NetIQ Access Manager 3.2

Performance and Sizing Guidelines

Performance, Reliability, and Scalability Testing

Revisions

This table outlines all the changes that have been made to this document (in reverse chronological order):

Version	Date	Details
1.4	August 13,2012	- Added Access Manager Service for Windows under ***Tuning Parameters***. - Added Access Manager Service for Windows under ***Results***.
1.3	July 30,2012	- Added an Appendix for tests with shared secrets. - Moved “Linux Access Gateway” and “SSL VPN Performance” to Appendix.
1.2	July 09, 2012	- Added Access Manager Appliance under ***Tuning Parameters***. - Added Access Manager Appliance under ***Results***.
1.1	June 18, 2012	- Modified Access Gateway Service for SLES under ***Tuning Parameters***.. - Modified Access Gateway Service for SLES under ***Results***.
1.0	June 04, 2012	- Added Access Gateway Appliance under ***Tuning Parameters***.. - Added Access Gateway Appliance under ***Results***.

Contents

1 Introduction

NetIQ® Access Manager is a comprehensive access management solution that provides secure access to Web and enterprise applications. Access Manager provides seamless Single Sign-on across technical and organizational boundaries. It uses industry standards that include Secure Assertions Markup Language (SAML) and Liberty Alliance protocols.

This white paper details the performance, reliability, and scalability of NetIQ® Access Manager so that you can deploy the correct configuration in your environment. The test results are simulated and every environment is different. But, the data should help in determining the design of your system. This paper specifically refers to the 3.2 release of NetIQ Access Manager shipped in May 2012.

1.1 Key Features of NetIQ Access Manager

The key features of Access Manager include:

- Contains basic and advanced authentication methods
- Has a federation-based architecture
- Allows Single Sign-on to all Web-based applications
- Secures access to enterprise applications through an integrated SSL VPN
- Enforces corporate policies for required software remote users
- Delivers roles-based access control for Web-based and enterprise applications
- Establishes federated links with trusted business partners

2 Test Strategy

The test was designed to represent a medium-sized business with heavy traffic to help predict performance for both smaller and larger implementations. The performance, reliability, and scalability tests cover the critical areas that customers need to know about how to design a system for their environment.

A sizing guide is included to help determine the number of users that can be supported on a specific number of servers.

The tests cover the major functional areas of public access, authentication, and authorization.

- The public requests test the gateway as a reverse proxy with caching to help increase the speed of your Web servers.
- The authentication requests test the distributed architecture that provides secure login to NetIQ Access Manager.
- The authorization requests test the policy evaluation that occurs after the login has been completed and before the page is delivered.
- The environment included a cluster of 4 Identity Servers and 4 Access Gateways. The number of users and the amount of traffic determine the size of the cluster.

2.1 Access Gateway

Performance Testing:

- HTTP traffic through a public resource
- HTTPS traffic through a public resource
- HTTPS traffic through a protected resource
- HTTPS traffic through a protected resource with Form Fill
- HTTPS traffic through a protected resource with Identity Injection
- HTTPS traffic through a protected resource with policies that contain roles
- HTTPS traffic through a protected resource with 10 additional page requests

Reliability Testing:

- HTTPS traffic for two weeks through a stress test
- Scalability (Clustering) testing:

- 2 x 4 x 4 (2 Administration Console servers, 4 Identity Server servers, and 4 Linux Access Gateway servers)
- 2 x 4 x 4 (2 Administration Console servers, 4 Identity Server servers, and 4 Access Gateway Appliance servers)

Failover Testing:

- HTTP/HTTPS traffic continues after a component failover

2.2 SSL VPN

Enterprise mode performance and reliability testing to a high bandwidth server:

- Initiate the SSL VPN connections from multiple clients in the Enterprise mode from a mix of Windows and SUSE® Linux Enterprise Desktop (SLED) clients.
- After the connection is established, initiate continuous traffic over the tunnel by using the FTP scripts.
- Run the test for 8 hours.
  Monitor the utilization and connection failures.

Kiosk mode performance and reliability testing to a high bandwidth server:

- Initiate the SSL VPN connections from multiple clients in the Kiosk mode from a mix of Windows and SLED clients.
- After the connection is established, initiate continuous traffic over the tunnel by using the FTP scripts.
- Run the test for 8 hours.
  Monitor the utilization and connection failures.

