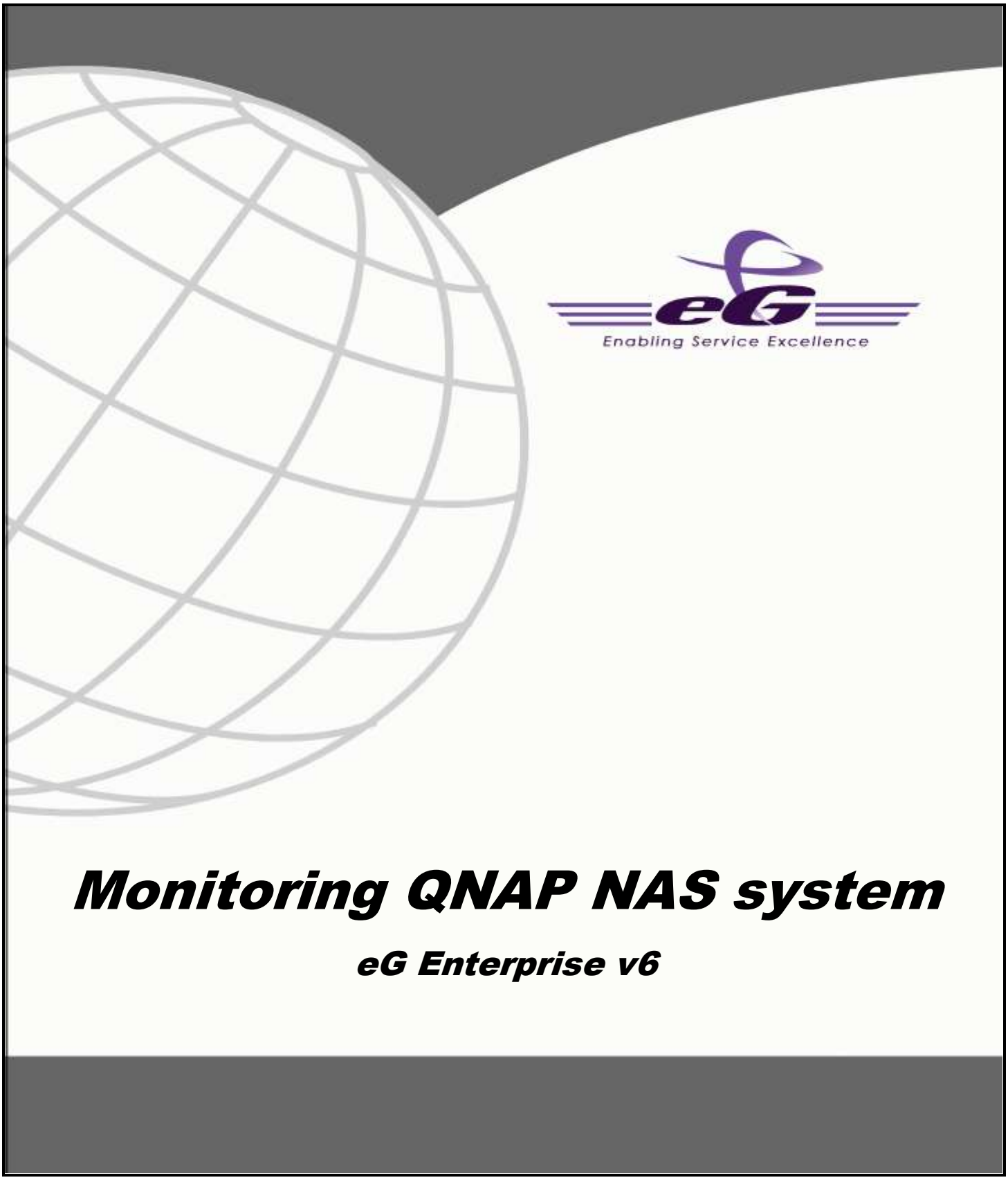

Monitoring QNAP NAS system

eG Enterprise v6

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations Inc. eG Innovations Inc. 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.

