
eG
Enabling Service Excellence

Table of contents

Table of Figures

1

Monitoring Citrix Netscaler LB

Citrix NetScaler application delivery solutions combine the features and functions of traditional data center point products - load balancing, caching, compression, SSL acceleration, and attack defense - into a single network appliance, built from the ground up to maximize the performance of mission-critical applications.

All Citrix NetScaler products are built on Citrix's patented Request Switching™ architecture, the industry's only wire-speed technology that handles every application request based on powerful user-defined policies. The Citrix NetScaler application-aware policy engine, AppExpert™, allows the creation of detailed policy-based decisions for individual requests, irrespective of connections. AppExpert lets administrators build sophisticated application request handling policies that enable powerful, comprehensive application-based features.

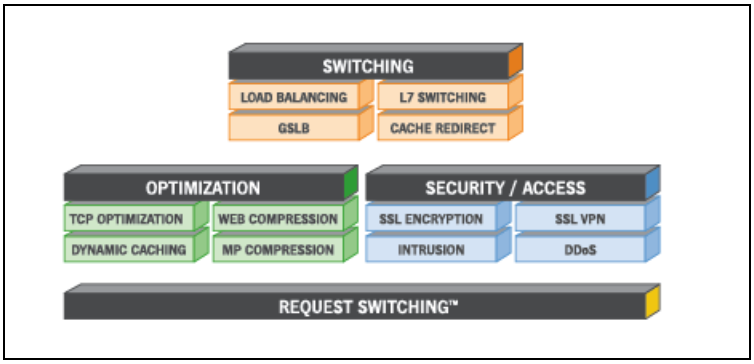

Figure 1.1: The Netscaler architecture

As business entities have begun to rely enormously on the Citrix Netscaler solutions to deliver service continuity and to ensure the secure transaction of business, the smooth functioning of the Netscaler appliance has become super-critical in Citrix infrastructures today. Round-the-clock monitoring of Netscaler products, proactive error reporting, and swift error-clearance are a must to ensure that the Citrix Netscaler is always up and running, and is well enough to attend to application requests from users.

The eG Enterprise-developed specialized *Netscaler LB* monitoring model uses the Netscaler's SNMP MIB to track the Netscaler availability and performance 24x7, warns administrators of probable issues in the functioning of Netscaler, and thus wards off potential performance bottlenecks.

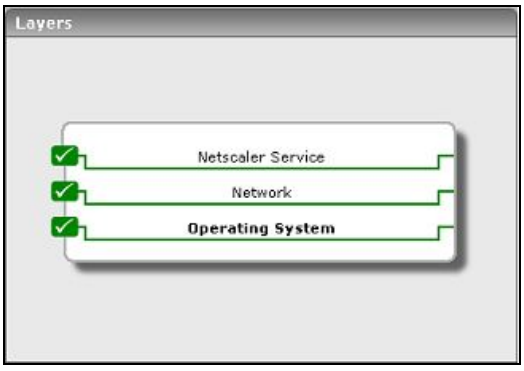

Figure 1.2: Layer model of the Citrix Nescaler

Each layer of this hierarchical layer model is mapped to tests that periodically execute on the Netscaler appliance to evaluate its performance. These tests use the **SNMPPORT** and **SNMPCOMMUNITY** string configurations to connect to the SNMP MIB of the Netscaler appliance, and extract a wide range of performance statistics from the MIB. The sections to come will discuss the tests associated with the each of the layers of the Netscaler monitoring model.

1.1 The Operating System Layer

Using the NsResources test associated with it, the **Operating System** layer tracks the memory and CPU utilization of the Netscaler host.

Figure 1.3: The test associated with the Operating System layer of the Netscaler device

1.1.1 Ns Resources Test

The **NsResources** test monitors the resource usage of the Netscaler device.

Target of the test : A Citrix Netscaler Appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for the Citrix Netscaler being monitored

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** – Refers to the port used by the Citrix Netscaler appliance. By default, this is NULL.
4. **SNMPPORT** - The port number through which the monitored component exposes its SNMP MIB.
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 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.
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) beyond which the SNMP query issues by this test should time out. The default period is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
CPU usage:	Indicates the current CPU usage of the Netscaler device.	Percent	A value close to 100% indicates a CPU bottleneck on the Netscaler device.
Memory usage:	Indicates the percentage of memory available on the Netscaler device that is currently in use.	Percent	
System memory:	Indicates the amount of memory available/configured on the Netscaler device.	MB	This is a configuration metric.
Number of CPUs:	Indicates the number of processing units available on the Netscaler device.	Number	This is a configuration metric.
SSL cards:	Indicates the number of cards available for SSL processing by the Netscaler device.	Number	This is a configuration metric.

