Monitoring QNAP NAS

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

QNAP Turbo Network Storage system, henceforth referred as QNAP NAS system which when deployed in business environments provides file storage, backup, disaster recovery, security management and virtualization applications for businesses; multimedia applications for home etc.

The QNAP NAS system is well known in today's business environments for its ease-of-use, robust operation, large storage capacity, and trustworthy reliability.The QNAP NAS system, helps in effectively improving business efficiency on file sharing, virtualization applications, storage management and surveillance in the business environments, as well as enriching entertainment life for home users with the offering of a fun multimedia center experience. This implies that a slightest deviation in the performance of the storage system if not detected and resolved at the earliest, can result in the loss of critical data. To avoid such an adversity, it is necessary to monitor the QNAP NAS system 24x7. This is where eG Enterprise helps administrators!

Chapter 2: How to Monitor QNAP NAS Using eG Enterprise?

eG Enterprise monitors the QNAP NAS system in an agentless manner. All that is required for this is a single eG agent on any remote Windows host in the environment. This agent is capable of polling the SNMP MIB of the QNAP NAS at regular intervals and collecting critical measures corresponding to its performance.

2.1 Managing the QNAP NAS

The eG Enterprise cannot automatically discover the QNAP NAS system so that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a QNAP NAS 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 **COMPONENT** page that appears next, select QNAP NAS as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

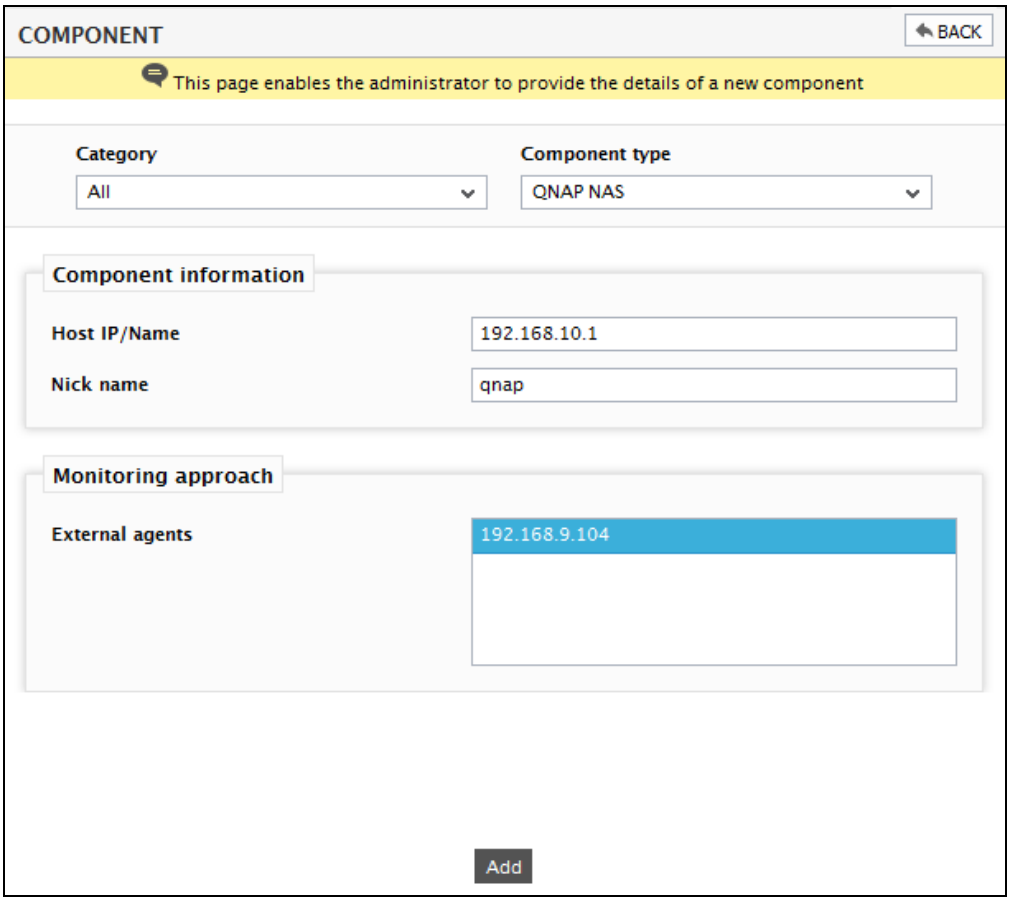

Figure 2.1: Adding an QNAP NAS

4. Specify the **Host IP/Name** and **Nick name** for the QNAP NAS component (see Figure 2.1). Then, click on the **Add** button to register the changes.
5. When you try to signout of the eG administrative interface, a list of unconfigured tests listing the tests requiring manual configuration, will appear (see Figure 2.2).