2.3 Test Setup

This section includes:

- Server Hardware for Access Gateway Appliance Tests
- Server Hardware for Access Gateway Service on SLES Tests
- Server Hardware for Access Manager Appliances Tests
- Server Hardware for SSL VPN Tests
- Client Hardware

- Load Balancers
- Configuration Details
- Performance/Reliability/Stress Tools

2.3.1 Server Hardware for Access Gateway Appliance Tests

The Access Gateway clustered tests are run on an ESXi 4.1 virtualized environment on 2 Dell PowerEdge R710 machines.

4 Access Gateway Appliances were running on an ESX server installed on a Dell PowerEdge R710 machine. This setup has the following configuration:

Dual 4-core CPU x 2.40 GHz, 96 GB RAM and six 15 K rpm hard disks.

2 Administration Consoles, 4 Identity Server, 2 Apache Web servers, and 3 eDirectory user stores were deployed on another ESX server installed on another Dell PowerEdge R710 machine. This setup has the following configuration:

Dual 6-core CPU x 2.925 GHz, 96 GB RAM, and six 15 k rpm hard disks.

Virtual Machine design is as follows:

- 2 Administration Consoles (2xCPU 2.925 GHz, 4 GB RAM)
- 4 Identity Servers (4xCPU 2.925 GHz, 16 GB RAM)
- 4 Access Gateway Servers (4xCPU 2.40 GHz, 16 GB RAM)
- 3 external eDirectory user stores running eDirectory v8.8 SP6 with 100,000 users (2xCPU 2.925 GHz, 4 GB RAM)
- 2 Apache2 Web server running on SLES 11 SP1 (2xCPU 2.925 GHz, 4 GB RAM)

2.3.2 Server Hardware for Access Gateway Service on SLES Tests

The Access Gateway Service clustered tests are run on an ESXi 4.1 virtualized environment on 2 Dell PowerEdge R710 machines.

The Access Gateway Service on 4 SLES servers were running on an ESX server installed on one Dell PowerEdge R710 machine. This setup has the following configuration:

- Dual 4-core CPU x 2.40 GHz, 96 GB RAM and six 15 K rpm hard disks.
- 2 Administration Consoles, 4 Identity Server servers, 2 Apache Web servers, and 3 eDirectory user stores were deployed on another ESX server installed on another Dell PowerEdge R710 machine.

This Dell PowerEdge R710 machine has the following configuration:

- Dual 6-core CPU x 2.925 GHz, 96 GB RAM, and six 15 k rpm hard disks.

Virtual Machine design is as follows:

- 2 Administration Consoles (2xCPU 2.925 GHz, 4 GB RAM)
- 4 Identity Servers (4xCPU 2.925 GHz, 16 GB RAM)
- 4 Access Gateway Servers (4xCPU 2.40 GHz, 16 GB RAM)
- 3 external eDirectoryTM user stores running eDirectory v8.8 SP6 with 100,000 users (2xCPU 2.925 GHz, 4 GB RAM)
- 2 Apache2 Web server running on SLES 11 SP1 (2xCPU 2.925 GHz, 4 GB RAM)

2.3.3 Server Hardware for Access Manager Appliances Tests

The Access Manager Appliances clustered tests are run on a combination of ESXi 5.0 and ESXi 4.1 virtualized environment setup on the Dell PowerEdge R720 and Dell PowerEdge R710 servers respectively.

The hardware configuration of the ESXi 5.0 server contains six dual core Intel Xeon CPUs @ 2.9 GHz, 96 GB RAM, eight 15 K rpm hard disk. This setup has the following configuration:

- 3 Access Manager Appliance instances each with 4x2.40 GHz CPUs and 32 GB RAM

The hardware configuration of the ESXi 4.0 server contains six dual core Intel Xeon CPUs @ 2.9 GHz, 96 GB RAM, eight 15 K rpm hard disk. This setup has the following configuration:

- 1 Access Manager Appliance instance with 4x2.40GHz CPU, 32 GB RAM
- 3 external eDirectoryTM user stores running eDirectory v8.8 SP6 with 100,000 users (2xCPU 2.925 GHz, 4 GB RAM)
- 2 Apache2 Web server running on SLES 11 SP1 (2xCPU 2.925 GHz, 4 GB RAM)

2.3.4 Server Hardware for the Access Gateway Service on Windows Tests

The Access Gateway Services on Windows tests are run on a combination of ESXi 5.0 and 4.1 virtualized environment setups on the Dell PowerEdge R 720 and Dell PowerEdge R710 servers respectively.