1.2 The Network Layer

Besides indicating the availability and responsiveness of network connections to the Netscaler device, the tests mapped to the **Network** layer also reveals the health of network interfaces supported by the device, and the performance of each of the VLANs configured on the device.

Figure 1.4: The tests associated with the Network layer

Since the **Network** test and **NetworkInterfaces** test have been dealt with in great detail in the *Monitoring Unix and Windows Servers* document, the following section discusses the NsVlans test only.

1.2.1 Ns VLANs Test

The Ns VLANs test monitors the network traffic over each of the VLANs configured on the Netscaler device.

Target of the test : A Citrix Netscaler Appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for every VLAN configured on the Citrix Netscaler being monitored

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** – Refers to the port used by the Citrix Netscaler appliance. By default, this is NULL.
4. **SNMPPORT** - The port number through which the monitored component exposes its SNMP MIB.
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 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.
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) beyond which the SNMP query issues by this test should time out. The default period is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Packets received:	Indicates the rate at which packets were received on a VLAN during the last measurement period.	Packets/Sec	
Data receive rate:	Indicates the rate at which data was received over a VLAN during the last measurement period.	MB/Sec	
Packets sent:	Indicates the rate at which	Packets/Sec	

Measurement	Description	Measurement Unit	Interpretation
	packets were transmitted on a VLAN during the last measurement p.		
Data transmit rate:	Indicates the rate at which data was transmitted over a VLAN during the last measurement period.	MB/Sec	
Packets dropped:	Indicates the packets dropped over a VLAN during the last measurement period.	Number	
Packet drop ratio:	Indicates the percentage of the total packets handled (i.e., sum of the packets received and transmitted) which were dropped during the last measurement period.	Percent	Ideally, this value should be close to 0.

1.3 The Netscaler Service Layer

Using the tests associated with it, this layer monitors the HTTP requests to the Netscaler device, its responses, and TCP traffic to and from the device; it also periodically watches the load on the device, so that the administrator is promptly alerted upon an overload.

Figure 1.5: The tests associated with the Netscaler Service layer

1.3.1 Ns HTTP Test

This test monitors HTTP connections handled by the Netscaler appliance, and reveals whether all HTTP requests have been responded to, and whether any incomplete requests/responses have been received/sent by the Netscaler.

Target of the test : A Citrix Netscaler Appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Citrix Netscaler being monitored

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** – Refers to the port used by the Citrix Netscaler appliance. By default, this is NULL.
4. **SNMPPORT** - The port number through which the monitored component exposes its SNMP MIB.
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 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.
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) beyond which the SNMP query issues by this test should time out. The default period is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
New HTTP requests:	Indicates the number of new HTTP requests to the netscaler device in the last measurement period.	Number	This is an indicator of workload on the netscaler device.
HTTP 1.0 requests:	Indicates the number of new HTTP v 1.0 requests to the netscaler device in the last measurement period.	Number	Since HTTP 1.0 connections are not capable of providing information about the client's ability to accept compressed data, which is one of the features of the Netscaler devices, it is important to be able to monitor the number of HTTP 1.0 connections relative to the the total connections.
Requests with incomplete headers:	Indicates the number of	Number	The Netscaler performs content filtering

Measurement	Description	Measurement Unit	Interpretation
	incomplete HTTP header received in the last measurement period with incomplete headers.		by inspecting every incoming request according to user- configured rules, which are based on HTTP headers. If these headers are incomplete, the Netscaler would not be able to interpret the rules correctly, thus exposing the server to potential attacks. A high value of this measure is hence, undesirable; the reasons for the same should be investigated and the root-cause should be promptly addressed.
Incomplete HTTP requests:	Indicates the number of incomplete HTTP requests received in the last measurement period.	Number	
Incomplete responses:	Indicates the number of incomplete HTTP responses from the Netscaler device during the last measurement period.	Number	This value should typically be small under normal operation.
Pipelined requests:	Indicates the number of pipelined requests since the last measurement period.	Number	HTTP/1.1 allows multiple HTTP requests to be written out to a socket together without waiting for the corresponding responses. The requestor then waits for the responses to arrive in the order in which they were requested. The act of pipelining the requests can result in a dramatic improvement in page loading times, especially over high latency connections.
Server busy errors:	Indicates number of HTTP requests for which server busy errors were sent during	Number	Ideally, this value should be close to 0.