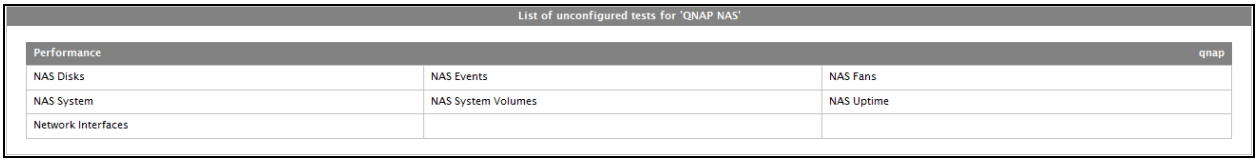

Figure 2.2: A list of unconfigured tests for the QNAP NAS component

6. Click on any test in the list of unconfigured tests. For instance, click on the **NAS Disks** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.

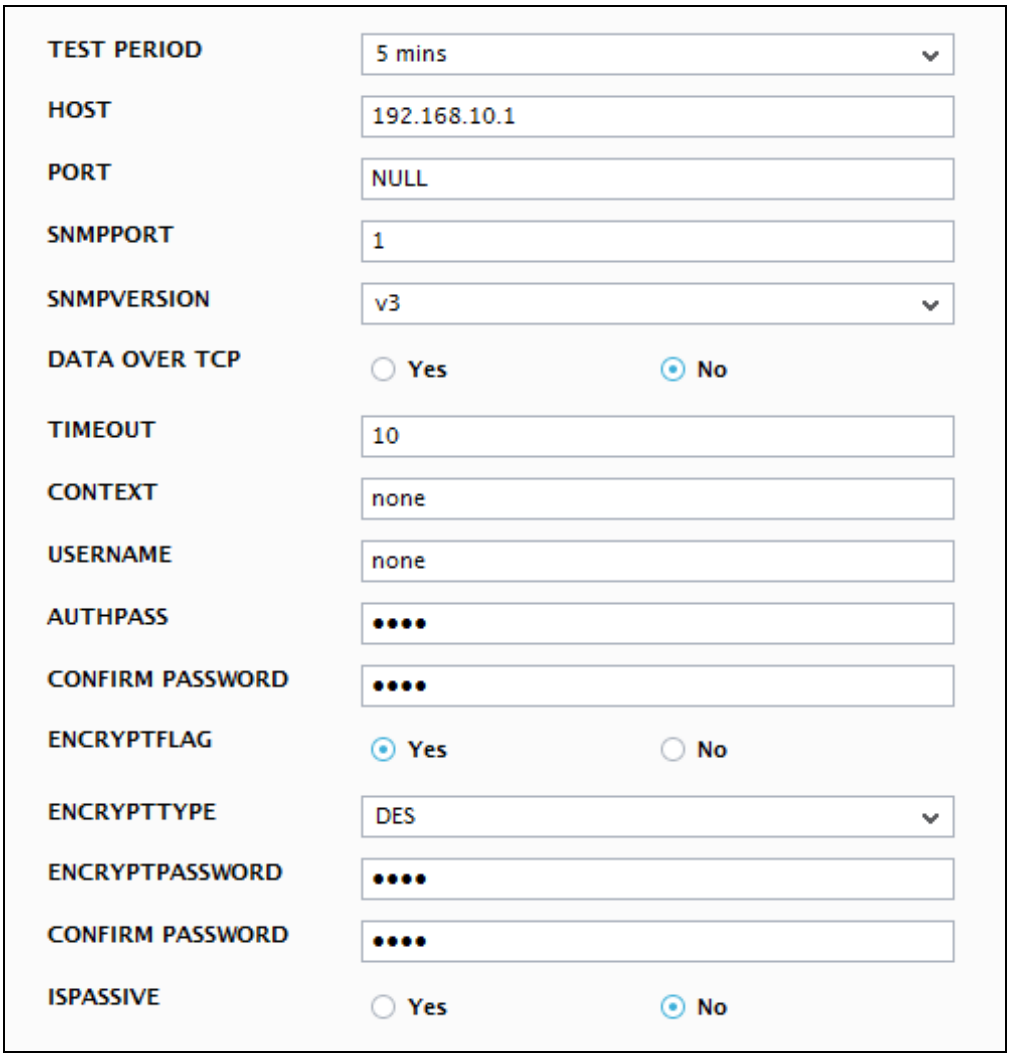

Figure 2.3: Configuring the NAS Disks test

7. To know how to configure the tests, refer to **Monitoring QNAP NAS system** chapter.
8. Next, try to signout of the eG administrative interface, now you will be prompted to configure **Network Interfaces** test. Refer to *Monitoring Cisco Router* document for the details on configuring the **Network Interfaces** test.
9. Once all configurations are configured, signout of the administrative interface.

