Monitoring Citrix NetScaler SDX

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Citrix NetScaler SDX is a service delivery networking platform for enterprise and cloud datacenters. A virtualized architecture supports multiple NetScaler instances on a single hardware appliance, while a control plane unifies provisioning, monitoring and management.

An administrator can effectively partition the physical box into as many as 16 virtual instances. This helps enterprises running specific virtual versions of the SDX with different settings, configurations and software versions tuned to work with specific services within an enterprise. It can be considered as an all-in-one web application delivery system (ADC) which can make applications run up to five times faster, ensure that the applications are always available with their load balancing capacities and reduce web application ownership costs.

Owing to these capabilities, the NetScaler SDX is widely used in cloud datacenters, where multi-tenancy, resource consolidation, and on-demand access to resources are key for ensuring user satisfaction. In such datacenters, if the SDX appliance unexpectedly reboots or if the appliance/VPX instances on it are even momentarily sluggish, the performance of business-critical applications on the cloud is sure to be badly hit! This in turn translates into a bad cloud experience for the end-users. To avoid this, administrators should closely track the availability, responsiveness, and overall health of the SDX appliance and the VPX instances operating on it, and capture performance anomalies well before end-users notice or complain. With eG Enterprise, administrators can do that and more!

eG Enterprise provides in-depth insights into the availability and performance of the SDX appliance and reports potential issues in its performance. With the help of the accurate problem identification and preemptive alerting capabilities of eG Enterprise, administrators can capture and resolve issues before they affect user experience.

This document discusses how eG Enterprise can be used to monitor the Citrix NetScaler SDX appliance and what metrics are collected in the process.

Chapter 2: How to Monitor Citrix NetScaler SDX Using eG Enterprise?

To monitor the SDX appliance, eG Enterprise employs an agentless approach. The broad steps for monitoring the SDX appliance using this approach are as follows:

1. Deploy an eG agent on any remote host in the environment. Use the installation procedure detailed in the *eG Installation Guide* to install the eG agent.
2. Manage the target SDX appliance using eG Enterprise.
3. The eG agent runs Nitro API commands on the SDX appliance to pull the metrics of interest . To enable the agent to connect to the target appliance and make Nitro API calls, you need to configure the tests run by the eG agent with the credentials of a user with read-only privileges on the appliance.
4. Finally, start the eG agent. To know how the start the eG agent, refer to the *eG Installation Guide*.

Steps 2 and 3 of this process are described in detail in the sections to come.

2.1 Managing the Citrix NetScaler SDX Appliance Using eG Enterprise

To manage a target SDX appliance using eG Enterprise, do the following:

1. Login to the eG administrative interface.
2. Invoke the Admin tile menu and select the Add/Modify option from the Components menu of the Infrastructure tile.
3. Then, select *Citrix NetScaler SDX* as the **Component type** and click the **Add New Component** button. Figure 2.1 will then appear.

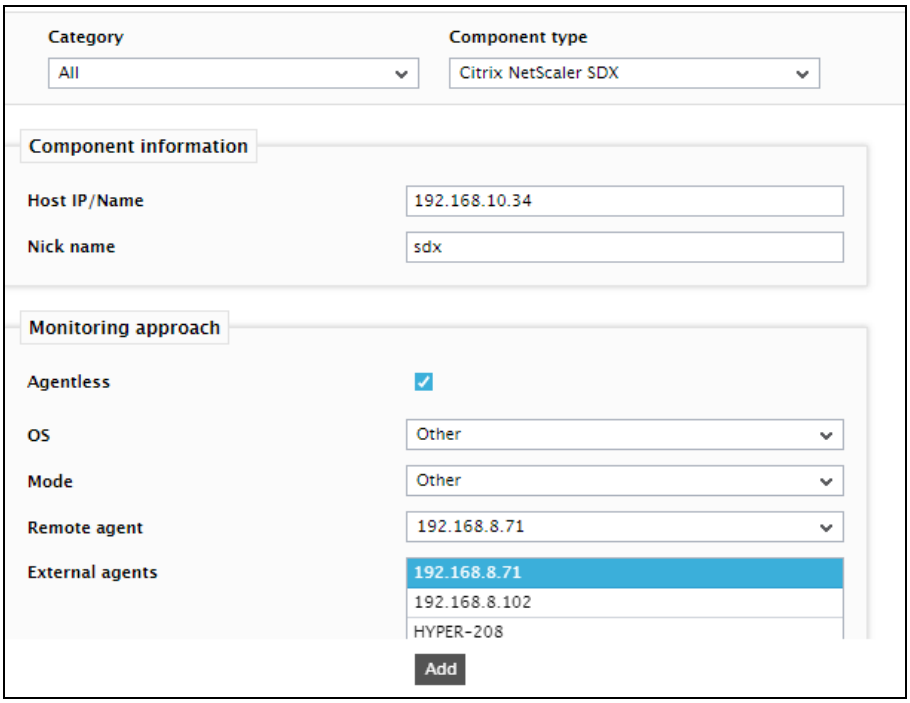

Figure 2.1: Adding a Citrix NetScaler SDX for monitoring

4. In Figure 2.1, provide the **Host IP/Name** of the SDX appliance to be monitored. Then, provide a **Nick name** for the appliance.
5. Since the SDX can be monitored only in an agentless manner, the **Agentless** flag will be switched on by default (see Figure 2.1).
6. Select *Other* from the **OS** and **Mode** drop-down lists.
7. Pick the **Remote agent** that will monitor the SDX appliance. Similarly, select the **External agent** that will report the network availability and responsiveness of the appliance.
8. Finally, click the **Update** button to add the appliance for monitoring.

2.2 Configuring Tests for the Citrix NetScaler SDX Appliance

Now that the appliance has been managed, click **Sign out** to exit the eG admin interface. Figure 2.2 will then appear listing the tests that will have to be manually configured for the target appliance.

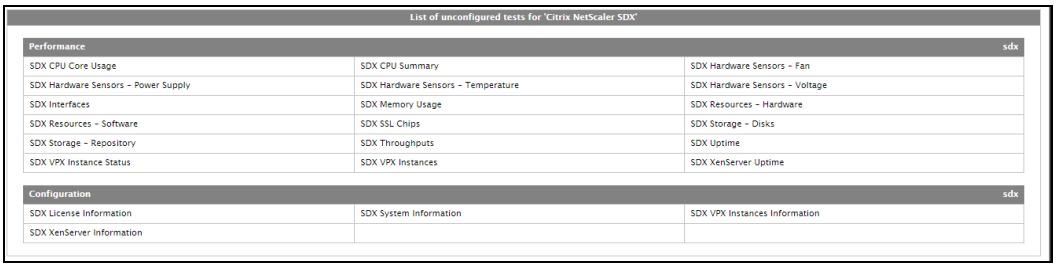

Figure 2.2: List of unconfigured tests

Configuring any one test for the target SDX appliance will automatically configure all other tests associated with that appliance. So, click on any test in Figure 2.2. For instance, let us configure the **SDX CPU Core Usage** test by clicking on it. Figure 2.3 will then appear displaying that test's parameters.

