Monitoring Juniper EX Switch

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Juniper EX Series Ethernet switches deliver access, aggregation, and core layer switching services in branch, campus, and data center networks to ensure fast, secure, reliable delivery of data and applications.

All EX Series Ethernet Switches address escalating demands for high availability, unified communications, mobility and virtualization within enterprise networks. The EX Series switches increase competitiveness and contribute to business success by delivering operational efficiency, business continuity, and network agility for end-to-end enterprise environments.

If this switch, which assures service operators of continuous network connectivity and secure transaction of business, starts malfunctioning suddenly, the connection to mission-critical services will be lost, thereby causing irreparable damage to reputation and revenue. It is therefore imperative that the operations of the Juniper Ex Switch are monitored 24 x 7. This can be easily achieved using eG Enterprise.

Chapter 2: How to Monitor Juniper EX Switch Using eG Enterprise?

eG Enterprise adopts agentless approach to monitor the Juniper EX Switch. A single eG external agent is all that is required to monitor a firewall. This agent, when deployed on a remote host, executes tests that connect to the SNMP MIB of the switch to be monitored, and collects statistics of interest from it. The key pre-requisite for monitoring the is to SNMP enable the switch. Once this requirement is kept in place, start monitoring the switch. There are two broad steps for monitoring the switch:

- Managing the Juniper EX Switch
- Configuring the tests

2.1 Managing the Juniper EX Switch

The eG Enterprise cannot automatically discover the Juniper EX Switch. 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 add a Juniper EX Switch, do the following:

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

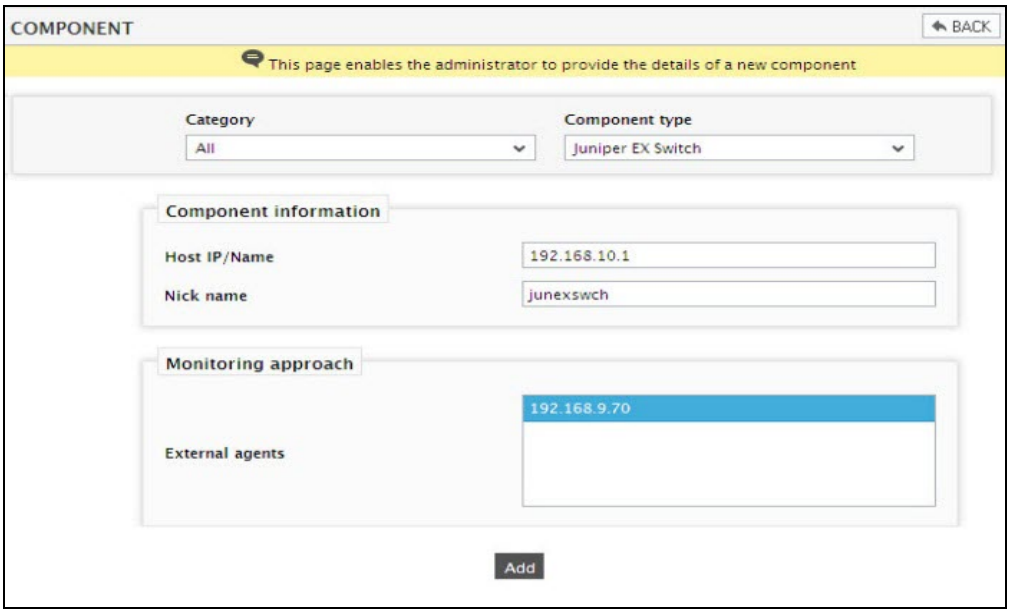

Figure 2.1: Adding a Juniper EX Switch server

4. Specify the **Host IP** and the **Nick name** of the Juniper EX Switch server in Figure 2.1. Then click the **Add** button to register the changes.