Chapter 3: Monitoring QNAP NAS system

eG Enterprise offers a specialized and dedicated monitoring model for the QNAP NAS system that monitors the core functions and hardware components of the QNAP NAS system, and proactively alerts administrators to the abnormalities in the performance of the storage system, so that the anamolies are rectified before the occurance of any data loss.

Figure 3.1: The layer model of the QNAP NAS system

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

- What is the current state of each disk in the QNAP NAS system?
- What is the capacity and the current operational temperature of each disk?
- What is the current state of each disk volume?
- Is each disk volume adequately spaced?
- How well each disk volume is utilized?
- What is the current operational speed of each fan in the QNAP NAS system?
- What is the current CPU/memory utilization of the QNAP NAS system?
- Is there adequate free memory available for the operation of the system?
- What is the current temperature of the QNAP NAS system?
- What is the uptime of the QNAP NAS system and how long it has been since the system was last rebooted?
- How many event trap messages have been sent from the QNAP NAS system?

The **Network** layer of the QNAP NAS system monitoring model is similar to that of a Windows Generic server model. Since the tests pertaining to this layer have been dealt with in the *Monitoring Unix and Windows Servers* document, the section to come focuses on the **Hardware** layer.

3.1 The Hardware Layer

Using the test mapped to this layer, you can proactively capture the potential failure of the hardware disks and the space crunch in the disk volumes, if any.

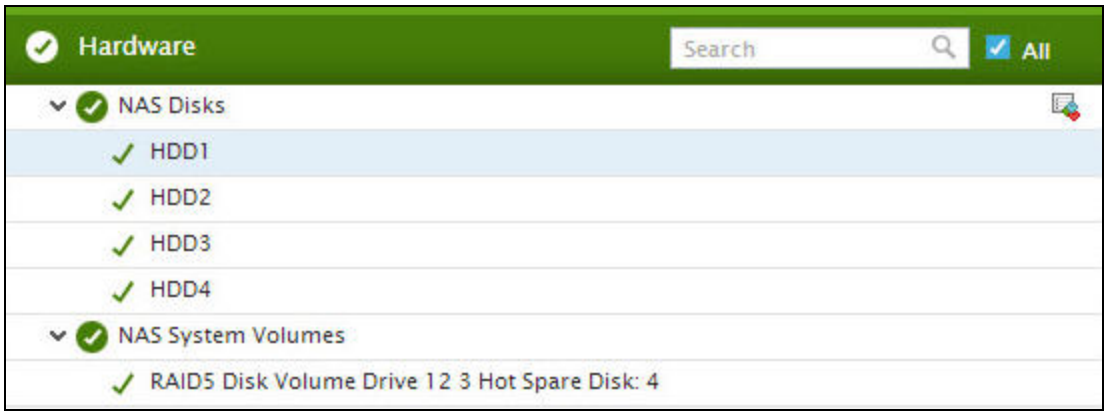

Figure 3.2: The tests mapped to the Hardware layer

Let us discuss each test of this layer (see Figure 3.2) in the forthcoming sections.

3.1.1 NAS Disks Test

This test monitors the current state, capacity and the temperature of each disk in the QNAP NAS system. Using this test, administrators can identify the error-prone disks that may fail any time so that they can avert potential disk failures. In addition, this test points administrators to the temperature of the disks using which abnormalities in the disk temperature can be easily identified and rectified before any irreversible damage is caused to the disk.