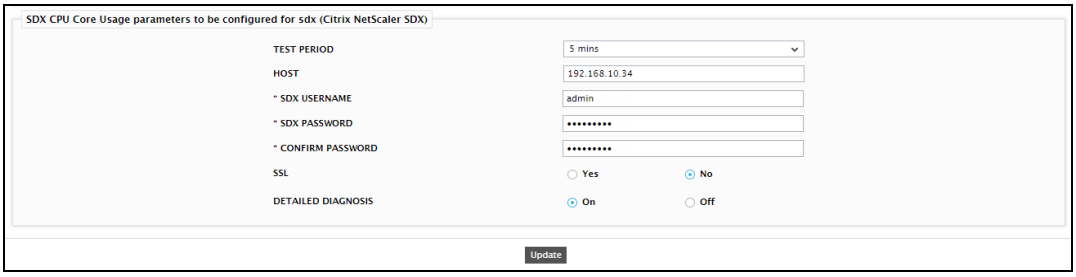

Figure 2.3: Configuring a test for the Citrix NetScaler SDX appliance

To know what the **SDX CPU Core Usage** test does and how to configure it, refer to the Section **3.2.1**. Once the test is configured, click the **Update** button in Figure 2.3 to save the changes. Finally, sign out of the eG administrative interface.

Chapter 3: Monitoring the Citrix NetScaler SDX Appliance

eG Enterprise provides a specialized monitoring model for the Citrix NetScaler SDX (see Figure 3.1).

Figure 3.1: Layer model of the Citrix NetScaler SDX

Each layer of this model (see Figure 3.1) is mapped to tests that run Nitro API commands on the target SDX appliance to report on the unavailability and poor responsiveness of the SDX appliance, capture hardware failures and resource contentions that the appliance is experiencing or may potentially encounter, and pinpoint VPX instances that are hogging resources.

With the help this monitoring model, administrators can find quick and accurate answers to the following performance queries:

- Is the SDX appliance available over the network? If so, how quickly is it responding to requests?
- Was the appliance restarted recently?
- Did the XenServer reboot recently?
- Is any interface down? If so, which one is it?
- Is any interface handling more traffic than the others? If so, which interface is it?
- Is any VPX instance inaccessible? If so, why? Is it because the VPX instance is down, or is it because the VM hosting the instance is not running?
- Is CPU been used optimally, or are any VPX instances hogging the CPU resources? If so, which ones are they? Which specific CPU cores are these instances using?
- Is the appliance sized with adequate memory and storage resources?
- Is any VPX instance utilizing memory abnormally? If so, which one is it?
- Is any storage repository running out of free space?
- Which physical disk has been over-utilized?

- Does the appliance have enough unused SSL chips? If not, then is it because one/more VPX instances are consuming too many SSL chips for processing SSL traffic? Which VPX instances are these?
- Is the throughput of the appliance optimal?
- Is any VPX instance consuming unusually high bandwidth?
- Which hardware components are presently in an abnormal state - is it a fan? or a power supply?
- Is the temperature of any hardware component abnormally high or low?
- Is any hardware component experiencing high voltage?

The sections that follow will discuss each layer of Figure 1 elaborately.

3.1 The Hardware Layer

The tests mapped to this layer report on the health of the critical hardware components of the SDX appliance.

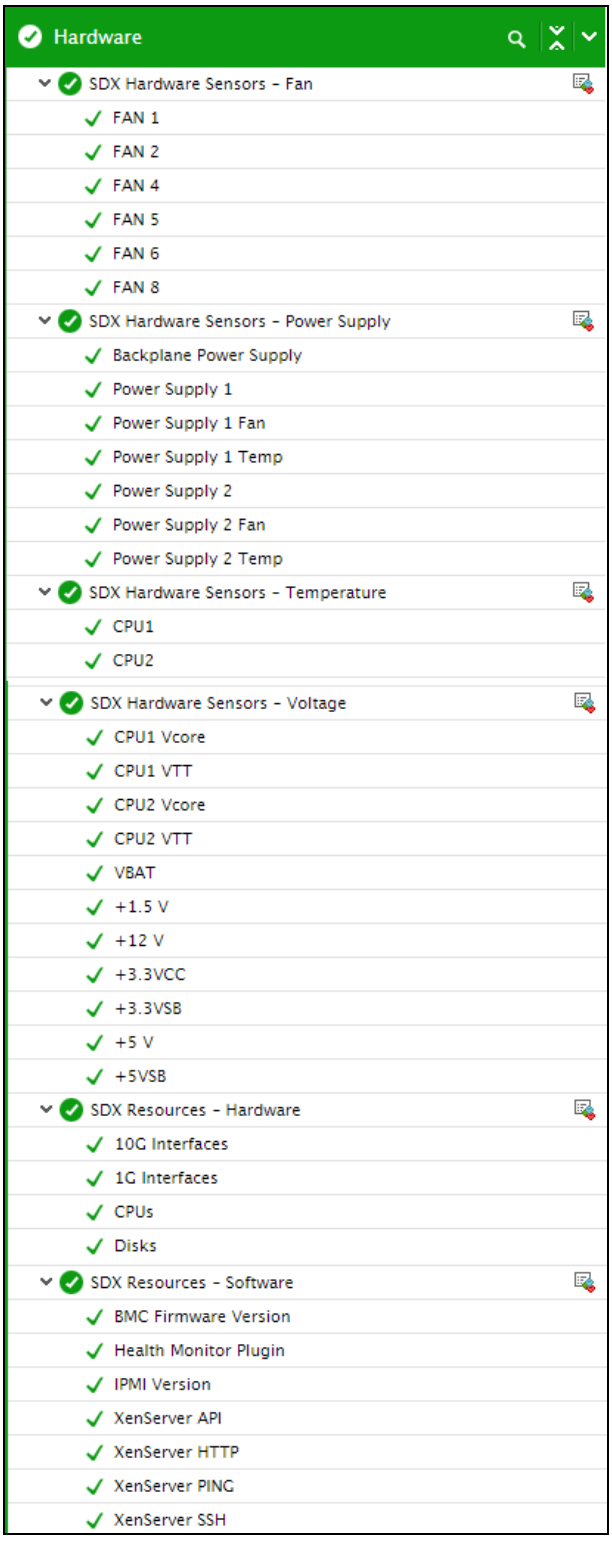

Figure 3.2: The tests mapped to the Hardware layer

3.1.1 SDX Hardware Sensors - Fan Test

If a fan cooling the SDX hardware malfunctions, it can cause the hardware temperature to soar and may even cause irreparable damage to the hardware. If this is to be avoided, the speed and state of each fan supported by the SDX appliance should be tracked, and administrators immediately notified of abnormalities. This is what the **SDX Hardware Sensors - Fan** test. This test monitors the speed and operational state of each fan the target SDX appliance supports and promptly alerts administrators if the fan experiences errors or if the speed of the fan increases abnormally.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each fan supported by the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this fan.		The values that this measure can report and their corresponding numeric values

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>have been listed in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>100</td><td>Ok</td></tr><tr><td>0</td><td>Error</td></tr></table>
If the value of this measure is 'Error' for a fan, it indicates a deviation from the expected value.
Note:
By default, this measure reports the above-mentioned Measure Values to indicate the current state of a fan. However, in the graph of this measure, the Measure Values will be represented using their corresponding numeric equivalents only.</td></tr>
<tr><td>Current fan speed</td><td>Indicates the current speed of this fan.</td><td>Rpm</td><td>A sudden and steep increase in the value of this measure could indicate a fan failure.</td></tr>
</table>

3.1.2 SDX Hardware Sensors - Power Supply Test

Citrix NetScaler SDX platforms can accommodate two power supplies, except the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 platforms which can accommodate four power supplies. All NetScaler appliances function properly with a single power supply, except the SDX 22040/22060/22080/22100/22120 and SDX 24100/24150 platforms which need two power supplies for proper operation. The other power supply(ies) serves as a backup.

