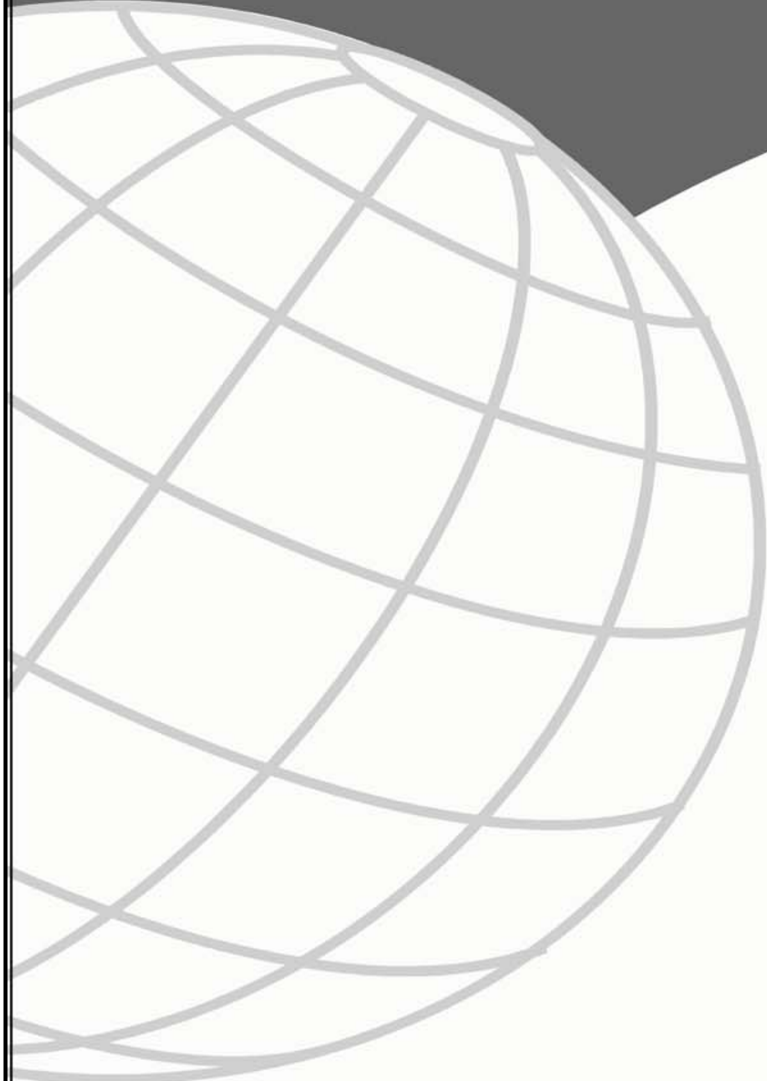


Enabling Service Excellence

Monitoring NetApp Products

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

Copyright

Table of Contents

Table of Figures

Chapter

1

Introduction

Network Appliance (NetApp) provides enterprise storage solutions that offer customers data management, backup and recovery, and remote office access to data.

As the varied offerings of NetApp play a crucial role in the delivery of business-critical services, problems in any of the NetApp products can bring the service to a stand-still, causing the business to lose revenue. To prevent such adverse reactions, it is recommended that you closely observe the performance of NetApp products, detect anaomalies on-the-fly, and resolve them before they can impact service delivery.

eG Enterprise provides specialized monitoring models for the NetApp Filer and NetApp NetCache products. This document details eG Enterprise's monitoring capabilities with regards to these two NetApp products.

Chapter

2

Monitoring NetApp Filers

The NetApp filer is a storage networking system built on the Data ONTAP operating system. It provides simultaneous file system access to UNIX, NT, and Web-based servers and clients using various file system access protocols like NFS, CIFS etc. Capable of handling terabytes of data, the NetApp Filer serves as a reliable and scalable storage solution for large enterprises and service providers.