Measurement	Description	Measurement Unit	Interpretation
	the last measurement period.		
Http gets:	Indicates the number of HTTP GETs received during the last measurement period.	Number	By analyzing HTTP GET and POST requests and filtering out known bad signatures, you can defend against HTTP-based attacks such as variants of Nimda and Code Red virus.
Http posts:	Indicates the number of HTTP POSTs received during the last measurement period.	Number	
HTTP responses:	Indicates the number of new HTTP responses generated from the Netscaler device during the last measurement period.	Number	Compare the value of new requests and responses. These values should be close to each other. A significant deviation may indicate a bottleneck or malfunctioning of the Netscaler device.
HTTP 1.0 responses:	Indicates the number of new HTTP v 1.0 responses sent back during the last measurement period.	Number	

1.3.2 Ns TCP Test

This test monitors TCP connections and retransmissions handled by the Netscaler appliance.

Target of the test : A Citrix Netscaler Appliance

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Citrix Netscaler being monitored

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** – Refers to the port used by the Citrix Netscaler appliance. By default, this is NULL.
4. **SNMPPORT** - The port number through which the monitored component exposes its SNMP MIB.

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 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.
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) beyond which the SNMP query issues by this test should time out. The default period is 10 seconds.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Server connections:	Indicates the number of	Number	

Measurement	Description	Measurement Unit	Interpretation
	server connections in the NetScaler device.		
Client connections:	Indicates the number of client connections in the NetScaler device.	Number	
Connections serving requests:	Indicates the number of connections to the Netscaler device that are currently serving requests.	Number	This metric is a key indicator of the workload handled by the Netscaler device.
Server connections in established state:	Indicates the number of server connections in NetScaler in established state.	Number	
Client connections in established state:	Indicates the number of client connections in NetScaler in established state.	Number	
Spare connections:	Indicates the number of spare connections ready to be used.	Number	
Surge queue length:	Indicates number of number of connections in surge queue.	Number	The Netscaler device can be used to limit the number of simultaneous requests that are passed on to a server. When a request is completed, additional requests are forwarded to the server. If a request arrives and the server is handling the maximum configured number of requests, the Netscaler device places the new request in a surge queue, where the request waits for its turn to be sent to the server for processing. The surge

Measurement	Description	Measurement Unit	Interpretation
			queue allows a server to run at peak capacity without the risk of having it spiral out of control because of a surge of incoming requests. The surge queue length indicates whether a server is able to keep up with its incoming workload or not. If the surge queue is consistently greater than 0, this indicates that the server is not able to keep up with the workload and additional server capacity is required. On the other hand, a periodic surge is not a cause for concern.
Server connections opened:	Indicates the total number of opened server connections.	Number	
Client connections opened:	Indicates the total number of opened client connections.	Number	
Data traffic received:	Indicates the TCP traffic received during the last measurement period.	MB/Sec	
Data transmit rate:	Indicates the TCP traffic transmitted during the last measurement period.	MB/Sec	
Connection establishment timeouts:	Indicates the number of times connection establishment timed out during the last measurement period.	Number	
Connection retries:	Indicates the number of times TCP connection established was retried during the last measurement period.	Number	

Measurement	Description	Measurement Unit	Interpretation
Client retransmissions:	Indicates the number of retransmissions from clients during the last measurement period.	Number	Ideally, the number of retransmissions should be a small fraction (< 5%) of the total number of transmissions.
Server retransmissions:	Indicates the number of retransmissions from servers during the last measurement period.	Number	Ideally, the number of retransmissions should be a small fraction (< 5%) of the total number of transmissions.
Retransmits sent:	Indicates the number of retransmissions sent during the last measurement period.	Number	
TCP retransmission failures:	Indicates the number of retransmission failures during the last measurement period.	Number	

1.3.3 Ns Usage Test

This test monitors the workload on the Netscaler appliance and the usage of its CPU resources.

Target of the test : A Citrix Netscaler Appliance

Agent deploying the test : An internal agent

Outputs of the test : One set of results for every Citrix Netscaler being monitored

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** – Refers to the port used by the Citrix Netscaler appliance. By default, this is NULL.
4. **SNMPPORT** - The port number through which the monitored component exposes its SNMP MIB.
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 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.