Regardless of the power backup available, an administrator may want to be alerted even if a single power supply fails. This way, he/she can arrange to have that power supply replaced before the backup fails too and brings the SDX appliance down! This is where the **SDX Hardware Sensors - Power Supply** test helps!

This test monitors each power supply of the SDX appliance and alerts administrator if any power supply fails. This way, the test prompts administrators to quickly replace the failed supply and ensure the high availability of the SDX appliance.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each power supply on the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only* privileges to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this power supply.		The values that this measure can report and their corresponding numeric values have been listed in the table below: Numeric Value: Measure Value 100: Presence detected 0: Power supply failure detected **Note:** By default, this measure reports the

Measurement	Description	Measurement Unit	Interpretation
			above-mentioned **Measure Value**s to indicate the current status of a power supply. However, in the graph of this measure, the **Measure Value**s will be represented using their corresponding numeric equivalents only.

3.1.3 SDX Hardware Sensors - Temperature Test

A sudden and steep rise or fall in the temperature of critical hardware components such CPU, memory module, etc., can damage the said hardware and render the SDX appliance unusable. If this is to be avoided, then administrators should continuously monitor the state and the temperature of each hardware component of the SDX appliance. This is exactly what the **SDX Hardware Sensors - Temperature** test does!

For each hardware component of the SDX appliance, this test reports the state of that component in terms of its temperature and the current temperature of that component. In the process, the test promptly alerts administrators to an unusual spike/drop in the temperature of the target appliance, and thus enables them to quickly bring the temperature under control before it causes irreparable damage.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each hardware component on the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.

Parameter	Description
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this hardware component, in terms of temperature.		The values that this measure can report and their corresponding numeric values have been listed in the table below: **Numeric Value** / **Measure Value** 100 / Ok 0 / Error The value Error for this measure indicates that the current temperature value is out of range. **Note:** By default, this measure reports the above-mentioned **Measure Value**s to indicate the current status of a hardware component. However, in the graph of this measure, the **Measure Value**s will be represented using their corresponding numeric equivalents only.
Current temperature	Indicates the current temperature of this hardware component.	Celsius	An unusually high or low value for this measure is a cause for concern as it could indicate a potential hardware failure.

3.1.4 SDX Hardware Sensors - Voltage Test

If mission-critical hardware components of the SDX appliance - eg., CPU cores - experience severe and frequent voltage fluctuations, it can cause serious damage to the components. This in turn can render the SDX appliance unusable. To ensure the continuous availability and usage of the SDX appliance, administrators should keep an eye on the voltage of current passing through its core hardware components at all times, capture a voltage surge as soon as it occurs, and correct it immediately. This is where the **SDX Hardware Sensors - Voltage** test helps administrators!

This test reports the voltage of each hardware component on the SDX appliance and also reveals the state of that component in terms of voltage. This way, the test brings sporadic spikes in voltage and its impact on hardware health to the immediate attention of administrators, thereby urging instant remedial action.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each hardware component on the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only* privileges to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this hardware component, in terms of voltage.		The values that this measure can report and their corresponding numeric values have been listed in the table below: **Numeric Value** / **Measure Value** 100 / Ok 0 / Error The value Error for this measure indicates that the current voltage value is out of range. **Note:** By default, this measure reports the above-mentioned **Measure Value**s to indicate the current status of a hardware component. However, in the graph of this measure, the **Measure Value**s will be represented using their corresponding numeric equivalents only.
Current voltage	Indicates the current voltage of this hardware component.	Volts	An unusually high value for this measure is a cause for concern as it could indicate a potential hardware failure.

3.1.5 SDX Resources - Hardware Test

Hardware resources such as CPU, memory, NICs, disks, etc., are crucial to the uninterrupted functioning of the SDX appliance. If even one of these hardware components experiences errors or deviates from their normal behavior, it is bound to adversely impact the overall health and availability of the SDX appliance. This is why, it is imperative that administrators receive instant notifications of any abnormality related to the hardware resources. For this purpose, administrators can use the SDX Resources - Hardware test.

This test monitors and reports the operational state and overall health condition of each hardware resource such as CPU, disk, interface, etc. In the process, the test promptly captures and reports hardware-related abnormalities and ensures the timely intervention of administrators.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each hardware resource supported by the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current state of this hardware resource.		The values that this measure can report and their corresponding numeric values have been listed in the table below:

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Ok</td><td>100</td></tr><tr><td>Error</td><td>0</td></tr></table> If the value of this measure is 'Error' for a resource, it indicates a deviation from the expected value. **Note:** By default, this measure reports the above-mentioned **Measure Value**s to indicate the current state of a hardware resource. However, in the graph of this measure, the **Measure Value**s will be represented using their corresponding numeric equivalents only.
Current value	Indicates the current value of this hardware resource.	Number	
Expected value	Indicates the expected value for this hardware resource	Number	A high value is desired for this measure.

3.1.6 SDX Resources - Software Test

Periodically, administrators should check the status of and track changes to critical software resources on an SDX appliance, such as the BMC Firmware, XenServer API, Health Monitor Plugin, Management Service, etc. This is because, if these software components do not function as expected, users may not be able to use the SDX appliance effectively. To avoid this, administrators should run the **SDX Resources - Software** test at regular intervals and keep tabs on the status of each of the software components on the SDX appliance.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each software resource supported by the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current state of this software resource.		The values that this measure can report and their corresponding numeric values have been listed in the table below: Numeric Value: Measure Value 100: Ok 0: Error The value 'Error' for this measure indicates the following for different resources: • For BMC Firmware version, it indicates deviation from the expected value; • For calls to XenServer, it

Measurement	Description	Measurement Unit	Interpretation
			indicates that the Management Service is unable to communicate with XenServer by using an API, HTTP, PING, or SSH call; • For Health Monitor Plugin, it indicates that the plugin is not installed on XenServer. **Note:** By default, this measure reports the above-mentioned **Measure Value**s to indicate the current state of a software resource. However, in the graph of this measure, the **Measure Value**s will be represented using their corresponding numeric equivalents only.
Current value	Indicates the current value of this software resource.	Number	

3.2 The SDX Layer

The test mapped to this layer measure how the SDX appliance uses the CPU, memory, SSL cores, and storage resources at its disposal. In the process, the tests proactively alert administrators to potential resource contentions on the appliance. Additionally, the tests monitor the uptime of the appliance and its XenServer hypervisor and sends out alerts if the appliance/XenServer reboot suddenly.