For the NetApp Filer to provide storage services without any interruptions, the hardware on the filer should remain fault-free, adequate storage resources should be available on the filer, the load on the filer should be kept optimal, and most importantly, the file system access protocols should operate normally. In order to ensure this, all the above-mentioned performance-impacting factors should be kept under a constant check – in other words, should be continuously monitored.

eG Enterprise provides an exclusive *NetApp Filer* monitoring model (see Figure 2.1), which scans the entire filer from its file system to its hardware for errors, and reports abnormalities (if any).

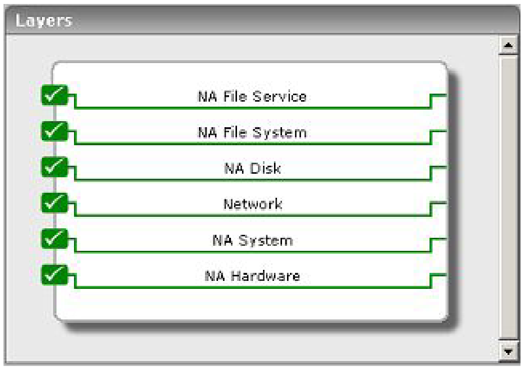


Figure 2.1: The layer model of a NetApp Filer

Each layer depicted by Figure 2.1 is mapped to a set of tests, which when executed, contact the SNMP MIB of the filer to extract the statistics of interest.

The sections to come discuss each of the layers and they metrics they help collect.

2.1 The NA Hardware Layer

Using the NaHardware test, this layer brings to light faulty filer hardware.

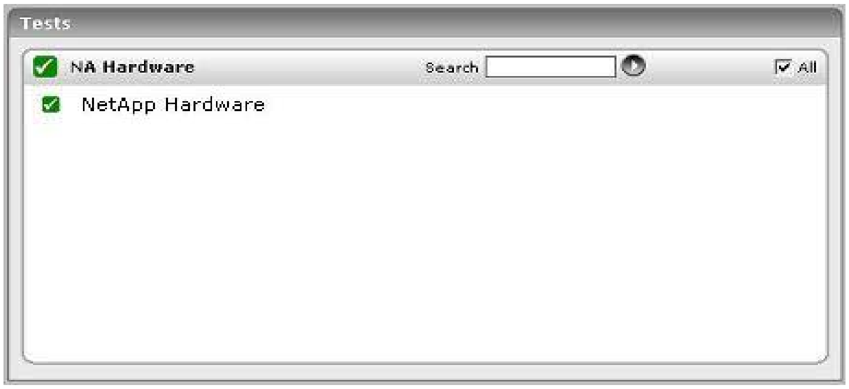


Figure 2.2: The tests associated with the NA Hardware layer

2.1.1 NetApp Hardware Test

The NaHardware test reports performance statistics pertaining to the NetApp filer hardware.

Purpose	Reports performance statistics pertaining to the NetApp filer hardware
Target of the test	A NetApp filer
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

<table>
<tr><td></td><td colspan="3">14. **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.
15. **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 a NetApp filer</td></tr>
<tr><td>**Measurements made by the test**</td><td>**Measurement**</td><td>**Measurement Unit**</td><td>**Interpretation**</td></tr>
<tr><td></td><td>**Over temperature:**
Indicates whether the hardware is currently operating above its maximum rated temperature.</td><td>Number</td><td>A value of 1 indicates over temperature and 0 indicates normal temperature.</td></tr>
<tr><td></td><td>**Failed fan count:**
Indicates the number of main unit backplane fans, the working status of which has currently changed.</td><td>Number</td><td>The detailed diagnosis capability, if enabled for this test, will list the fans that have failed and the reason for their failure.</td></tr>
<tr><td></td><td>**Failed powersupply count:**
Indicates the number of power supplies and power rails, the working status of which has currently changed.</td><td>Number</td><td>The detailed diagnosis capability, if enabled for this test, will list the power rails that have failed and the reason for their failure.</td></tr>
<tr><td></td><td>**Nvram battery status:**
Indicates the current status of the NVRAM battery or batteries.</td><td>Number</td><td>A value of 0 indicates a problem, and 1 indicates that the battery is functioning normally. The detailed diagnosis capability, if enabled for this test, will provide a brief description of the problem (if any).
Batteries which are fully or partially discharged may not fully protect the system during a crash.</td></tr>
</table>

2.2 The NA System Layer

This layer reveals how well the system resources are utilized by the NetApp filer.

