement Unit	Interpretation
Total events	Indicates the number of trap messages of this event that were sent from this system.	Number	The detailed diagnosis of this measure if enabled, lists the name and details of each event like Sender, Trap Time, Trap Type, etc.

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.