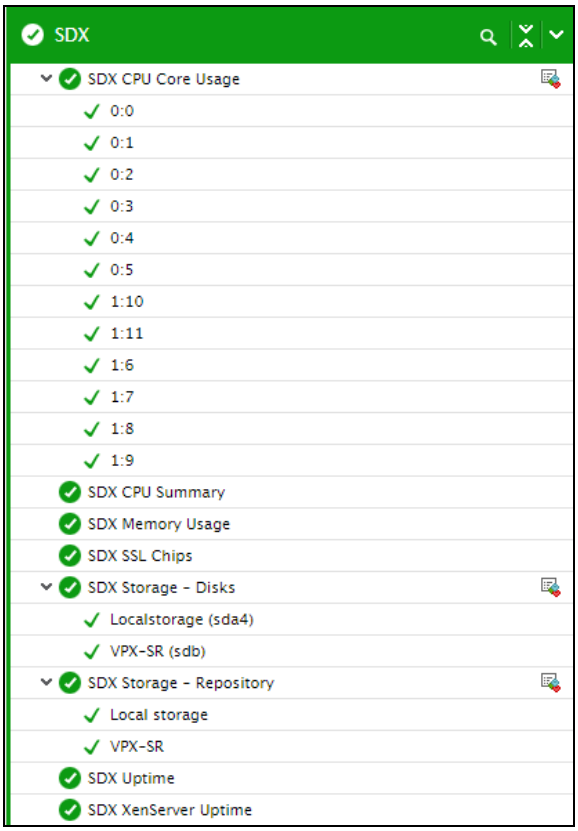

Figure 3.3: The tests mapped to the SDX layer

3.2.1 SDX CPU Core Usage Test

The SDX CPU Summary test alerts administrators to abnormal CPU usage on an SDX appliance, which can typically be caused by one/more CPU cores being utilized excessively. The question now is, which CPU cores are contributing to the CPU contention. The SDX CPU Core Usage test answers this question by reporting the average CPU usage of each CPU core of an SDX appliance.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each CPU core of the target NetScaler SDX.

Configurable parameters for the test

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

Parameter	Description
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the passwordby retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Average CPU core usage	Indicates the percent CPU usage of this CPU core.	Percent	A value close to 100% is a cause of concern, as it could indicate excessive usage of a core by one/more VPX instances on the target SDX appliance. If this condition is left unchecked, it can cause the overall performance of the SDX to significantly

Measurement	Description	Measurement Unit	Interpretation
			deteriorate and badly impact user-experience with the appliance. Use the detailed diagnosis of this measure to know which instances are utilizing the core. Then, check the value of the CPU usage measure (reported by the SDX VPX Instances test) for each of those instances to know which instance is hogging the CPU resources.

The detailed diagnosis of the *Avg CPU core usage* measure reveals the core number, the physical CPU resources mapped to each core, and the instances that are utilizing the core. If a core is over-utilized, then this information will point you to the instances that could be contributing to the excessive usage.

Details of CPU core

CORE NUMBER	PHYSICAL CPU	HYPER THREADS	INSTANCES
Sep 05, 2017 20:34:13			
0	1	2, 3	MSCNSVP01

Figure 3.4: The detailed diagnosis of the Avg CPU core usage measure

3.2.2 SDX CPU Summary Test

Typically, when creating VPX instances on a Citrix NetScaler SDX appliance, you can allocate CPU cores to each instance depending on their processing requirements. While a single core is usually set aside for the use of the Management Service on the SDX appliance, the rest are available for allocation to the VPX instances.

If one/more instances engage in CPU-intensive operations, it can result in a severe contention for CPU resources on the appliance. This in turn can degrade the performance of the VPX instances and the SDX appliance as a whole. To avoid this, SDX administrators should continuously track the overall CPU usage of the SDX appliance and capture a potential CPU contention before it aggravates and adversely impacts performance. The **SDX CPU Summary** test helps administrators with this!

This test reports the number of CPU cores the SDX appliance supports and the average CPU usage of the appliance across all the cores. In the process, the test warns administrators of a

probable CPU contention on the appliance and prompts speedy action, so that performance does not suffer.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the passwordby retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the percent CPU usage of the SDX appliance.	Percent	A value close to 100% is a cause of concern, as it could indicate excessive CPU usage by one/more VPX instances on the target SDX appliance. If this condition is left unchecked, it can cause the overall performance of the SDX to significantly deteriorate and badly impact user-experience with the

Measurement	Description	Measurement Unit	Interpretation
			appliance. Under such circumstances, it might be good practice to compare the value of the CPU usage measure of the SDX VPX Instances test across all VPX instances operating on the target appliance. This will point you to the VPX instances that are CPU-hungry and are contributing to the CPU contention. To prevent the contention, you can decide to either allocate more cores to the CPU-starved instances or change the CPU allocation mode of the instance - i.e., from shared to dedicated or vice-versa.
CPU cores	Indicates the total number of CPU cores the SDX appliance supports.	Number	

3.2.3 SDX Memory Usage Test

The NetScaler SDX appliance provides memory that can be shared across VPX instances provisioned on the appliance.

Since memory is shared, if one/more instances consume memory excessively, the other instances will be forced to contend for limited memory resources. This, naturally, will degrade the performance of those instances and also that of the SDX appliance. If such a memory contention is to be prevented, administrators should track the memory used by the appliance, proactively detect a potential memory contention, and rapidly initiate pre- emptive measures. This is where the **SDX Memory Usage** test helps!

This test monitors the memory usage of the SDX appliance and promptly alerts administrators if usage exceeds permissible limits. In the process, the test warns administrators of a probable memory contention and urges them to take immediate action.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each interface supported by the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total memory	Indicates the total memory capacity of the SDX appliance.	GB	
Free memory	Indicates the amount of memory that is unused.	GB	A high value is desired for this measure.
Used memory	Indicates the amount of memory that is in use.	GB	If the value of this measure is equal to or close to the value of the Total memory measure, it is a cause for concern.
Memory usage	Indicates the percentage of memory that is used.	Percent	If the value of this measure is close to 100%, it indicates that appliance and the instances on it will soon run out of memory resources. Under such circumstances, it is good practice to use the SDX VPX Instances test to identify the memory-hungry

Measurement	Description	Measurement Unit	Interpretation
			VPX instances that are provisioned on the SDX appliance. By generating time-of-day graphs of the memory usage of those instances, you can figure out if those instances have been consuming a lot of memory consistently or sporadically. If the anomaly is consistent, you may want to consider increasing the memory allocation to such instances and decreasing the memory allocation to those that use less memory.