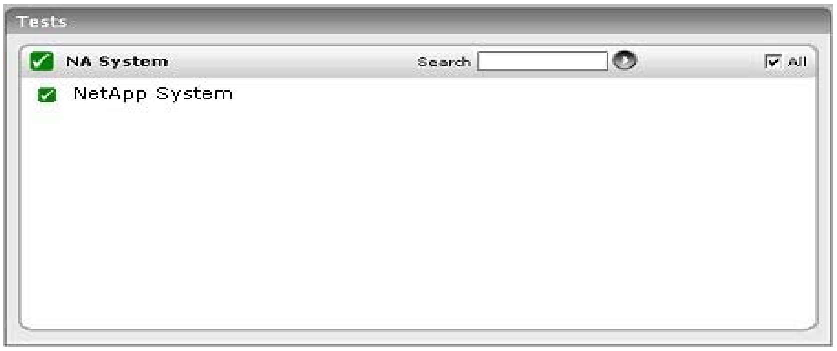


Figure 2.3: The tests associated with the NA System layer

2.2.1 NetApp System Test

The NaSystem test monitors the usage of system resources by the NetApp filer.

Purpose	Monitors the usage of system resources by the NetApp filer
Target of the test	A NetApp filer
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for a NetApp filer		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Cpu busy time: Indicates the percentage of time that the CPU was busy during the last measurement period.	Percent	A high value may be indicative of excessive load on the appliance.
	Global status: Indicates the overall status of the appliance.		
	Data received over the network: Indicates the rate of data received by all the network interfaces.	Bytes/Sec	
	Data sent over the network: Indicates the rate of data transmitted by all the network interfaces.	Bytes/Sec	
	Disk reads: Indicates the rate of data read from the disk.	Reads/Sec	A dramatic increase in this value may be indicative of an I/O bottleneck on the appliance.
	Disk writes: Indicates the rate of data written to the disk.	Writes/Sec	A dramatic increase in this value may be indicative of an I/O bottleneck on the appliance.

2.3 The Network Layer

Using the **Network** test, the **Network** layer indicates whether or not the NetApp filer is available over the network.

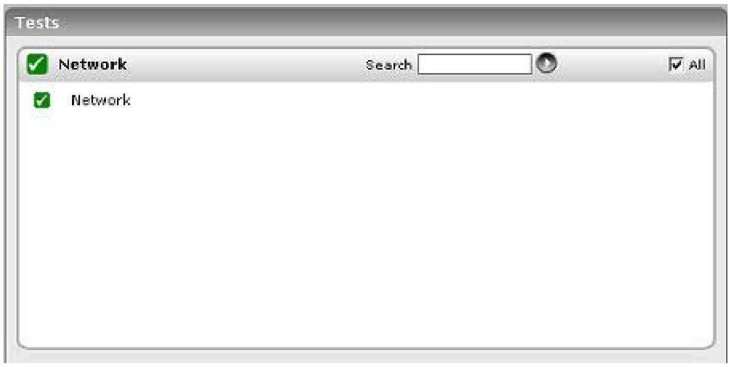


Figure 2.4: The tests associated with the Network layer

This test has been dealt with extensively in the *Monitoring Unix and Windows Servers* document.

2.4 The NA Disk Layer

The test associated with this layer monitors the disk usage on the filer.