2.2 Configuring the tests

1. When you attempt to sign out, a list of unconfigured tests will appear as shown in Figure 2.2.

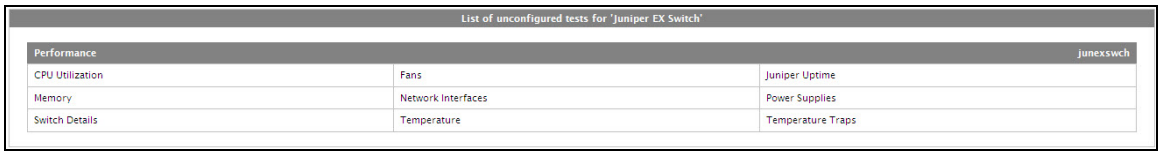

Figure 2.2: List of Unconfigured tests to be configured for the Juniper EX Switch server

2. Click on the tests to configure them. To know how to configure these tests, refer to the **Monitoring Juniper EX Switch** chapter.
3. To configure the details on configuring the **Network Interfaces** test, refer to *Monitoring Cisco Router* document.
4. Once the **Network Interfaces** test is configured, signout of the eG administrative interface.

Chapter 3: Monitoring Juniper EX Switch

eG Enterprise provides a specialized Juniper EX Switch monitoring model (see Figure 3.1), which periodically polls the SNMP MIB of the switch to measure the CPU usage, temperature and memory of each hardware component of the switch and notifies administrators of potential resource crunches and failures of the power supply, fans etc.

Figure 3.1: The layer model of the Juniper EX Switch

Using the metrics reported , administrators can find quick and accurate answers for the following performance questions:

- Is the CPU utilization of each hardware component optimal? If not, which hardware component is utilizing the emaximum CPU?
- Which hardware component is consuming the maximum memory resources? Is the buffer memory and heap memory allocated to each hardware component utilized effectively?
- Is the temperature maintained optimally for all the hardware components of the Juniper EX Switch?
- Is any VPN tunnel hogging the bandwidth resources? If so, which one is it?
- Are too many fragmented packets flowing through the firewall? If so, why? Is it because of an incorrect configuration?
- What is the mode of the routing engine available in the Juniper EX Switch?

The **Network** layer of the Juniper EX Switch model is similar to that of a Windows Generic server model. The tests associated to the **Network** layer have been dealt with in the *Monitoring Unix and Windows Servers* document.

3.1 The Operating System Layer

This layer tracks the current CPU usage, memory, temperature and the uptime of each hardware component of the Juniper EX Switch. Besides this, this layer helps you in identifying the number of trap messages that were sent by the switch for failures of the power supply units , fans and abnormal deduction in temperature of the hardware components.

Figure 3.2: The tests mapped to the Firewall Service layer

3.1.1 CPU Utilization Test

This test monitors the current CPU utilization of each hardware component available in the Juniper EX Switch and reports whether/not the hardware component is consuming too much of CPU resources.

Target of the test : A Juniper EX Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each hardware component of the Junpier EX Switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.

Parameter	Description
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the 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

Parameter	Description
	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 percentage of CPU utilized by this hardware component.	Percent	A very high value of this measure indicates a CPU bottleneck. Comparing the value of this measure across the hardware components will help you in identifying the component that is using the CPU resources at its maximum.

3.1.2 Uptime Test

This test measures the uptime of each hardware component of the Juniper EX Switch and reports administrators if any hardware component has been running without reboot for a longer period of time.

Target of the test : A Juniper EX Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each hardware component of the Juniper EX Switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP

Parameter	Description
	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.
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

Parameter	Description
	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
Uptime	Indicates the total time this hardware component has been up since the last reboot.	Mins	Administrators may wish to be alerted if a hardware component has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

3.1.3 Memory Test

This test reports the total memory allocated to each hardware component of the target Juniper EX Switch. Using this test, you can monitor the buffer memory utilization and heap memory utilization of each hardware component. This way, you can identify the hardware component that is running short of memory.