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) beyond which the SNMP query issues by this test should time out. The default period is 10 seconds

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
New client connections:	Indicates the number of new client connections to the Netscaler device in the last measurement period.	Number	

Measurement	Description	Measurement Unit	Interpretation
New server connections:	Indicates the number of new connections established between servers and the Netscaler device in the last measurement period.	Number	
Tcp offload factor:	This factor monitors the connections from the Netscaler device to servers as a factor of the connections it receives from clients.	Percent	One of the key benefits of the Netscaler device is its ability to offload TCP connection processing from the servers to the Netscaler device itself. By doing so, the Netscaler device allows the existing server infrastructure to support a larger workload. The lower the value of this metric, the greater the benefits of the Netscaler device.
Current client connections:	Indicates the number of connections currently established by clients to the Netscaler device.	Number	
Current server connections:	Indicates the number of connections currently established by the Netscaler device to servers.	Number	
Client connections refused:	Indicates the number of connections from clients that were refused by the Netscaler device during the last measurement period.	Number	This value should be close to 0 for ideal operation.
Cookie sequence mismatch rejects:	Indicates the number of connections rejected because of syn cookie sequence number mismatch.	Number	Normal SYN cookies contain encoded information that makes it near impossible to request a connection to a host from a forged (spoofed) originating address. In this scenario, the attacker must guess a valid TCP sequence

Measurement	Description	Measurement Unit	Interpretation
			number used by that server to connect to some other legitimate host. The cryptographic protection in the standard SYN cookie makes this attack possible with as few as one million guesses, which is not impossible for a determined attacker. NetScaler uses an enhanced SYN cookie protection scheme that is fully compatible with the TCP/IP protocol, but have rendered the "forged connection" technique obsolete. Each new connection is unrelated to previous connections, and knowing a valid sequence number used for a previous connection will not enable an attacker to forge a connection. A large value of this measure could indicate failed attempts made to hack into a network. Further investigation is hence, necessary.
Cookie signature mismatch rejects:	Indicates the number of connections rejected because of syn cookie signature mismatch.	Number	
Unacknowledged SYNs received:	Indicates the number of connections dropped because of unacknowledged SYN packets.	Number	When a client attempts to establish a TCP connection to a server, the client and server exchange a set sequence of messages. This connection technique applies to all TCP connections (for example, Telnet, web, E-mail, and so on). The sequence for the TCP connections are: • The client sends a SYN message to the server. • The server acknowledges the SYN message by sending a SYN-ACK

Measurement	Description	Measurement Unit	Interpretation
			message to the client. • The client finishes establishing the connection by responding to the server with an ACK message When the sequence is complete, the connection between the client and server is open, and service-specific data can be exchanged between the client and server. The potential for attack arises at the point when the back-end server has sent an acknowledgment (SYN-ACK) to the client but has not received the ACK message from the client; this is referred to as a half-open connection in the server. A high value of this measure indicates that too many such half-open connections exist in the server, which could consume excessive system memory, causing the server system to crash or hang, or deny service to legitimate clients.
Open connections to servers:	Indicates the number of connections established with servers.	Number	
Server connection hits:	Indicates the number of client transactions in the last measurement period that used the server connection in the reuse pool.	Number	Netscaler appliances support a 'Connection Keep-Alive' feature that is enabled for HTTP protocols, so that persistent connections are available between the system and the client over the WAN link and also between the system and the server. This is achieved by mimicking HTTP “connection-persistence” behavior to both the client and server. The server

Measurement	Description	Measurement Unit	Interpretation
			always perceives that it is communicating with a persistent client (even if the client is not persistent) and the client always thinks it is communicating with a persistent server (even if the server is configured not to do keep-alive; for example, the server is configured to do one request per connection). One of the key benefits of this feature to a server is the creation and maintenance of a pool of ready-to-go fast server connections (i.e., the reuse pool). This pool ensures that connection requests from clients are serviced by the pool itself without having to open actual connections on the server, and thus greatly reduces the connection-burden on the server. If the value of the *Server connection hits* measure is very low or the *Server connection misses* measure is very high, it indicates that the pool is not been effectively utilized. A very low *Server connection pool hit ratio* is also indicative of the same. If such a situation persists, it can only result in more physical connections been opened on the server, and consequently, excessive CPU and memory erosion at the server-level. You can counter this abnormal event by ensuring that the Connection Keep-Alive feature is always enabled.
Server connection misses:	Indicates the number of new connections made during the last measurement period because the server connection was unavailable in reuse pool.	Number	
Server connection pool hit ratio:	This metric is a measure of the efficiency of the server reuse pool.	Percent	
CPU usage:	Indicates the current CPU usage of the Netscaler device.	Percent	Ideally, this value should be low.

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 **Citrix Environments**. 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.