



Monitoring Juniper DX Device

eG Innovations Product Documentation

www.eginnovations.com



Table of Contents

CHAPTER 1: INTRODUCTION	1
CHAPTER 2: HOW DOES EG ENTERPRISE MONITOR JUNIPER DX DEVICE?	2
2.1 Managing the Juniper DX Device	2
2.2 Configuring the tests	3
CHAPTER 3: MONITORING THE JUNIPER DX DEVICE	5
3.1 The Operating System Layer	5
3.1.1 SysHost Test	5
3.2 The Network Layer	8
3.3 The DX System Layer	8
3.3.1 System Stats Test	9
3.4 The DX Cluster Layer	12
3.4.1 Cluster HTTP Test	13
3.4.2 ClusterHttpStats Test	15
3.4.3 Cluster I/O Test	18
3.4.4 Cluster SSL Test	21
3.4.5 Cluster Status Test	24
3.5 The DX Target Servers Layer	26
3.5.1 Target Server Status Test	27
3.5.2 Target Server I/O Test	29
3.5.3 Target Server Response Test	31
3.5.4 Target Server SSL Test	34
3.5.5 Target Server Http Test	37
ABOUT EG INNOVATIONS	40

Table of Figures

Figure 2.1: Adding a Juniper DX device	3
Figure 2.2: A list of unconfigured tests	3
Figure 2.3: Configuring the Target Server Status test	4
Figure 3.1: Layer model of the Juniper DX device	5
Figure 3.2: The test associated with the Operating System layer	5
Figure 3.3: The tests associated with the Network layer	8
Figure 3.4: The tests associated with the DX System layer	9
Figure 3.5: The tests associated with the DX Cluster layer	12
Figure 3.6: The tests associated with the DX Target Servers layer	26

Chapter 1: Introduction

The DX Application Acceleration Platform represents a new concept in web server acceleration. It addresses the inefficiencies in server architecture, network architecture, and network protocols that limit the performance of your web site and web servers. The DX appliance solves these inefficiencies by providing its own highly-optimized network architecture and breakthrough data optimization and connection handling capabilities to make your web pages download faster and your web servers more efficient than ever before.

This implies that persistent/even intermittent glitches in the functioning of the DX device could cause a marked deterioration in web server performance. Therefore, continuous monitoring of the device and timely problem detection becomes imperative. This is where the eG Enterprise helps big time.

Chapter 2: How does eG Enterprise Monitor Juniper DX Device?

By executing a wide variety of tests on the DX device and thoroughly analyzing the critical performance metrics extracted from the SNMP-MIB exposed by the device, the eG Enterprise suite promptly identifies probable issues with the device and proactively cautions administrators of it, so that any damage - big or small - is averted in time.

- The eG Enterprise is capable of monitoring the Juniper DX device in *agentless* manner.
- The Juniper DX devices are managed manually using the eG administrative interface.

Before attempting to monitor the DX device, make sure that above pre-requisites are kept in place. There are two broad steps for monitoring the Infoblox appliance;

- Managing the Juniper DX Device
- Configuring the tests

These steps are explained in the following sections.

2.1 Managing the Juniper DX Device

The eG Enterprise cannot automatically discover a Juniper DX device so that you need to manually add the component for monitoring. To manage a Juniper DX component, do the following:

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

COMPONENT

BACK

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

Category

All

Component type

Juniper DX

Component information

Host IP/Name

192.168.10.1

Nick name

junidx

Monitoring approach

External agents

192.168.9.70

Add

Figure 2.1: Adding a Juniper DX device

- 4. Specify the **Host IP/Name** and **Nick name** of the Juniper DX component to be monitored as shown in Chapter 2. Then, click **Add** button to register the changes.