Trademarks

Microsoft Windows, Windows NT, Windows 2000, Windows 2003 and Windows 2008 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

Table of Figures

1

Monitoring QNAP NAS system

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.

eG Enterprise Suite 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 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, Section 1.1 focuses on the **Hardware** layer.

1.1 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 2: The tests mapped to the Hardware layer

Let us discuss each test of this layer (see Figure 2) in the forthcoming sections.

1.1.1 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.

Purpose	Monitors the current state, capacity and temperature of each disk in the QNAP NAS system
Target of the test	A QNAP NAS system
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*. 4. **SNMPPORT** – The SNMP Port number of the QNAP NAS system(161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter.

	8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the 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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 16. **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 QNAP NAS system over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**. 17. **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.		
ll Outputs of the test	One set of results for each disk of the QNAP NAS system that is to be monitored		
Measurements made by the	**Measurement**	**Measurement Unit**	**Interpretation**

<table>
<tr><td rowspan="3">test</td><td>Disk status:
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:
Indicates the total capacity of this disk.</td><td>TB</td><td></td></tr>
<tr><td>Disk temperature:
Indicates the current temperature of this disk.</td><td>Celcius</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>

1.1.2 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.

Purpose	Auto-discovers the disk volumes and reports the disk space utilization of each of the volumes
Target of the	A QNAP NAS system

test	
Agent deploying the test	An internal agent
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*. 4. **SNMPPORT** – The SNMP Port number of the QNAP NAS system(161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the 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

<table>
<tr><td></td><td colspan="3">13. ENCRYPTPASSWORD – Specify the encryption password here.
14. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.
15. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
16. 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 QNAP NAS system over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
17. 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.
18.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each disk volume of the QNAP NAS system that is to be monitored</td></tr>
<tr><td rowspan="3">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Status:
Indicates the current state of this disk volume.</td><td>Number</td><td>The values that this measure reports and their corresponding numeric equivalents are shown in the table below:
<table><tr><th>Numeric Value</th><th>Measure Value</th></tr><tr><td>1</td><td>Ready</td></tr><tr><td>2</td><td>No Disk</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure Values to indicate the current state of this disk volume. However, the graph of this measure will represent the same using the numeric equivalents only.</td></tr>
<tr><td>Total volume:
Indicates the total amount of space available in this disk volume.</td><td>TB</td><td></td></tr>
</table>

	Used volume: Indicates the amount of space that is already utilized in this disk volume.	TB	Ideally, the value of this measure should be low. If this value grows close 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.

1.2 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: The tests mapped to the Operating System layer

Let us discuss each test of this layer (see Figure 3) in detail in the forthcoming sections.

1.2.1 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.

Purpose	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.

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*. 4. **SNMPPORT** – The SNMP Port number of the QNAP NAS system(161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.

<table>
<tr><td></td><td colspan="3">12. ENCRYPTTYPE – If the 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
13. ENCRYPTPASSWORD – Specify the encryption password here.
14. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.
15. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
16. 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 QNAP NAS system over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
17. 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.
18.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each fan of the QNAP NAS system that is to be monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Speed:
Indicates the speed at which this fan operates.</td><td>RPM</td><td>Ideally, the speed of the fans must be within normal limits.</td></tr>
</table>

1.2.2 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.

.

Purpose	Monitors the CPU, temperature and memory usage of the QNAP NAS system
Target of the test	A QNAP NAS system
Agent deploying the test	An external agent

Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*. 4. **SNMPPORT** – The SNMP Port number of the QNAP NAS system(161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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 11. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 12. **ENCRYPTTYPE** – If the 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 13. **ENCRYPTPASSWORD** – Specify the encryption password here. 14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 15. **TIMEOUT -** Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">16. 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 QNAP NAS system over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
17. 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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the QNAP NAS system that is to be monitored</td></tr>
<tr><td rowspan="6">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>CPU utilization:
Indicates the current CPU utilization of this system.</td><td>Percent</td><td>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.</td></tr>
<tr><td>Total memory:
Indiactes the current memory that is available in this system.</td><td>MB</td><td></td></tr>
<tr><td>Free memory:
Indicates the amount of memory that is available for use in this system.</td><td>MB</td><td>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.</td></tr>
<tr><td>Available memory in percentage:
Indicates the percentage of memory that is currently avalible for use in this syetem.</td><td>Percent</td><td>A high value is desired for this measure.</td></tr>
<tr><td>Temperature:
Indicates the current temperature of this system.</td><td>Celcius</td><td>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.</td></tr>
</table>

1.2.3 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.

Purpose	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
Configurable parameters for the test	1. **TEST PERIOD** - How often should the test be executed 2. **HOST** – The host for which the test is to be configured 3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*. 4. **SNMPPORT** – The SNMP Port number of the QNAP NAS system(161 typically) 5. **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. 6. **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. 7. **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 the **USERNAME** parameter. 8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**. 9. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 10. **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

<table>
<tr><td></td><td colspan="3">
11. ENCRYPTFLAG – This flag appears only when v3 is selected as the snmpversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the ENCRYPTFLAG is set to NO by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the YES option.
12. ENCRYPTTYPE – If the 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
13. ENCRYPTPASSWORD – Specify the encryption password here.
14. CONFIRM PASSWORD – Confirm the encryption password by retyping it here.
15. TIMEOUT - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the TIMEOUT text box. The default is 10 seconds.
16. 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 QNAP NAS system over TCP (and not UDP). For this, set the DATA OVER TCP flag to Yes. By default, this flag is set to No.
17. 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.
18.
</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for the QNAP NAS system that is to be monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Has the NAS device restarted?:
Indicates whether the system has been rebooted during the last measurement period or not.</td><td>Boolean</td><td>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.</td></tr>
</table>

	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.	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.

1.3 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 4: The tests mapped to the NAS Service layer

1.3.1 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.

Purpose	Monitors the read cache of the NFS datastore and reports the level of I/O activity on the NFS datastore
Target of the test	A QNAP NAS system
Agent deploying the test	An external/remote agent

Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** - The host for which the test is to be configured.
3. **PORT** – The port at which the specified **HOST** listens. By default, this is *NULL*.
4. **SOURCEADDRESS** – 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.
5. **OIDVALUE** Provide a comma-separated list of OID and value pairs returned by the traps. The values are to be expressed in the form, *DisplayName:OID-OIDValue*. For example, assume that the following OIDs are to be considered by this test: *.1.3.6.1.4.1.9156.1.1.2* and *.1.3.6.1.4.1.9156.1.1.3*. The values of these OIDs are as given hereunder:

OID	Value
.1.3.6.1.4.1.9156.1.1.2	Host_system
.1.3.6.1.4.1.9156.1.1.3	NETWORK

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

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

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

Trap5: .1.3.6.1.4.1.9156.1.1.5-any.

6. **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.
7. **TRAPOIDS** – By default, this parameter is set to *all*, indicating that the eG agent considers all the traps received from the specified sourceaddresses. To make sure that the agent considers only specific traps received from the sourceaddress, then provide a comma-separated list of OIDs in the trapoids text box. A series of OID patterns can also be specified here, so that the test considers only those OIDs that match the specified pattern(s). For instance, **94.2*,*.1.3.6.1.4.25**, where * indicates leading and/or trailing spaces.
8. **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.

<table>
<tr><td></td><td colspan="3">9. 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 enabled/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.</td></tr>
<tr><td>Outputs of the test</td><td colspan="3">One set of results for each event that occurred on the QNAP NAS system that is to be monitored</td></tr>
<tr><td rowspan="2">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td>Interpretation</td></tr>
<tr><td>Number of events:
Indicates the number of trap messages of this event that were sent from this system.</td><td>Number</td><td>The detailed diagnosis of this measure if enabled, lists the name of the event.</td></tr>
</table>

2 Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **QNAP NAS** system. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.