Monitoring NetApp NetCache

eG Innovations Product Documentation

www.eginnovations.com

Table of Contents

Table of Figures

Chapter 1: Introduction

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. This is where eG Enterprise helps administrators!

Chapter 2: How to Monitor NetApp NetCache Using eG Enterprise?

eG Enterprise monitors the NetApp NetCache using a single eG external agent on any remote host in the environment. This agent is capable of polling the SNMP MIB Of the NetApp NetCache at regular intervals and fetching statistics related its performance.

The broad steps for monitoring NetApp NetCache using eG Enterprise are as follows:

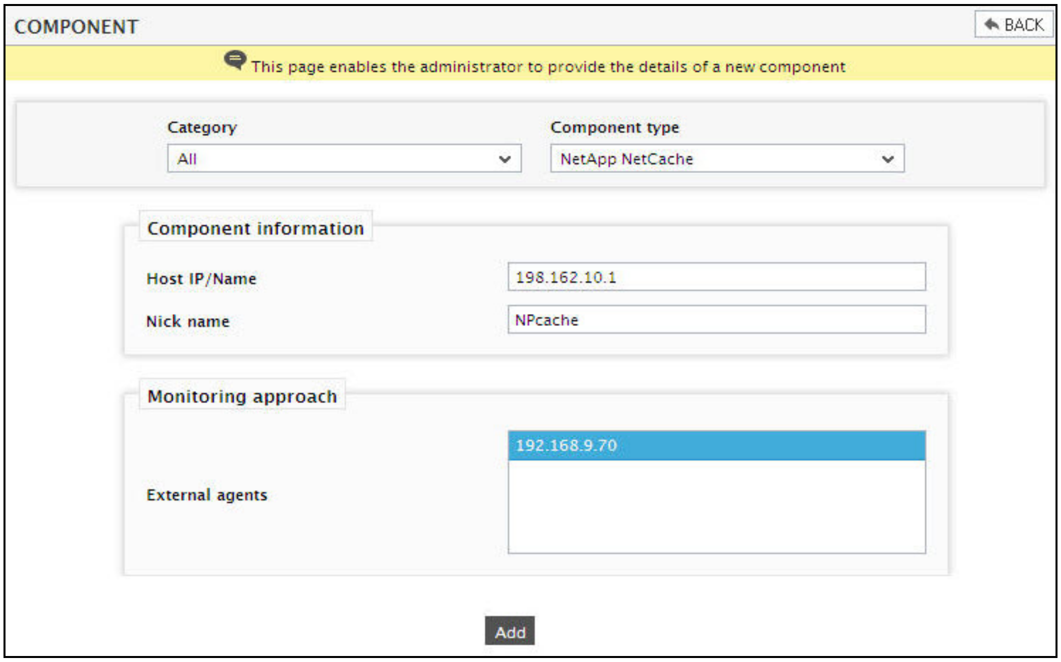
- Managing the NetApp NetCache
- Configuring the tests

These steps have been discussed in following sections.

2.1 Managing the NetApp NetCache

The eG Enterprise cannot automatically discover the NetApp NetCache. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a NetApp NetCache component, do the following:

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



COMPONENT

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

Category: All

Component type: NetApp NetCache

Component information

Host IP/Name: 198.162.10.1

Nick name: NPcache

Monitoring approach

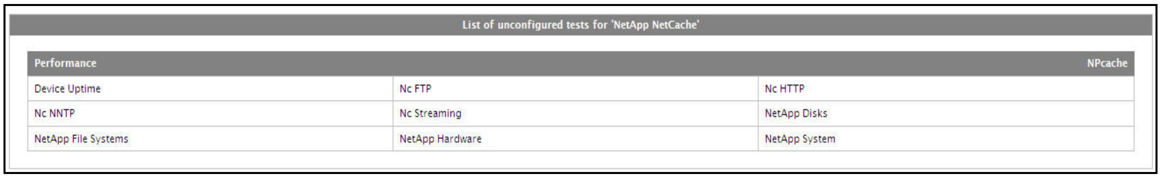
External agents: 192.168.9.70

Figure 2.1: Adding a new NetApp NetCache

4. Specify the **Host IP** and the **Nick name** for the NetApp NetCache in Figure 2.1. Then, click the **Add** button to register the changes.

2.2 Configuring the tests

1. When you attempt to sign out of eG administrative interface, a list of unconfigured tests will appear as shown in Figure 2.2. This list reveals the unconfigured tests requiring manual configuration.