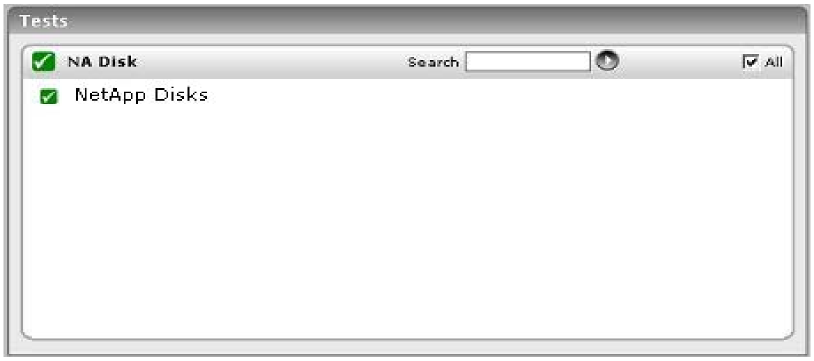


Figure 2.5: The tests associated with the NA Disk layer

2.4.1 NetApp Disks Test

This test monitors the disk drives of the NetApp filer.

Purpose	Monitors the disk drives of the NetApp filer
Target of the test	A NetApp filer
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

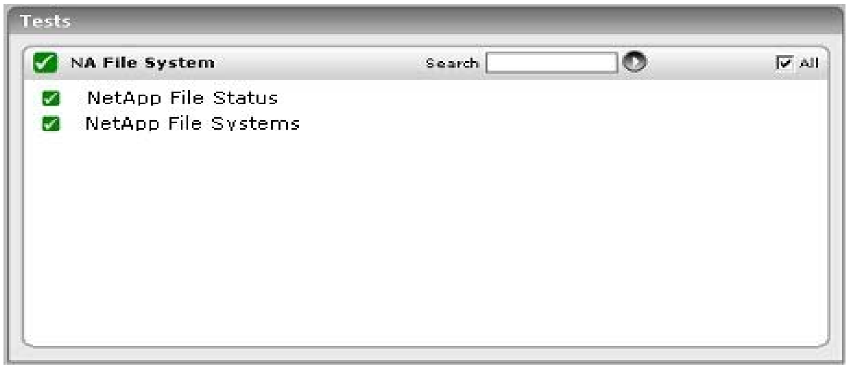
	14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.		
Outputs of the test	One set of results for a NetApp filer		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Total disk count: Indicates the total number of disks on the system.	Number	
	Active disk count: Indicates the number of disks which are currently active, including parity disks.	Number	
	Recons disk count: Indicates the number of disks which are currently being reconstructed.	Number	
	Recons parity disk count: Indicates the number of parity disks which are currently being reconstructed.	Number	
	Verify parity disk count: Indicates the number of parity disks which are currently being verified.	Number	
	Failed disk count: Indicates the number of disks which are currently broken.	Number	
	Spare disk count: Indicates the number of spare disks currently available.	Number	

2.5 The NA File System Layer

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

- Is adequate disk space available on all file systems?

- Is any file system running out of disk space?
- Is any file system using inodes excessively? If so, which file system is it?



Tests

☑ NA File System Search ☑ All

☑ NetApp File Status

☑ NetApp File Systems

Figure 2.6: The tests associated with the NA File System layer

2.5.1 NetApp File Systems Test

This test monitors the NetApp filer's file system.

Purpose	Monitors the file system of the NetApp filer
Target of the test	A NetApp filer
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for every file system being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Used disk space: Indicates the total disk space that is in use in the referenced file system.	MB	
	Free disk space: Indicates the total disk space that is free for use in the referenced file system.	MB	
	Percent used disk space: Indicates the percentage of disk space currently in use in the referenced file system.	Percent	When the utilization of a file system approaches 100%, many applications using the partition could begin to experience failures.
	Used inodes: Indicates the total number of inodes in use in the referenced file system.	Number	
	Free inodes: Indicates the total number of inodes that are available for use in the referenced file system.	Number	
	Percent used inodes: Indicates the percentage of disk space currently in use based on inode counts, in the referenced file system.	Percent	If this value approaches 100%, then new files can no longer be created in the file system.

2.5.2 NetApp File Status Test

This test monitors the inodes used by the file system of a NetApp filer device.