3.2.4 SDX SSL Chips Test

The term 'SSL Core / Chip' is used to represent an assignment in hardware of a number of Cavium cores. The SDX appliance uses these Cavium cores to accelerate SSL traffic in hardware. Each VPX instance on a NetScaler SDX instance is assigned one/more SSL cores/chips at the time of configuration. If one/more instances over-utilize the SSL chips, other instances may not have enough SSL chips for processing their SSL traffic. This can cause a significant delay in SSL processing on the VPX instances. This is where the SDX SSL Chips test helps! This test monitors and reports the SSL core usage on the SDX appliance and warns administrators of a potential contention for SSL cores/chips. Administrators are thus enabled to promptly initiate measures for averting the contention and the resulting slowness.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the

Parameter	Description
	credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total SSL chips	Indicates the total number of SSL cores/chips on the SDX appliance.	Number	
Free SSL chips	Indicates the number of SSL cores/chips that are unused.	Number	A high value is desired for this measure.
Used SSL chips	Indicates the number of SSL cores/chips that are in use.	Number	A low value is desired for this measure.
SSL chip usage	Indicates the percentage of SSL cores/chips that are utilized.	Percent	A value close to 100% for this measure could indicate that one/more VPX instances are hogging the SSL cores/chips. You may want to allocate more SSL cores/chips to such instances, so as to avert a potential resource contention. When allocating SSL cores to an instance, remember that memory and SSL cores are interlinked. This means that when assigning each SSL core it will be necessary to assign 1Gb of memory per core.

3.2.5 SDX Storage - Disks Test

To ensure peak performance of an SDX appliance, it needs to be sized with adequate physical disk resources. If not, then frequent disk space contention and I/O overloads will end up significantly degrading the performance of the appliance. To avoid this, administrators must closely track physical disk usage, proactively alert administrators to a potential disk space crunch or a disk I/O contention, and thus enable administrators to initiate corrective action.

This is exactly what the **SDX Storage - Disks** test does. This test auto-discovers the physical disks supported by the SDX appliance, and for each physical disk, reports the current capacity, space usage, and the I/O activity on that disk. In the process, the test points to the disks that are not sized commensurate to their usage. Based on the pointers provided by this test, administrators can then proceed to resize their storage.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each physical disk on the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Disk size	Indicates the current capacity of this disk.	GB	
Disk utilized	Indicates the amount of space in this disk that is utilized.	GB	A low value is desired for this measure.
Disk free	Indicates the amount of space in this disk that is currently unused.	GB	A high value is desired for this measure.
Disk usage	Indicates the percentage of space in this disk that is in use.	Percent	Compare the value of this measure across disks to know which disk is being used excessively. Typically, a value close to 100% is a cause for concern, as it implies that the disk is running out of space. You may want to consider adding more storage resources to prevent a serious storage contention.
Transactions	Indicates the rate of transactions to this disk.	Transactions/Sec	This is a good indicator of the level of I/O activity on a disk.
Blocks read	Indicates the rate at which data blocks are read from this disk.	Reads/Sec	You can use this value to measure the rate of output from the disk.
Blocks written	Indicates the rate at which data blocks are written to this disk.	Writes/Sec	You can use this value to measure the rate of input from the disk.
Total blocks read and written	Indicates the rate at which I/O operations are performed on this disk.	Operations/Sec	This is a good indicator of the workload of a disk. Compare the value of this measure across disks to identify that disk that is experiencing an I/O overload.

3.2.6 SDX Storage - Repository Test

A storage repository consists of virtual disks and partitions created from a physical disk. If a storage repository runs out of disk space or is in an abnormal state, the VPX instances mapped to that

repository will no longer be able to use the repository; this can bring the operations of the VPX instances to a standstill! This is why, it is important that the state and disk space usage of each storage repository is tracked continuously, and abnormalities immediately brought to the attention of administrators. The **SDX Storage - Repository** test helps with this!

Using this test, administrators can determine whether any storage repository is in a bad / abnormal state presently. The test also proactively alerts administrators to a potential space crunch on a repository, so that administrators can do what is necessary to prevent instance performance to suffer.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each storage repository.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current state of this storage repository.		The values that this measure can report and their corresponding numeric

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>values have been listed in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>100</td><td>Good</td></tr><tr><td>0</td><td>Bad</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values to indicate the current state of a storage repository. However, in the graph of this measure, the Measure Values will be represented using their corresponding numeric equivalents only.</td></tr>
<tr><td>Disk size</td><td>Indicates the current capacity of this storage repository.</td><td>GB</td><td></td></tr>
<tr><td>Disk utilized</td><td>Indicates the amount of disk space in this storage repository that is utilized by the VPX instances.</td><td>GB</td><td>A low value is desired for this measure.</td></tr>
<tr><td>Disk free</td><td>Indicates the amount of disk space in this storage repository that is currently unused.</td><td>GB</td><td>A high value is desired for this measure.</td></tr>
<tr><td>Disk usage</td><td>Indicates the percentage of disk space in this storage repository that is in use.</td><td>Percent</td><td>Compare the value of this measure across storage repositories to know which repository is being used excessively.
Typically, a value close to 100% is a cause for concern, as it implies that the VPX instances are consuming disk</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			space excessively. You may want to consider allocating more virtual disks to the instances, so that the potential storage contention is averted.

3.2.7 SDX Uptime Test

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

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

This test monitors the uptime of critical SDX appliances.

Target of the test : A NetScaler SDX appliance

Agent deploying the test : A remote agent

Outputs of the test : One set of results for every appliance being monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-

Parameter	Description
	enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.
Report Manager Time	By default, this flag is set to **Yes**, indicating that, by default, the detailed diagnosis of this test, if enabled, will report the shutdown and reboot times of the SDX appliance in the manager's time zone. If this flag is set to **No**, then the shutdown and reboot times are shown in the time zone of the system where the remote agent is running.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Has the SDX device been rebooted?	Indicates whether the SDX device has been rebooted during the last measurement period or not.		If this measure shows 1, it means that the device was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this device was rebooted.
Uptime during the	Indicates the time period	Seconds	If the device has not been rebooted

Measurement	Description	Measurement Unit	Interpretation
last measure period	that the system has been up since the last time this test ran.		during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the device was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the device was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period - the smaller the measurement period, greater the accuracy.
Total uptime of the SDX device	Indicates the total time that the device has been up since its last reboot.		This measure displays the number of years, months, days, hours, minutes and seconds since the last reboot. Administrators may wish to be alerted if a device has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

3.2.8 SDX XenServer Uptime Test

NetScaler SDX uses the XenServer hypervisor to partition its acceleration services by carriers and service providers, so that individual accelerators can be created for separate cloud customers.

SDX administrators can assure their cloud customers of uninterrupted acceleration only if they can ensure the high availability of the XenServer that underlies the SDX appliance. For this purpose, administrators can use the SDX XenServer Uptime test.