List of unconfigured tests for 'NetApp NetCache'

Performance		NPcache
Device Uptime	Nc FTP	Nc HTTP
Nc NNTP	Nc Streaming	NetApp Disks
NetApp File Systems	NetApp Hardware	NetApp System

Figure 2.2: List of unconfigured tests for the NetApp NetCache

2. To configure the tests, click on the test names in the list of unconfigured tests. For the details on configuring the tests, refer to **Monitoring NetApp NetCache** chapter.

3. Once all the tests are configured, signout of the eG administrative interface.

Chapter 3: Monitoring NetApp NetCache

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

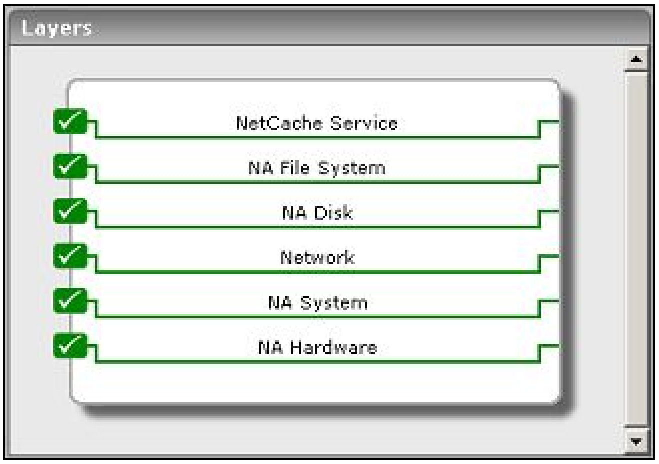


Figure 3.1: The layer model of a NetApp NetCache device

As the bottom 5 layers of Figure 3.1have already been discussed in *Monitoring NetApp Unified Storage* 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.

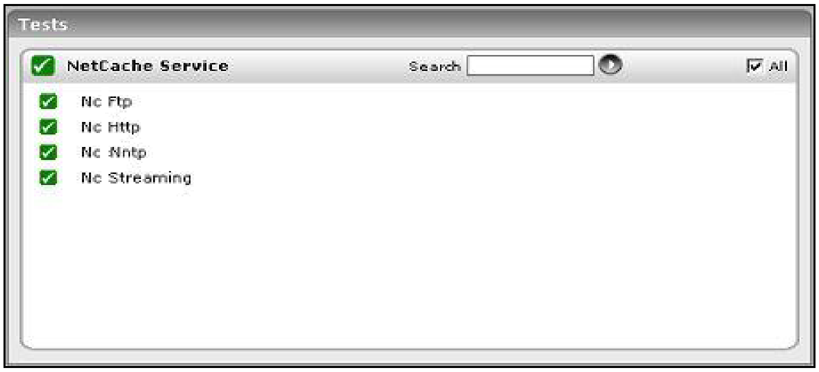


Figure 3.2: The tests associated with the NetCache Service layer

3.1.1 Nc HTTP Test

This test 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

Outputs of the test : One set of results for a NetApp NetCache.

Configurable parameters for the test

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

Parameter	Description
	eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: - **MD5** – Message Digest Algorithm - **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: - **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
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

This test monitors the FTP requests to the NetCache using SNMP.

Target of the test : A NetApp NetCache

Agent deploying the test : An external agent

Outputs of the test : One set of results for a NetApp NetCache.

Configurable parameters for the test

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

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

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Server connections	Indicates the number of simultaneous TCP/IP connections to the servers.	Number	

Measurement	Description	Measurement Unit	Interpretation
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

This test monitors the NNTP requests to the NetCache using SNMP.

Target of the test : A NetApp NetCache

Agent deploying the test : An external agent

Outputs of the test : One set of results for a NetApp NetCache.

Configurable parameters for the test

Parameter	Description
Test period	How often should the test be executed.
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.

Parameter	Description
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

Parameter	Description
	selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	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.

Measurement	Description	Measurement Unit	Interpretation
Response time per byte	Indicates the response time per byte for NNTP requests.	Secs	

3.1.4 Nc Streaming Test

This test monitors the streaming requests to the NetCache using SNMP.

Target of the test : A NetApp NetCache

Agent deploying the test : An external agent

Outputs of the test : One set of results for a NetApp NetCache.

Configurable parameters for the test

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

Parameter	Description
Context	This parameter appears only when **v3** is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPVersion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPVersion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

Parameter	Description
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	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	

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.