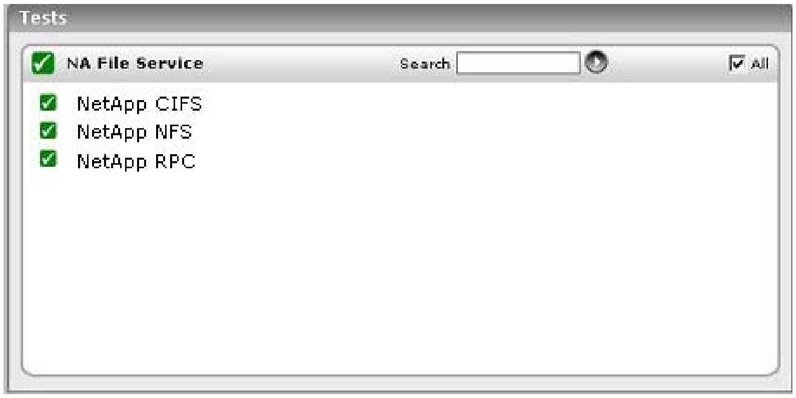
Purpose	Monitors the inodes used by the file system of a NetApp filer device
Target of the test	A NetApp filer
Agent deploying the test	An external agent

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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for every file system being monitored		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Inodes used: Indicates the percentage of inodes currently in use by the file system.	Percent	A very high value is indicative of excessive inode utilization by a file system.

2.6 The NA File Service Layer

The tests mapped to this layer monitor the accesses to the file system, and in the process, reveals how effective the access protocols were.



Tests

☑ NA File Service Search ☑ All

☑ NetApp CIFS
☑ NetApp NFS
☑ NetApp RPC

Figure 2.7: The tests associated with the NA File Service layer

2.6.1 NetApp RPC Test

The NaRpc test reports the statistics related to the RPC (Remote Procedure Call) service executing on a NetApp filer. RPC is designed for network programming, allowing a program to make a subroutine call on a remote machine.

Purpose	Reports the statistics related to the RPC (Remote Procedure Call) service executing on a NetApp filer
Target of the test	A NetApp filer
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for a NetApp filer		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Call rate: Indicates the rate of RPC calls received.	Calls/Sec	
	Bad call rate: Indicates the rate of calls rejected by the RPC layer.	Calls/Sec	
	Percent bad calls: Indicates the percentage of calls rejected by the RPC layer.	Percent	
	Null call receive rate: Indicates the rate at which RPC calls were not available for reception.	Calls/Sec	
	Bad length call rate: Indicates the rate at which RPC calls with a length shorter than a minimum-sized RPC call, were received.	Calls/Sec	
	Xdr failed call rate: Indicates the rate at which RPC calls with a header that could not be XDR decoded, were received.	Calls/Sec	

2.6.2 NetApp NFS Test

The NaNfs test reports the statistics related to the NFS (Network File System) service executing on a NetApp filer.

Purpose	Reports the statistics related to the NFS (Network File System) service executing on a NetApp filer
Target of the test	A NetApp filer

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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for a NetApp filer		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Call rate: Indicates the rate of NFS calls received.	Calls/Sec	
	Bad call rate: Indicates the rate of calls rejected by the NFS layer.	Calls/Sec	
	Percent bad calls: Indicates the percentage of NFS calls rejected by the NFS layer.	Percent	

2.6.3 NetApp CIFS Test

The NaCifs test reports the statistics related to the CIFS (Common Internet File System) service executing on a NetApp filer.

Purpose	Reports the statistics related to the CIFS (Common Internet File System) service executing on a NetApp filer
Target of the test	A NetApp filer
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for a NetApp filer		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Connected users: Indicates the current number of CIFS users on the filer.	Number	
	Active sessions: Indicates the current number of active CIFS sessions on the filer.	Number	
	Operation rate: Indicates the number of CIFS operations done by the filer, since the last time the statistics were cleared.	Operations/Sec	
	Call rate: Indicates the rate at which CIFS calls were received.	Calls/Sec	
	Bad call rate: Indicates the rate at which CIFS calls were rejected	Calls/Sec	
	Read rate: Indicates the rate at which CIFS read operations were performed on a file or directory.	Percent	
	Write rate: The rate at which CIFS write operations were performed on a file or directory	Writes/Sec	

Chapter

3

Monitoring NetApp NetCache

The Network Appliance Netcache line of products is a fully scalable suite of appliances and security systems designed to tackle the problems of Web content delivery and regulation.