This test monitors the uptime of the SDX XenServer and promptly alerts administrators if an unscheduled reboot occurred or if a scheduled reboot failed.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only* privileges to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.
Report Manager Time	By default, this flag is set to **Yes**, indicating that, by default, the detailed diagnosis of this test, if enabled, will report the shutdown and reboot times of the XenServer in the manager's time zone. If this flag is set to **No**, then the shutdown and reboot times are shown in the time zone of the system where the remote agent is running.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled:

Parameter	Description
	• The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Has the Xen server been rebooted?	Indicates whether the server has been rebooted during the last measurement period or not.	Boolean	If this measure shows 1, it means that the server was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this server was rebooted. The detailed diagnosis of this measure, if enabled, will provide you with the details of the last reboot of the XenServer. Such details will include the shutdown date/time, reboot date/time, the shutdown duration (in minutes), and whether the host has been configured for maintenance or not.
Uptime of the Xen server during the last measure period:	Indicates the time period that the system has been up since the last time this test ran.	Secs	If the server has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the server was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the server was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this

Measurement	Description	Measurement Unit	Interpretation
			metric is dependent on the measurement period - the smaller the measurement period, greater the accuracy.
Total uptime of the Xen server:	Indicates the total time that the server has been up since its last reboot.	Mins	Administrators may wish to be alerted if a server has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

3.3 The Network Layer

Using the tests mapped to this layer, SDX administrators can:

- Periodically check whether/not the SDX appliance is available over the network;
- Measure the responsiveness of the appliance over the network;
- Monitor the NICs supported by the appliance, observe the level of traffic received / transmitted by each interface, and identify which NIC is consuming the maximum bandwidth;
- Measure the throughput of the appliance and initiate investigations if throughput is poor;

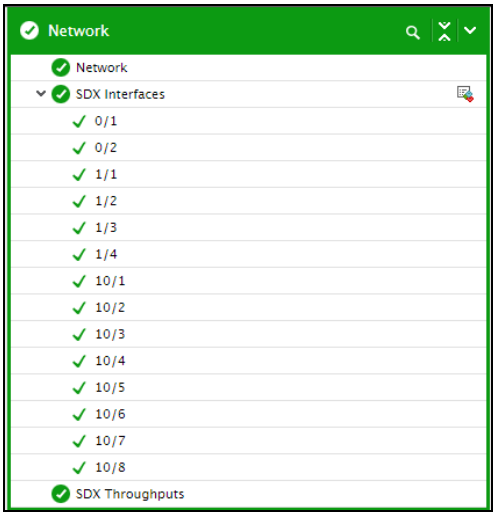

Figure 3.5: The tests mapped to the Network layer

3.3.1 SDX Interfaces Test

Like CPU cores, memory and storage, the NetScaler SDX Appliances also provide NIC interfaces and SSL crypto hardware that can be shared across NetScaler VPX instances that are provisioned on the appliance.

If an NIC on the SDX appliance goes down or is handling more traffic than the rest, the performance of the instances using that network interface is sure to be impacted. Such an anomaly can also threaten the availability of the SDX appliance as a whole. To avert such an outcome, it is good practice for administrators to keep an eye on the up/down state of each NIC and observe the data/packet traffic flowing into and out of the NIC. This way, administrators will be able to instantly detect the unavailability or overloading of an NIC and initiate corrective measures. This is what the **SDX Interfaces** test seeks to achieve!

This test auto-discovers the NICs on a target SDX appliance, reports the state of each NIC, and also reveals how much traffic is handled by every NIC. In the process, the test quickly pinpoints unavailable NICs and the ones handling heavy traffic.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each interface supported by the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only* privileges to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this

Parameter	Description
	case, set the SSL flag to **No**.
Show Enabled Interface Only	If this flag is set to **Yes**, then the network interfaces that have an admin state of "Enabled" will only be monitored by the eG agent. By default, this flag is set to **No**, indicating that by default the eG agent will monitor all network interfaces that are enabled/disabled.
Show Up Interface Only	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose current status is "up" - are monitored. By default, this flag is set to **No**, indicating that by default the test will monitor all network interfaces that are up/down.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
State	Indicates the current state of this interface.		The values that this measure can report and their corresponding numeric values have been listed in the table below: Numeric Value: 100 — Measure Value: Up Numeric Value: 0 — Measure Value: Down If the value of this measure is *Up*, it means that the interface is receiving traffic normally. If the value of this measure is *Down*, it indicates a network issue because of which the interface is unable to send or receive traffic. **Note:** By default, this measure reports the above-mentioned **Measure Value**s to indicate the current state of an interface. However, in the graph of this measure, the measure values will be represented using their corresponding numeric equivalents only.

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Admin state</td><td>Indicates the current admin state of this interface.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been listed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Enabled</td><td>1</td></tr><tr><td>Disabled</td><td>0</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure Values to indicate the current admin state of each interface. However, in the graph of this measure, the measure values will be represented using their corresponding numeric equivalents only.</td></tr>
<tr><td>Total virtual functions</td><td>Indicates the total number of virtual functions available on this interface.</td><td>Number</td><td>The NetScaler SDX appliance also provides SSL crypto hardware that can be shared across NetScaler VPX instances that are provisioned on the appliance. Crypto capacity is typically represented and allocated in units of SSL cores and chips. Crypto virtual interfaces - also known as Virtual Functions - represent the basic access of the SSL hardware. When the SSL hardware operates in cryptographic blocks, they can be used to form virtual functions.</td></tr>
<tr><td>Assigned virtual functions</td><td>Indicates the number of virtual functions assigned to this interface.</td><td>Number</td><td>You can assign up to seven virtual functions on a 1G interface and up to 40 virtual functions on a 10G interface.</td></tr>
<tr><td>Received packets</td><td>Indicates the rate at which this interface receives packets.</td><td>Packets/Sec</td><td>These are good indicators of the level of network activity on an interface.
You can compare the value of each of</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
Transmitted packets	Indicates the rate at which this interface transmitted packets.	Packets/Sec	these measures across interfaces to identify the busiest / overloaded interface.
Data received	Indicates the rate at which this interface receives data.	MB/Sec	
Data transmitted	Indicates the rate at which this interface transmitted data.	MB/Sec	
Received errors	Indicates the rate at which errors occurred during data reception on this interface.	Errors/Sec	Ideally, the value of these measures should be 0.
Transmitted errors	Indicates the rate at which errors occurred during data transmission by this interface.	Errors/Sec	

3.3.2 SDX Throughputs Test

When users complain of slowness of the SDX appliance, administrators should first check the throughput of the appliance. Throughput reveals how well/badly the appliance processes network traffic. Low throughput is indicative of a traffic processing bottleneck, which can cause users to experience slowness when interacting with the appliance. To receive real-time insights into the throughput of the SDX appliance, administrators can use the **SDX Throughputs** test. This test measures the throughput of the SDX appliance in real-time and alerts administrators if the throughput is low. Additionally, the test also reveals where the bottleneck is - when processing incoming network traffic? or outgoing network traffic?

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Input throughput	Indicates the rate at which the SDX appliance processes incoming network traffic.	Mbps	If the value of the Total throughput measure is abnormally high or is increasing consistently, you may want to compare the value of the Input throughput and Output throughput measures to understand when the maximum slowness occurred - when processing incoming traffic? or when processing outgoing traffic?
Output throughput	Indicates the rate at which the SDX appliance processes outgoing network traffic.	Mbps	
Total throughput	Indicates the rate at which the SDX appliance processes network traffic.	Mbps	This is the sum of the Input throughput and Output throughput measures and reveals the overall network throughput of the appliance. A consistent drop in the value of this measure could indicate that the appliance does not have adequate bandwidth resources for processing network traffic.