2.2 Configuring the tests

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

List of unconfigured tests for 'Juniper DX'		
Performance		junidx
Cluster HTTP	Cluster I/O	Cluster SSL
Cluster Status	ClusterHttpStats	Device Uptime
Network Interfaces	SysHost	System Stats
Target Server HTTP	Target Server I/O	Target Server SSL
Target Server Status	TrgtSvrRsp	

Figure 2.2: A list of unconfigured tests

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

TEST PERIOD	5 mins
HOST	192.168.10.1
SNMPPORT	161
TIMEOUT	10
DATA OVER TCP	<input type="radio"/> Yes <input checked="" type="radio"/> No
SNMPVERSION	v3
CONTEXT	none
USERNAME	admin
AUTHPASS	•••••
CONFIRM PASSWORD	•••••
AUTHTYPE	MD5
ENCRYPTFLAG	<input checked="" type="radio"/> Yes <input type="radio"/> No
ENCRYPTTYPE	DES
ENCRYPTPASSWORD	•••••
CONFIRM PASSWORD	•••••

Figure 2.3: Configuring the Target Server Status test

3. Click on the **Target Server Status** test to configure it. This test reports the status of each of the target servers in the Web cluster accelerated by the Juniper DX device. To configure the test, provide the following details in Figure 1.3 that appears:
4. The next time you try to sign out of the admin interface, you will be prompted to configure the **Network Interfaces** test. To know how to configure this test, refer to *Monitoring Cisco Routers* document.
5. Finally, **Update** the test configuration, and sign out of the eG administrative interface.

Chapter 3: Monitoring the Juniper DX Device

eG Enterprise presents a specialized monitoring model for continuous monitoring of the Juniper DX device. The tests that the eG agent runs and the measures collected by every test are mapped to each layer of the specialized *Juniper DX* layer model offered by the eG Enterprise suite for the Juniper DX device (see Figure 3.1).

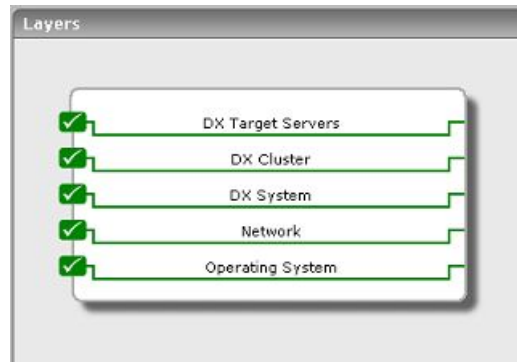


Figure 3.1: Layer model of the Juniper DX device

The sections to come will discuss each of the layers at length.

3.1 The Operating System Layer

Using the SysHost test mapped to it (see Figure 3.2), this layer monitors the CPU and memory utilization of the Juniper DX device.



Figure 3.2: The test associated with the Operating System layer

3.1.1 SysHost Test

This test reports the average CPU and memory utilization of the Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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 <i>none</i> .
AuthPass	Specify the password that corresponds to the above-mentioned Username. This

Parameter	Description
	parameter once again appears only if the SNMPversion selected is v3 .
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	<p>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:</p> <ul style="list-style-type: none"> • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
EncryptFlag	<p>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.</p>
EncryptType	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Avg. CPU usage	Indicates the average CPU utilization of the Juniper DX device.	Percent	A high value could signify a CPU bottleneck.
Avg memory usage	Indicates the average memory utilization of the Juniper DX device.	Percent	A very high value of this measure is an indication of high memory utilization on the device.

3.2 The Network Layer

The **Network** layer measures the network connectivity to and from the Juniper DX device, the availability of its network interfaces, and the uptime of the device (see Figure 3.3).



Figure 3.3: The tests associated with the Network layer

Since these tests have been discussed in great detail in the previous chapters, let us move to the next layer.

3.3 The DX System Layer

With the help of the SysStats test associated with it (see Figure 3.4), the **DX System** layer extracts a wide variety of metrics that enable administrators to assess the following performance parameters:

- Session behaviour on the Juniper DX device
- Request-processing capability of the Juniper DX device

- The data traffic on the device
- The connection-handling capability of the device



Figure 3.4: The tests associated with the DX System layer

3.3.1 System Stats Test

This test reports various statistics related to the session-handling capability, the data traffic, the request processing capability, and the connection-handling capability of the Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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
Active sessions	Indicates the number of sessions on the Juniper DX device that are currently active.	Number	
Sessions handled	Indicates the number of sessions handled in the last measurement period.	Number	
Requests handled	Indicates the number of requests handled in the last measurement period.	Number	
Requests processed	Indicates the number of requests processed in the last measurement period.	Number	
Connections accepted	Indicates the number of connections accepted in the last measurement period.	Number	

Measurement	Description	Measurement Unit	Interpretation
Connections refused	Indicates the number of connections refused in the last measurement period.	Number	
Data in	Indicates the data traffic to the Juniper DX device in the last measurement period.	MB	
Data out	Indicates the data traffic from the Juniper DX device in the last measurement period.	MB	
Data saved	Indicates the data saved in the last measurement period.	MB	

3.4 The DX Cluster Layer

A Web Cluster is a set of web servers to be accelerated. The DX appliance listens for incoming web traffic to a specific Virtual IP address and port, and distributes it over the target hosts (web servers) in the cluster. Typically, all the web servers in a particular cluster serve identical content; that is, each cluster usually represents a distinct website or property.