NetApp NetCache appliances addresses the three major challenges facing Web service operators today:

- **Internet security**. The NetCache products form the basis of the NetApp Internet Access and Security (IAS) solution, allowing Internet security capabilities that are crucial to maintaining a secure and properly regulated environment. These include proxy, caching, access control, content filtering, Web antivirus, SSL scanning, IM and P2P blocking, antispam, and reporting.
- **Web content and application acceleration**. The NetCache appliances reduce delays, bandwidth usage, and server load to improve delivery of Web content and Web-based applications such as ERP and CRM systems.
- **Video delivery**. The NetCache appliances help to improve on the delivery quality of online training resources, executive video broadcasts, and large-scale video-on-demand services.

This simply means that IT service operators manning critical Web-based services will not tolerate even the slighest of disturbances in the performance of the NetCache appliances, as it can cause serious security breaches, escalate bandwidth usage and related costs, and kill the quality of video broadcasts, thereby severely damaging the user experience with the service.

If such an outcome is to be avoided, the NetCache appliances should be constantly monitored.

eG Enterprise offers an exclusive *NetApp NetCache* monitoring model (se Figure 3.1) which monitors the hardware, resource usage, and services offered by the NetCache appliances, and reports anomalies (if any).

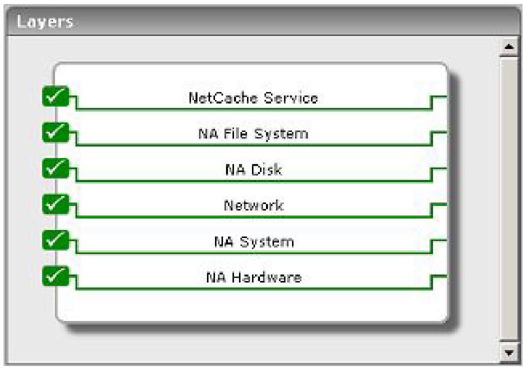


Figure 3.1: The layer model of a NetApp NetCache device

As the bottom 5 layers of Figure 3.1 have already been discussed in Chapter 2 of this document, the section that follows will talk about the **NetCache Service** layer only.

3.1 The NetCache Service Layer

The tests associated with this layer monitor the HTTP, FTP, and NNTP requests to the NetCache appliance. In addition, the layer also reveals how well the appliance handles video streaming requests.

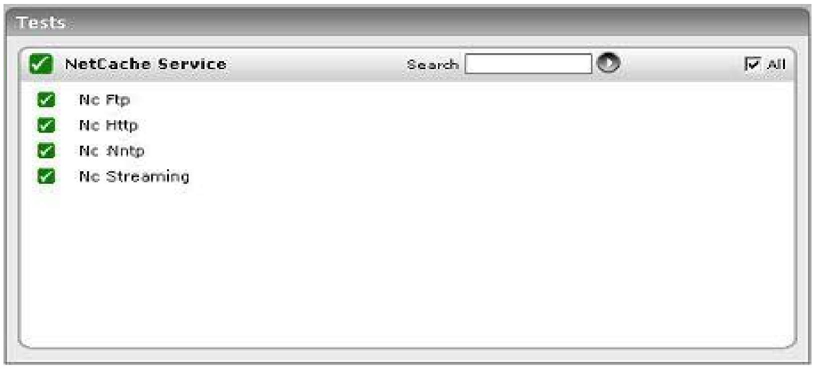


Figure 3.2: The tests associated with the NetCache Service layer

3.1.1 Nc HTTP Test

The NcHttp test monitors the HTTP requests to a NetApp NetCache device using SNMP.