Target of the test : A QNAP NAS system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each disk of the QNAP NAS system that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the

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

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Disk status</td><td>Indicates the current state of this disk.</td><td></td><td>The values that this measure can report and their corresponding numeric values are menitoned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Ready</td><td>0</td></tr><tr><td>No disk</td><td>5</td></tr><tr><td>Invalid</td><td>6</td></tr><tr><td>RwError</td><td>9</td></tr><tr><td>Unknown</td><td>4</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current state of this disk. However, the graph of this measure will be represented using the corresponding numeric equivalents as mentioned in the table above.</td></tr>
<tr><td>Disk capacity</td><td>Indicates the total capacity of this disk.</td><td>TB</td><td></td></tr>
<tr><td>Disk temperature</td><td>Indicates the current temperature of this disk.</td><td>Celsius</td><td>Compare the temperature readings registered by each disk to accurately identify the disks that could be experiencing abnormal temperatures. Such disks might have to be subjected to closer observation to figure out the root-cause of the anomaly.</td></tr>
</table>

3.1.2 NAS System Volumes Test

A volume or logical drive is a single accessible storage area with a single file system, typically (though not necessarily) resident on a single partition of a hard disk. If a single disk volume in the QNAP NAS system is over-utilized, it can damage the user experience with the entire storage

system. It is hence the responsibility of the storage administrator to keep an eye out for space contentions and processing bottlenecks with each of the disk volumes in the QNAP NAS, detect such anomalies even before they occur, and resolve them before users complain. The **NAS System Volumes** test helps the storage administrator discharge his duties efficiently. This test auto-discovers the disk volumes and reports the disk space utilization of each of the volumes. This enables administrators to proactively detect a potential disk space contention, identify which disk volume is running out of space, and resolve the problem before it is out of control.

Target of the test : A QNAP NAS system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each disk volume of the QNAP NAS system that is to be monitored.

Configurable parameters for the test

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

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

Parameter	Description
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**.
IsPassive	If the value chosen is **Yes**, then the QNAP NAS system under consideration is a passive server in a QNAP NAS system cluster. No alerts will be generated if the system is not running. Measures will be reported as "Not applicable" by the agent if the system is not up.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current state of this disk volume.	Number	The values that this measure reports and their corresponding numeric equivalents are shown in the table below: **Numeric Value** / **Measure Value** 1 / Ready 2 / No Disk **Note:** By default, this measure reports the above-mentioned **Measure Value**s to indicate the current state of this disk volume. However, the graph of this measure will represent the same using the numeric equivalents only.
Total volume	Indicates the total amount of space available in this disk volume.	TB	
Used volume	Indicates the amount of space that is already	TB	Ideally, the value of this measure should be low. If this value grows close

Measurement	Description	Measurement Unit	Interpretation
	utilized in this disk volume.		to that of the Total volume measure, then you may consider adding more space to the volume, or free up the space in the volume by deleting unnecessary data.
Free volume	Indicates the amount of space that is currently available for use in this disk volume.	TB	A high value is desired for this measure. A gradual/sudden decrease in the value of this measure indicates that the disk volume is currently running out of space.
Free percentage	Indicates the percentage of space that is currently available in this volume.	Percent	A high value is desired for this measure. A value close to 0 indicates that the disk volume is currently running out of space.

3.2 The Operating System Layer

Using the tests mapped to this layer, administrators can determine the physical CPU/memory utilization of the system, the uptime of the system etc

Figure 3.3: The tests mapped to the Operating System layer

Let us discuss each test of this layer (see Figure 3.3) in detail in the forthcoming sections.

3.2.1 NAS Fans Test

This test auto-discovers the fans of the QNAP NAS system and reports the overall health of each fan in terms of the speed with which it operates.

Target of the test : A QNAP NAS system

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan of the QNAP NAS system that is to be monitored.

Configurable parameters for the test

Parameter	Description
Test Period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; The default value is 161.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Speed	Indicates the speed at which this fan operates.	RPM	Ideally, the speed of the fans must be within normal limits.

3.2.2 NAS System Test

This test monitors the CPU, temperature and memory usage of the QNAP NAS system and proactively alerts the administrator to potential resource contentions.

.**Target of the test :** A QNAP NAS system

Agent deploying the test : An external agent

Outputs of the test : One set of results for the QNAP NAS system that is to be monitored.