3.4 The VPX Instances Layer

With the help of the tests mapped to this layer, administrators can:

- Know which VPX instances are running on the target SDX appliance;
- Promptly detect the inaccessibility of an instance and determine its reason - is it because the instance is down? or the VM hosting the instance is down?
- Track the resource usage of each instance and isolate instances that are hogging resources;

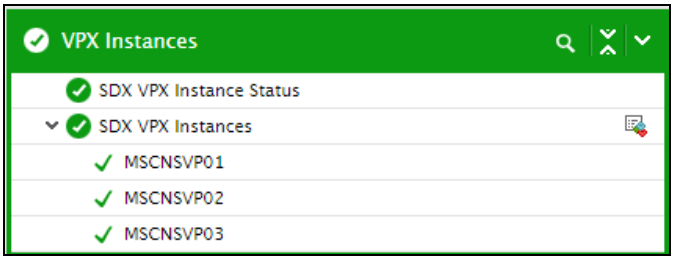

Figure 3.6: The tests mapped to the VPX Instances layer

3.4.1 SDX VPX Instance Status Test

To quickly identify the number and names of VMs and VPX instances that are operating on an SDX appliance and to rapidly determine their status, use the **SDX VPX Instance Status** Test.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface

Parameter	Description
	Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Total VPX instances	Indicates the total number of VPX instances on the monitored NetScaler SDX appliance.	Number	Use the detailed diagnosis of this measure to know the names of the VMs and VPX instances on the target SDX appliance.
VPX instances with UP state	Indicates the count of VPX instances that are up and running currently.	Number	Use the detailed diagnosis of this measure to know the names of the VPX instances that are in the UP state and the names of VMs hosting the UP instances.
VPX instances with Down state	Indicates the number of VPX instances that are not running presently.	Number	Use the detailed diagnosis of this measure to know which VPX instances are down and which VMs host them.
Running VMs	Indicates the number of	Number	Use the detailed diagnosis of this

Measurement	Description	Measurement Unit	Interpretation
	VMs that are up and running currently.		measure to know the name and IP address of the running VMs and the names of the VPX instances they host.
Halted VMs	Indicates the count of halted VMs.	Number	Use the detailed diagnosis of this measure to know which VMs on the target SDX appliance are not running currently and which are the VPX instances they host.

With the help of the detailed diagnosis of the *Total VPX instances* measure, you can instantly identify the VPX instances that have been configured on each of the VMs on the SDX appliance.

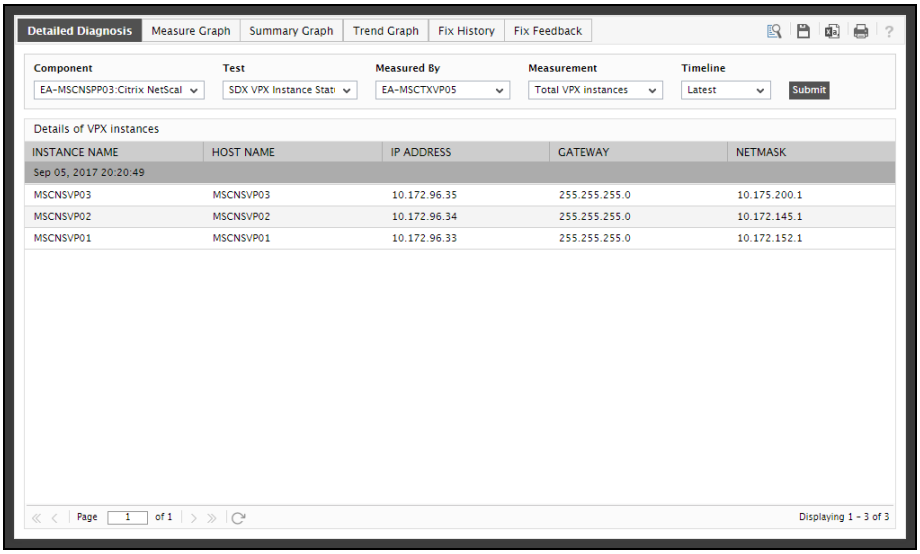

Figure 3.7: The detailed diagnosis of the Total VPX Instances measure

Using the detailed diagnosis of the *VPX instances with UP state* measure, you can accurately identify the VPX instances that are currently up and running.

Details of up VPX Instances

INSTANCE NAME	HOST NAME	IP ADDRESS	GATEWAY	NETMASK
Sep 05, 2017 20:20:49				
MSCNSVP03	MSCNSVP03	10.172.96.35	255.255.255.0	10.175.200.1
MSCNSVP02	MSCNSVP02	10.172.96.34	255.255.255.0	10.172.145.1
MSCNSVP01	MSCNSVP01	10.172.96.33	255.255.255.0	10.172.152.1

Figure 3.8: The detailed diagnosis of the VPX instances in UP state measure

If you want to know which VMs on the SDX appliance are up and running, use the detailed diagnosis of the *Running VMs* measure.

Details of running VMs

INSTANCE NAME	HOST NAME	IP ADDRESS	GATEWAY	NETMASK
Sep 05, 2017 20:20:49				
MSCNSVP03	MSCNSVP03	10.172.96.35	255.255.255.0	10.175.200.1
MSCNSVP02	MSCNSVP02	10.172.96.34	255.255.255.0	10.172.145.1
MSCNSVP01	**MSCNSVP01**	**10.172.96.33**	**255.255.255.0**	**10.172.152.1**

Figure 3.9: The detailed diagnosis of the Running VMs measure

3.4.2 SDX VPX Instances Test

NetScaler SDX supports multiple NetScaler instances on a single hardware appliance. An administrator can effectively partition the physical box into as many as 16 virtual instances. This helps enterprises running specific virtual versions of the SDX with different settings, configurations and software versions tuned to work with specific services within an enterprise.

If any of these virtual NetScaler instances is rendered unavailable, then users may be denied access to the critical services associated with that instance. Moreover, if an instance is poorly sized with CPU, memory, and network resources, or is utilizing resources excessively, the performance of that instance and the other instances supported by that SDX will naturally deteriorate for want of adequate resources. This is why, the availability, resource configuration, and resource usage of each virtual NetScaler instance should be monitored and administrators proactively notified of any inaccessibility or resource contention on any instance. This is what the **SDX VPX instances** test does!

This test auto-discovers the VPX instances that the target NetScaler SDX appliance supports and reports the availability of each instance. If the test alerts to an instance unavailability, you can use this test to once again verify why that instance is inaccessible - is it because the instance is down or the VM hosting that instance is halted? The test also monitors the resource configuration of each instance and the percent resource consumption of every instance; in the process, the test points you to resource-hungry instances, and thus The uptime of each instance is also reported, so that administrators can promptly detect unscheduled instance reboots and unplanned instance downtime.