Purpose	Monitors the HTTP requests to a NetApp NetCache device using SNMP
Target of the test	A NetApp NetCache
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for a NetApp NetCache		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Server connections: Indicates the number of simultaneous TCP/IP connections to the servers.	Number	
	Client connections: Indicates the number of simultaneous TCP/IP connections to clients.	Number	
	Request rate: Indicates the rate of HTTP requests to the NetCache.	Reqs/Sec	
	Hit request rate: Indicates the rate at which HTTP requests resulted in hits.	Reqs/Sec	A high value will increase the bandwidth savings, thereby reducing the response time.
	Miss request rate: Indicates the rate at which HTTP requests resulted in misses.	Reqs/Sec	A high value will increase the response time.
	Avg response time: Indicates the average response time for all HTTP requests.	Secs	A high value over a period of time may be indicative of poor cache hits.
	Avg hit response time: Indicates the average response time for HTTP hit requests.	Secs	A high value over a period of time may indicate poor cache performance.
	Avg miss response time: Indicates the average response time for HTTP miss requests.	Secs	

	Response time per byte: Indicates the response time per byte for HTTP requests.	Secs	

3.1.2 Nc FTP Test

The NcFtp test monitors the FTP requests to the NetCache using SNMP.

Purpose	Monitors the FTP requests to a NetApp NetCache device using SNMP
Target of the test	A NetApp NetCache
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for a NetApp NetCache		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Server connections: Indicates the number of simultaneous TCP/IP connections to the servers.	Number	
	Client connections: Indicates the number of simultaneous TCP/IP connections to clients.	Number	
	Request rate: Indicates the rate of FTP requests to the NetCache.	Reqs/Sec	
	Hit request rate: Indicates the rate at which FTP requests resulted in hits.	Reqs/Sec	A high value will increase the bandwidth savings, thereby reducing the response time.
	Miss request rate: Indicates the rate at which FTP requests resulted in misses.	Reqs/Sec	A high value will increase the response time.
	Response time per byte: Indicates the response time per byte for FTP requests.	Secs	

3.1.3 Nc NNTP Test

The NcNnp test monitors the NNTP requests to the NetCache using SNMP.

Purpose	Monitors the NNTP requests to a NetApp NetCache device using SNMP
Target of the test	A NetApp NetCache
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for a NetApp NetCache		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Server connections: Indicates the number of simultaneous TCP/IP connections to the servers.	Number	
	Client connections: Indicates the number of simultaneous TCP/IP connections to clients.	Number	
	Request rate: Indicates the rate of NNTP requests to the NetCache.	Reqs/Sec	
	Cacheable request rate: Indicates the rate of NNTP requests that are cacheable	Reqs/Sec	A high value will increase the bandwidth savings, thereby reducing the response time.
	Proxy request rate: Indicates the rate of NNTP requests that are non-cacheable	Reqs/Sec	A high value will increase the response time.
	Response time per byte: Indicates the response time per byte for NNTP requests.	Secs	

3.1.4 Nc Streaming Test

The NcStreamingTest monitors the streaming requests to the NetCache using SNMP.

Purpose	Monitors the streaming requests to a NetApp NetCache device using SNMP
Target of the test	A NetApp NetCache
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. **SNMPPORT** – The port at which the server exposes its SNMP MIB. The default is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the target device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear. 6. **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. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **authpass** by retyping it here. 9. **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 10. **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. 11. **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **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.		
Outputs of the test	One set of results for a NetApp NetCache		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Server connections: Indicates the number of simultaneous TCP/IP connections to the servers.	Number	
	Client connections: Indicates the number of simultaneous TCP/IP connections to clients.	Number	
	Request rate: Indicates the rate of streaming requests to the NetCache.	Reqs/Sec	
	Hit request rate: Indicates the rate at which streaming requests resulted in hits.	Reqs/Sec	A high value will increase the bandwidth savings, thereby reducing the response time.
	Miss request rate: Indicates the rate at which streaming requests resulted in misses.	Reqs/Sec	A high value will increase the response time.
	Response time per byte: Indicates the response time per byte for streaming requests.	Secs	

Chapter

4

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 **NetApp products**. 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.