The eG agent, by executing the tests associated with the **DX Cluster** layer (see Figure 3.5), reports critical statistics pertaining to each of the web clusters managed by the DX device.

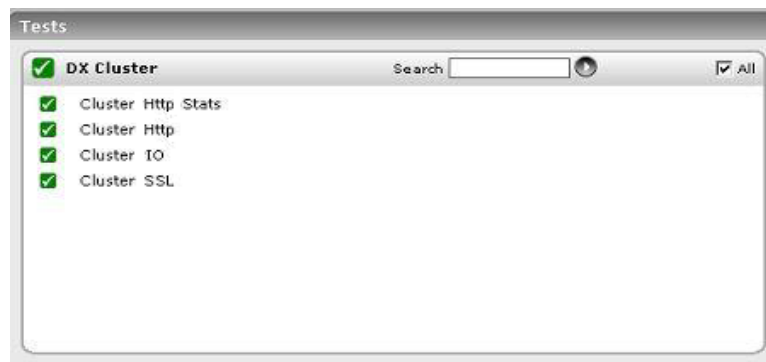


Figure 3.5: The tests associated with the DX Cluster layer

3.4.1 Cluster HTTP Test

This test reports the HTTP statistics per Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Web cluster supported by the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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

Parameter	Description
	contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active requests	Indicates the number of active HTTP requests to the cluster.	Number	
300 responses	Indicates the number of HTTP requests with response code between 300-399 in the last measurement period.	Number	300 responses could indicate page caching on the client browsers. Alternatively 300 responses could also indicate redirection of requests. A sudden change in this value could indicate a problem condition.
400 errors	Indicates the number of HTTP requests with response code between 400-499.	Number	A high value indicates a number of missing/error pages.
500 errors	Indicates the number of HTTP requests with response code between 500-599 in the last measurement period.	Number	Since responses with a status code of 500-600 indicate server side processing errors, a high value reflects an error condition.

3.4.2 ClusterHttpStats Test

This test reports the HTTP statistics per Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Web cluster supported by the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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 <i>none</i> .
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
	<p>the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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
Active requests	Indicates the number of HTTP requests to the cluster that are currently active.	Number	

Measurement	Description	Measurement Unit	Interpretation
Total requests	Indicates the total number of HTTP requests to the cluster during the last measurement period.	Number	
GET requests	Indicates the number of GET HTTP requests to the cluster.	Number	
POST requests	Indicates the number of POST HTTP requests to the cluster.	Number	

3.4.3 Cluster I/O Test

This test reports the IO statistics for every Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Web cluster served by the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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
Active sessions	Indicates the number of new sessions in the listen side in the last measurement period.	Number	
Sessions handled	Indicates the number of reused sessions in the listen side in the last measurement period.	Number	
Sessions refused	Indicates the number of sessions to the cluster that were refused in the last measurement period.	Number	
Active requests	Indicates the number of requests to this cluster that are currently active.	Number	
Total requests	Indicates the total number of requests to the cluster in	Number	

Measurement	Description	Measurement Unit	Interpretation
	the last measurement period.		
Listen data in	Indicates the listen data traffic to this cluster in the last measurement period.	MB	
Listen data out	Indicates the listen data traffic from this cluster in the last measurement period.	MB	
Target data in	Indicates the target data traffic to the cluster in the last measurement period.	MB	
Target data out	Indicates the target data traffic from the cluster in the last measurement period.	MB	

3.4.4 Cluster SSL Test

This test reports the SSL statistics for every Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Web cluster supported by the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .

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 <i>none</i> .
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: <ul style="list-style-type: none"> • 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

Parameter	Description
	default. To ensure that SNMP requests sent by the eG agent are encrypted, select the Yes option.
EncryptType	<p>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:</p> <ul style="list-style-type: none"> • 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
New sessions in the listen side	Indicates the number of new sessions in the listen side in the last measurement period.	Number	
Reused listen sessions	Indicates the number of reused sessions in the listen side in the last measurement period.	Number	
New target sessions	Indicates the number of new sessions in the target side in the last measurement period.	Number	

Measurement	Description	Measurement Unit	Interpretation
New target reused sessions	Indicates the number of reused sessions in the target side in the last measurement period.	Number	

3.4.5 Cluster Status Test

This test reports the status of the Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Web cluster that is supported by a Juniper DX device

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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

Parameter	Description
	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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • 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

Parameter	Description
	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
Cluster is not available	Indicates the availability of the Web cluster.	Percent	The value 100 indicates that the cluster is available, and 0 indicates that the cluster is not currently available.

3.5 The DX Target Servers Layer

This layer monitors the performance of the target web servers in a Web cluster, and reports a wide range of performance data pertaining to each of the servers. Figure 3.6 depicts the tests associated with this layer.



Figure 3.6: The tests associated with the DX Target Servers layer

3.5.1 Target Server Status Test

This test reports the status of the target server in the Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every target server that is supported by the Juniper DX device

Configurable parameters for the test

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

Parameter	Description
	SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • DES – Data Encryption Standard • AES – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such

Parameter	Description
	environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to Yes . By default, this flag is set to No .

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Target server availability	Indicates the availability of the target server.	Percent	A value of 100 indicates that the server is available, and a value of 0 indicates that the server is not currently available.

3.5.2 Target Server I/O Test

This test reports the IO statistics for each of the target servers supported by the Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every target server supported by the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • 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
Data in	Indicates the data traffic to the target server in the last measurement period.	MB	
Data out	Indicates the data traffic from the target server in the last measurement period.	MB	

3.5.3 Target Server Response Test

This test reports the HTTP error statistics of the target servers in the Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every target server served by the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
EncryptFlag	<p>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.</p>
EncryptType	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
300 responses	Indicates the number of HTTP requests with response code between 300-399 in the last measurement period.	Number	300 responses could indicate page caching on the client browsers. Alternatively 300 responses could also indicate redirection of requests. A sudden change in this value could indicate a problem condition.
400 responses	Indicates the number of HTTP requests with response code between 400-499.	Number	A high value indicates a number of missing/errored pages.
500 responses	Indicates the number of HTTP requests with response code between 500-599 in the last measurement period.	Number	Since responses with a status code of 500-600 indicate server side processing errors, a high value reflects an error condition.
404 responses	Indicates the number of HTTP requests with the response code 404 in the last measurement period.	Number	The 404 or Not Found error message is an HTTP standard response code indicating that the client was able to communicate with the server but either the server could not find what was requested, or it was configured not to fulfill the request and not reveal the reason why. A 404 error is often returned when pages have been moved or deleted.

3.5.4 Target Server SSL Test

This test reports the SSL statistics of the target servers in the Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every target server supported by the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • MD5 – Message Digest Algorithm • SHA – Secure Hash Algorithm
EncryptFlag	<p>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.</p>
EncryptType	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
New sessions	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
	new SSL sessions to a target server.		
Reused sessions	Indicates the number of reused SSL sessions to a target server.	Number	

3.5.5 Target Server Http Test

This test reports the HTTP statistics of the target servers in the Web cluster that is supported by a Juniper DX device.

Target of the test : A Juniper DX Device

Agent deploying the test : An external agent

Outputs of the test : One set of results for every target server supported by the Juniper DX device being monitored

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the device listens. By default, this will be <i>NULL</i> .
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is <i>161</i> .
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

Parameter	Description
	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 <i>none</i> .
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	<p>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:</p> <ul style="list-style-type: none"> • 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	<p>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:</p> <ul style="list-style-type: none"> • DES – Data Encryption Standard • AES – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.

Parameter	Description
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
300 responses	Indicates the number of HTTP requests with response code between 300-399 in the last measurement period.	Number	300 responses could indicate page caching on the client browsers. Alternatively 300 responses could also indicate redirection of requests. A sudden change in this value could indicate a problem condition.
400 errors	Indicates the number of HTTP requests with response code between 400-499.	Number	A high value indicates a number of missing/error pages.
500 errors	Indicates the number of HTTP requests with response code between 500-599 in the last measurement period.	Number	Since responses with a status code of 500-600 indicate server side processing errors, a high value reflects an error condition.

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.

Copyright © 2018 eG Innovations Inc. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.