Configurable parameters for the test

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

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

Parameter	Description
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
IsPassive	If the value chosen is **Yes**, then the QNAP NAS system under consideration is a passive server in a QNAP NAS system cluster. No alerts will be generated if the system is not running. Measures will be reported as "Not applicable' by the agent if the system is not up.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU utilization	Indicates the current CPU utilization of this system.	Percent	A sudden increase in this value could indicate an unexpected/sporadic spike in the CPU usage of the system. A consistent increase however could indicate a gradual, yet steady erosion of CPU resources, and is hence a cause for concern.
Total memory	Indiactes the current memory that is available in this system.	MB	
Free memory	Indicates the amount of memory that is available for use in this system.	MB	A sudden decrease in this value could indicate an unexpected/sporadic spike in the memory utilization of the system. A consistent decrease however could indicate a gradual, yet steady erosion of memory resources, and is hence a cause for concern.
Available memory in percentage	Indicates the percentage of memory that is	Percent	A high value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
	currently avalible for use in this syetem.		
Temperature	Indicates the current temperature of this system.	Celcius	Ideally, the temperature of the system must be within normal limits i.e., 0 - 40°C or 32°F - 104°F. A sudden/gradual increase in the temperature is a cause of concern which needs to be probed immediately so that malfunctioning of the system can be averted.

3.2.3 NAS Uptime Test

In most production environments, it is essential to monitor the uptime of critical systems in the infrastructure. By tracking the uptime of each of the systems, administrators can determine what percentage of time a system 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 systems. By knowing that a specific system has been up for an unusually long time, an administrator may come to know that the scheduled reboot task is not working on a system.

This test monitors the reboot and uptime of the QNAP NAS system.

Target of the test : A QNAP NAS system

Agent deploying the test : An external agent

Outputs of the test : One set of results for the QNAP NAS system that is to be monitored.

Configurable parameters for the test

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

Parameter	Description
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
UserName	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG 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	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
IsPassive	If the value chosen is **Yes**, then the QNAP NAS system under consideration is a passive server in a QNAP NAS system cluster. No alerts will be generated if the system is not running. Measures will be reported as “Not applicable’ by the agent if the system is not up.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Has the NAS device restarted?	Indicates whether the system has been rebooted during the last measurement period or not.	Boolean	If this measure shows 1, it means that the system 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 system was rebooted.

Measurement	Description	Measurement Unit	Interpretation
Uptime 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 system 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 system 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 system 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 NAS	Indicates the total time that the system 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 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 NAS Service Layer

This layer proactively alerts the administrators with a detailed insight on the event trap messages sent from the QNAP NAS system.

Figure 3.4: The tests mapped to the NAS Service layer

3.3.1 NAS Events Test

This test enables administrators to promptly capture and report the count and details of critical information, warning, and critical events that are generated on the server.

Target of the test : A QNAP NAS system

Agent deploying the test : An external/remote agent

Outputs of the test : One set of results for each event that occurred on the QNAP NAS system that is to be monitored.

Configurable parameters for the test

Parameters	Description
Test Period	How often should the test be executed.
Host	The host for which the test is to be configured.
Port	The port at which the specified host listens. By default, this is *NULL*.
Source Address	Specify a comma-separated list of IP addresses or address patterns of the hosts from which traps are considered in this test. For example, 10.0.0.1,192.168.10.*. A leading '*' signifies any number of leading characters, while a trailing '*' signifies any number of trailing characters.
OID Value	Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: .1.3.6.1.4.1.9156.1.1.2 and .1.3.6.1.4.1.9156.1.1.3. The values of these OIDs are as given hereunder:

Parameters	Description

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

In this case the OIDValue parameter can be configured as Trap1:.1.3.6.1.4.1.9156.1.1.2-Host_system,Trap2:.1.3.6.1.4.1.9156.1.1.3-Network, where Trap1 and Trap2 are the display names that appear as descriptors of this test in the monitor interface.

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

Typically, if a valid value is specified for an OID in the OID-value pair configured, then the test considers the configured OID for monitoring only when the actual value of the OID matches with its configured value. For instance, in the example above, if the value of OID .1.3.6.1.4.1.9156.1.1.2 is found to be hostT and not Host_system, then the test ignores OID .1.3.6.1.4.1.9156.1.1.2 while monitoring. In some cases however, an OID might not be associated with a separate value – instead, the OID itself might represent a value. While configuring such OIDs for monitoring, your OIDValue specification should be: DisplayName:OID-any. For instance, to ensure that the test monitors the OID .1.3.6.1.4.1.9156.1.1.5, which in itself, say represents a failure condition, then your specification would be:

Trap5: .1.3.6.1.4.1.9156.1.1.5-any.

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

Trap6:.1.3.6.1.4.1.9156.1.1.4;.1.3.6.1.4.9156.1.1.5-any.

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

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

TrapOIDs — By default, this parameter is set to all, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Number of events	Indicates the number of trap messages of this event that were sent from this system.	Number	The detailed diagnosis of this measure if enabled, lists the name of the event.

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.