Target of the test : A NetScaler SDX

Agent deploying the test : A remote agent

Outputs of the test : One set of results for each VPX instance supported by the target NetScaler SDX.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
SDX Username and SDX Password	To monitor a NetScaler SDX device, the eG agent should be configured with the credentials of a user with *read-only privileges* to the target device. Specify the credentials of such a user in the SDX Username and SDX Password text boxes.
Confirm Password	Confirm the password by retyping it here.
SSL	The eG agent collects performance metrics by invoking NITRO (NetScaler Interface Through Restful interfaces and Objects) APIs on the target NetScaler SDX device. Typically, the NITRO APIs can be invoked through the HTTP or the HTTPS mode. By default, the eG agent invokes the NITRO APIs using the HTTPS mode. This is why, the SSL flag is set to **Yes** by default. If the target NetScaler SDX device is not SSL-enabled, then the NITRO APIs can be accessed through the HTTP mode only. In this case, set the SSL flag to **No**.
Report Manager Time	By default, this flag is set to **Yes**, indicating that, by default, the detailed diagnosis of this test, if enabled, will report the shutdown and reboot times of the VPX instances in the manager's time zone. If this flag is set to **No**, then the shutdown and reboot times are shown in the time zone of the system where the remote agent is running.
DD Frequency	Refers to the frequency with which detailed diagnosis measures are to be generated for this test. The default is *1:1*. This indicates that, by default, detailed measures will be generated every time this test runs, and also every time the test detects a problem. You can modify this frequency, if you so desire. Also, if you intend to disable the detailed diagnosis capability for this test, you can do so by specifying *none* against DD Frequency.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Virtual machine state</td><td>Indicates the current state of the VM hosting this VPX instance.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been listed in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>100</td><td>Running</td></tr><tr><td>0</td><td>Halted</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure Values to indicate the current state of a VM. However, in the graph of this measure, the Measure Values will be represented using their corresponding numeric equivalents only.</td></tr>
<tr><td>Instance state</td><td>Indicates the current state of this VPX instance.</td><td></td><td>The values that this measure can report and their corresponding numeric values have been listed in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>100</td><td>Up</td></tr><tr><td>0</td><td>Down</td></tr></table>
When a user complains that a NetScaler VPX instance is inaccessible, then check the value of this measure for that instance to determine whether/not that instance is up and running. If it is, then check the value of the Virtual machine state measure for the same instance to</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			determine whether the Virtual machine is running or halted. **Note:** By default, this measure reports the above-mentioned **Measure Value**s to indicate the current state of a VPX instance. However, in the graph of this measure, the **Measure Value**s will be represented using their corresponding numeric equivalents only.
CPU usage	Indicates the percentage of allocated CPU used by this VPX instance.	Percent	A value close to 100% is indicative of excessive CPU usage by the VPX instance. Compare the value of this measure across instances to know which instance is over-utilizing CPU. You may want to consider increasing the CPU allocation to that instance.
Total memory	Indicates the total memory of this VPX instance.	MB	
Memory usage	Indicates the percentage of memory used by this instance.	MB	A value close to 100% is indicative of excessive memory usage by the VPX instance. Compare the value of this measure across instances to know which instance is over-utilizing memory. You may want to consider increasing the memory allocation to that instance.
Input throughput	Indicates the bandwidth consumed by incoming traffic to this VPX instance.	Mbps	
Output throughput	Indicates the bandwidth	Mbps	

Measurement	Description	Measurement Unit	Interpretation
	consumed by outgoing traffic from this VPX instance.		
Total throughput	Indicates the total bandwidth consumption of this instance.	Mbps	Total throughput is the sum of the Input throughput and Output throughput measures of the VPX instance. If this value increases consistently, it is indicative of excessive bandwidth consumption by the instance. You may want to periodically compare the value of Total throughput (i.e., actual throughput) with the value of the Assign throughtput (i.e., allocated throughput measure of an instance. This will reveal if bandwidth sizing for that instance has been done on the basis of its real-time bandwidth consumption. Based on these observations, you can choose to reconfigure the bandwidth allocation to the instance. For example, you may have set the throughput allocation mode as fixed for an instance, and may have hard-allocated throughput resources to that instance. Later however, by tracking changes to the value of the Total throughput measure, you may discover that the hard limit is often violated, causing the SDX appliance to drop traffic. In such a case, you may want to consider changing the allocation mode to burstable. When using the burstable option, options are available to allow over commitment of throughput above the set throughput value that is required.
Assign throughput	Indicates the throughput assigned/allocated to this instance.	Mbps	

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>HTTP request</td><td>Indicates the rate at which this instance receives HTTP requests.</td><td>Requests/Sec</td><td></td></tr>
<tr><td>HA master state</td><td>Indicates whether this instance is the primary or secondary instance in an HA setup.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>100</td><td>Primary</td></tr><tr><td>0</td><td>Secondary</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values to indicate the master state of the instance. However, in the graph of this measure, the Measure Values will be represented using their corresponding numeric equivalents only.</td></tr>
<tr><td>Is HA synchronization enabled?</td><td>Indicates whether/not HA synchronization is enabled on this instance.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>1</td><td>Yes</td></tr><tr><td>0</td><td>No</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values to indicate the HA sync status of an instance. However, in the graph of</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>this measure, the Measure Values will be represented using their corresponding numeric equivalents only.</td></tr>
<tr><td>Is L2 mode enabled?</td><td>Indicates whether/not L2 mode is allowed on this instance.</td><td></td><td>In Layer 2 (L2) mode, a NetScaler instance acts as a learning bridge and forwards all packets for which it is not the destination. Some features, such as Cloud Bridge, require that L2 mode be enabled on the NetScaler instance. With L2 mode enabled, the instance can receive and forward packets for MAC addresses other than its own MAC address. However, if a user wants to enable L2 mode on a NetScaler instance running on an SDX appliance, the administrator must first allow L2 mode on that instance.

If the L2 mode is allowed on an instance, then this measure will report the value Yes. If the L2 mode is not allowed, then this measure will report the value No for that instance.

The numeric values that correspond to the measure values are as follows:

<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>1</td><td>Yes</td></tr><tr><td>0</td><td>No</td></tr></table>
Note:

By default, this measure reports the above-mentioned Measure Values to indicate the L2 mode status. However, in the graph of this</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>measure, the Measure Values will be represented using their corresponding numeric equivalents only.</td></tr>
<tr><td>Assigned packets</td><td>Indicates the rate at which this instance can receive packets.</td><td>Packets/Sec</td><td></td></tr>
<tr><td>Number of SSL cores up</td><td>Indicates the number of SSL cores that are currently up and running.</td><td>Number</td><td>The term ‘SSL Core’ is used to represent an assignment in hardware of a number of Cavium cores. The SDX appliance uses these Cavium cores to accelerate SSL traffic in hardware.</td></tr>
<tr><td>Number of SSL cores</td><td>Indicates the total number of SSL cores assigned to this instance.</td><td>Number</td><td>Instances cannot share SSL cores. Any SSL cores that are allocated at the time of provisioning an instance are dedicated to that instance.

Memory and SSL Cores are interlinked, so when assigning each SSL core it will be necessary to assign 1Gb of memory per core.</td></tr>
<tr><td>Has the VPX instance device been rebooted?</td><td>Indicates whether/not this instance was rebooted during the last measurement period.</td><td></td><td>The values that this measure can report and their corresponding numeric values are listed in the table below:

<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>1</td><td>Yes</td></tr><tr><td>0</td><td>No</td></tr></table>
Note:

By default, this measure reports the above-mentioned Measure Values to indicate the reboot status of an instance. However, in the graph of this measure, the Measure Values</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			will be represented using their corresponding numeric equivalents only.
Uptime of the VPX instance during the last measure period	Indicates the time period for which this instance was up since the last time this test ran.	Secs	If the instance has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the instance was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the instance was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period - the smaller the measurement period, greater the accuracy.
Total uptime of the VPX instance	Indicates the total time for which this instance was up since its last reboot.		This measure displays the number of years, months, days, hours, minutes and seconds since the last reboot. Administrators may wish to be alerted if an instance has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

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.