Target of the test : A Juniper EX Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each hardware component of the target Juniper EX Switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.

Parameter	Description
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the 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

Parameter	Description
	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
Memory	Indicates the total memory allocated to this hardware component.	MB	
Buffer utilization	Indicates the percentage of buffer memory utilized by this hardware component.	Percent	A low value is desired for this measure. A gradual/sudden increase in the value of this measure is a cause of concern which indicates that the buffer memory is running short of resources. You can either increase the size of the buffer memory or free up the space that is already utilized to contain the

Measurement	Description	Measurement Unit	Interpretation
			value of this measure within possible limits. Comparing the value of this measure across the hardware components will help you in identifying the hardware component that is utilizing the memory resources extensively.
Heap utilization	Indicates the percentage of heap memory utilized by this hardware component.	Percent	

3.1.4 Temperature Test

This test monitors the temperature of each hardware component of the target Juniper EX switch and alerts if any abnormalities are detected.

Target of the test : A Juniper EX Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each hardware component of the Juniper EX Switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen

Parameter	Description
	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 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**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Temperature	Indicates the current temperature of this hardware component.	Celsius	A gradual/sudden increase in the value of this measure is a cause of concern which could eventually result in the failure of the hardware component.

3.1.5 Temperature Traps Test

Temperature fluctuation of hardware components, if not promptly detected and resolved, can prove to be fatal to the availability and overall health of a Juniper EX Switch. This test intercepts the temperature traps sent by the hardware components of the switch, extracts information related to temperature errors/failures from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect current temperature and potential failure of the hardware components due to a sudden shoot up of temperature, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A Juniper EX Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event that occurred on the target Juniper EX Switch.

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.
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: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

In this case the OIDValue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-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 .1.3.6.1.4.1.9156.1.1.2 is found to be host and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 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 .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then

Parameters	Description
	your specification would be: Trap5: .1.3.6.1.4.1.9156.1.1.5-any. In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be: Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-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.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Temperature alerts	Indicates the number of times this event was triggered during the last measurement period.	Number	The failure events may be generated due to the temperature failure of the hardware components of the Juniper EX Switch. If the failure events are not rectified within a certain pre-defined timeperiod, the switch will be

Measurement	Description	Measurement Unit	Interpretation
			shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Juniper EX Switch.

3.1.6 Power Supplies Test

The chassis of the Juniper EX Switch is a rigid sheet-metal structure that houses the hardware components. The field-replaceable units (FRUs) in the EX series switches are:

- Power supply
- Fan tray
- Uplink module
- SFP transceiver
- SFP+ transceiver
- XFP transceiver

The power supply in the switches is a hot-removable and hot-insertable field-replaceable unit (FRU) that you can install on the rear panel without powering off the switch or disrupting the switching function. Some of the EX series switches have an internal redundant power supply, making the power supply fully redundant.

Abnormal power fluctuation to the hardware components often lead to the malfunctioning of the Juniper EX Switch which when left unnoticed can prove to be fatal to the availability and overall health. This test intercepts the traps sent by the switch, extracts information related to power supply failures from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the abnormalities in the power supply if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A Juniper EX Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of event that occurred on the target Juniper EX Switch.

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>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: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:
<table>
<tr><th>OID</th><th>Value</th></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr>
<tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr>
</table>
In this case the OIDValue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-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 .1.3.6.1.4.1.9156.1.1.2 is found to be host and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 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 .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:

Trap5: .1.3.6.1.4.1.9156.1.1.5-any.</td></tr>
</table>

Parameters	Description
	In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be: Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-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.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Failed power supplies	Indicates the number of times this event was triggered due to power supply failure during the last measurement period.	Number	The failure events may be generated due to the failure of the Power supply units of the Juniper EX Switch. If the failure events are not rectified within a certain pre-defined timeperiod, the switch will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Juniper EX Switch.