The ESXi 5.0 server hardware configuration consists of six dual core Intel Xeon CPUs @ 2.9 GHz, 96 GB RAM, and eight 15 K rpm hard disks. This setup has the following configuration:

- 4 Access Gateway Services on Windows 2008 R2 servers each with 4x2.40 GHz CPUs and 16 GB RAM

The hardware configuration of the ESXi 4.0 server contains six dual core Intel Xeon CPUs @ 2.9 GHz, 96 GB RAM, eight 15 K rpm hard disks. This setup has the following configuration:

- 2 Administration Consoles (2xCPU 2.925 GHz, 4 GB RAM)

- 4 Identity Servers (4xCPU 2.925 GHz, 16 GB RAM)
- 3 external eDirectoryTM user stores running eDirectory v8.8 SP6 with 100,000 users (2xCPU 2.925 GHz, 4 GB RAM)
- 2 Apache2 Web server running on SLES 11 SP1 (2xCPU 2.925 GHz, 4 GB RAM)

2.3.5 Client Hardware

Client machine running the LoadRunner application had various configurations:

- Operating system: Windows XP, Windows Server 2003
- Processor: Single core CPU, Dual core CPU
- Memory: 2 GB, 4 GB

2.3.6 Load Balancers

The following L4 switches are used as load balancers for our testing:

- Zeus ZXTM LB (software L4 switch)
- Brocade ServerIron ADX 1000 (hardware L4 switch)
- Alteon 3408 (hardware L4 switch)

2.3.7 Configuration Details

- HTML pages are approximately 50 KB with 50 small images embedded for all public page tests.
- For authentication, authorization, identity injection, and form fill tests, HTML page was a small page of 200 B with one hyperlink in it. These tests focus on the authentication, authorization, identity injection, and form fill performance rather than the page rendering performance.
- The Access Manager user stores configurations that contain 20 threads with 100,000 users in a single container. We validated that multiple containers received the same performance, but these tests were done with optimization and fast hardware. If you do not optimize and increase the speed of your hardware, you will see decreased performance. The primary user store used in the tests was eDirectory 8.8.6.

2.3.8 Performance/Reliability/Stress Tools

The HP Mercury LoadRunner tool is used for testing the Identity Server and Access Gateway. This tool replicates large IP ranges correctly between multiple clients in a clustered environment. This allowed the tests to more closely simulate real-world environments with real browser interaction such as Internet Explorer and Firefox.

The following are the specifications of the LoadRunner tests:

- The virtual user has 500 threads among 17 clients. This is the optimal amount of threads before the system started to receive excessive login times.
- The scripts used are HTML-based scripts describing user actions. This is listed under the recording level and the HTML advanced option. This type of script helps to clear cached data inside the script but still downloads all the data that is linked to the page.

If you do not have a sufficient IP address setup for LoadRunner, you must use solid load balancing on the Layer 4 switch. You must have parameters for the users to avoid the same user for every connection.

The SSL VPN tests were done with the NetIQ Superlab test automation tool, SLATH, with the help of tools such as ftp-script, HTTP torture, LTFX, and iperf. The focus of the testing was to exercise the scalability of the product across multiple protocols and high bandwidth.

The combinations of tools were used to increase the performance.

2.4 Other Factors Influencing Performance

Apart from the hardware and test configuration, other factors in a network also impact overall performance.

These factors include:

- **L4 Switches:** If the switch is slow or misconfigured, it can severely impact performance. System Test recommends that clustered Access Manager components to be plugged directly into the switch or segmented accordingly. It is also critical that you enable sticky bit/persistence on the L4 switch. When this feature is not enabled, the product handles the traffic correctly, but can run up to 50% slower when persistence is disabled.
- **Network Bandwidth:** Gigabit copper networking is used throughout the testing process, so this is a requirement for the product to meet the testing results. If you are running at 100 MB or have a slow Internet connection, the product cannot solve this bottleneck.
- **Web Servers:** The application servers are a major cause for slowness because they process most of the information. The tests used static and dynamic pages with more than 50 images. The tests were based upon real-world traffic to give a general idea of response times less than a second. The public requests can vary widely based upon size of the page, caching settings, and content, so this needs to be considered.
- **LDAP User Stores:** This critical component can be another major cause for slowness, depending upon configuration, hardware, and the layout of the directory. The user store is usually the most common problem with performance, so testing must be done with the LDAP user stores that will be used in the environment. Expect adjustments if you are attempting to get the maximum speed out of the cluster for the different LDAP user stores. eDirectory is primarily used throughout the testing to give a baseline for the product.