3.1.7 Fans Test

EX4200 switches have a single fan tray on the rear panel. The fan tray is a hot-removable and hot-insertable field-replaceable unit (FRU): You can remove and replace it without powering off the switch or disrupting switch functions.

The fan tray used in the switch comes with load-sharing redundancy that can tolerate a single fan failure at room temperature (below 113° F/45° C) to still provide sufficient cooling.

Under normal operating conditions, the fans in the fan tray run at less than full speed. If a fan fails or the ambient temperature rises above the threshold 113° F (45° C), the speed of the remaining fans is automatically adjusted to keep the temperature within the acceptable range, 32° F (0° C) through 113° F (45° C).

The system raises an alarm if the fan fails or if the ambient temperature inside the chassis rises above the acceptable range. If the temperature inside the chassis rises above the threshold temperature, the system shuts down automatically.

This test intercepts the fan failure traps sent by the switch, extracts relevant information related to the failure from the traps, and reports the count of these trap messages to the eG manager. This information enables administrators to detect the fan failures if any, understand the nature of these failures, and accordingly decide on the remedial measures.

Target of the test : A Juniper EX Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each type of failure event that occurred on the target Juniper EX Switch.

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.
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: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

<table><tr><th>OID</th><th>Value</th></tr><tr><td>.1.3.6.1.4.1.9156.1.1.2</td><td>Host_system</td></tr><tr><td>.1.3.6.1.4.1.9156.1.1.3</td><td>NETWORK</td></tr></table>
In this case the OIDValue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-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 .1.3.6.1.4.1.9156.1.1.2 is found to be host and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 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 .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:

Trap5: .1.3.6.1.4.1.9156.1.1.5-any.

In some cases, multiple trap OIDs may be associated with a single value. For instance, if two different OIDs (1.3.6.1.4.1.9156.1.1.4 and 1.3.6.1.4.9156.1.1.5) representing a failure condition needs to be monitored by the test, then, your specification should be:

Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-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 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.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Failed fans	Indicates the number of events of this type that were triggered during the last measurement period.	Number	The failure events may be generated due to the failure of the fans of the Juniper EX Switch. If the failure events are not rectified within a certain pre-defined timeperiod, the storage system will be shutdown automatically. Ideally, the value of this measure should be zero. A high value is an indication of performance degradation of the Juniper EX Switch.

3.2 The JEX Service Layer

This layer tracks the CPU mode of each routing engine available in the Juniper EX Switch.

Figure 3.3: The tests mapped to the JEX Service layer

3.2.1 Switch Details Test

The Routing Engine runs the Junos OS. Software processes that run on the Routing Engine maintain the routing tables, manage the routing protocols used on the router, control the router interfaces, control some chassis components, and provide the interface for system management and user access to the router.

You can install one or two Routing Engines in the router. Each Routing Engine must be installed directly into an SCB. A USB port on the Routing Engine accepts a USB memory device that allows you to load Junos OS. The Routing Engines install into the front of the chassis in vertical slots directly into the SCBs labeled 0 and 1. If two Routing Engines are installed, one functions as the master and the other acts as the backup. If the master Routing Engine fails or is removed and the backup is configured appropriately, the backup takes over as the master.

This test reports the mode of each routing engine available in the Juniper EX Switch.

Target of the test : A Juniper EX Switch

Agent deploying the test : An external agent

Outputs of the test : One set of results for each hardware component of the Junpier EX Switch that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in

Parameter	Description
	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
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

Parameter	Description
	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
Mode	Indicates the mode of this routing engine.		The values reported by this measure and their numeric equivalents are available in the table below: **Measure Value** / **Numeric Value** Unknown – 1 Master – 2 Backup – 3 Disabled – 4 **Note:**

Measurement	Description	Measurement Unit	Interpretation
			This measure reports the **Measure Value**s listed in the table above to indicate the mode of this routing engine. However, in the graph of this measure, the mode of the routing engine is indicated using only the **Numeric Value**s listed in the above table.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.