- **Timeout:** If you run a performance test, you must factor in sessions that are stored on the server. The tests have a 5 minute timeouts so that the tests do not overrun the total users on the system of 100,000 active sessions on the cluster. You must take this into account while planning for capacity testing on a cluster.
  Configuring the session timeout for a resource is mostly dependent on the security requirement. If security is not the concern, here are some of the recommendations to fine tune the session timeout configuration to reap the best performance:

  a. If the users access a protected resource for small time and leave the session idle after accessing few pages, configuring small session timeout for such resources is recommended. This will enable the system to remove the idle sessions faster from the system and hence the system does not need to store an idle session.

  b. If the users access a protected resource for long time, configuring a long session timeout is recommended. It will reduce the internal traffic to update the user access and improve the overall performance of the system.

- **Users:** Ensure that you have enough users on the system to run the performance test. If you run 50 threads of logins against Access Manager with each one using the same user to authenticate, Access Manager matches each user and handles all 50 sessions as the sessions of one user. This will skew the test goals and results because it is not a valid user scenario and invalidate the test results.

- **LDAP Attributes or shared secrets:** If access gateway policies require LDAP attributes or shared secrets, you may have to consider the following factors in configuration to get a better performance.

  Retrieving a shared secret attribute takes a considerable amount of time due to the way we store the secrets in remote LDAP user store or in the Administration Console secret store. If the user is accessing multiple Web resources and each Web resource needs a new set of shared secrets or LDAP attributes, each time a new LDAP user store connection to the remote secret store or remote LDAP user store needs to be established. So, whenever new shared secrets or LDAP attributes are required, user will experience a slow response time.

  The best practice is to send all these attributes or shared secrets at the time of authentication itself. You can configure this in the Liberty Service Provider configuration under the Identity Server cluster configuration. With this the ESP will cache all the shared secrets or LDAP attributes required for the entire session at the time of authentication. Hence, the secrets or attributes for subsequent requests are served from the local ESP cache.

  Refer to ***Tests with Shared Secrets*** for the shared secret test results.

3 Tuning Parameters

The following parameters were tuned during the test to optimize the system performance. These parameters must be configured based on the customer environments.

The following parameters are recommended for testing in the staging environment before running on the production environment.

3.1 Identity Server

Tomcat Connector Maximum Thread Setting

In /opt/novell/nam/idp/conf/server.xml, set maxThreads="1000" for port 8443 Connector

```
<Connector NIDP_Name="connector" SSLEnabled="true" URIEncoding="utf-8"
acceptCount="100" address="x.x.x.x" ciphers="XX, XX ,XX, XX" clientAuth="false"
disableUploadTimeout="true" enableLookups="false"
keystoreFile="/opt/novell/devman/jcc/certs/idp/connector.keystore"
keystorePass="p2SnTyZPHn9qe66" maxThreads="1000" minSpareThreads="5" port="8443"
scheme="https" secure="true"
sslImplementationName="com.novell.nidp.common.util.net.server.NIDPSSLImplementation"
sslProtocol="TLS"/>
```

Note: For the Access Manager Appliance installations, the port number will be 2443.

This parameter enables the Identity Server to handle more threads simultaneously to improve the performance. The thread number must be fine-tuned for every customer environment based on the number of attributes attached to a user session. When each user session is holding large number of attributes, each user session requires more heap memory.

The available stack memory reduces as a result. If number of threads configured in this scenario is high, Tomcat will try to spawn more threads and fails due to non-availability of the stack memory. Customer must fine-tune the number of threads based on the attribute usage.

Note: In the Access Manager Service for Windows, the server.xml file is located at C:\Program Files (x86)\Novell\Tomcat\conf\server.xml.

Java Memory Allocations

The Tomcat configuration file controls the amount of memory that Tomcat can allocate for Java.

- If you have installed your Identity Server on a server with the minimum 4 GB of memory, you can modify two parameters in this file to improve performance under heavy load.

  In /opt/novell/nam/idp/conf/tomcat7.conf, set the following parameters:

Replace the Xms and Xmx values to 2048:

```
JAVA_OPTS="-server -Xms2048m -Xmx2048m -Xss128k "
```

This enables the Tomcat process to come up with 2 GB pre-allocated memory.

- If your Identity Server machine has more than 4 GB memory, recommendation is to allocate 50% to 75% of the memory to the Identity Server Tomcat. This needs to be fine-tuned based on each customer’s environment.

- In the performance tests, Identity Server Tomcat was set to 12288 for both Xms and Xmx.where the server had 16 GB memory.

- Change the -Dnids.freemem.threshold value to a value between 5 and 15.
  This parameter prevents user sessions from using up all memory and ensures that there is free memory available so that the other internal Java processes can run. When this threshold is reached, the user receives a 503 server busy message and a threshold error message is logged to the catalina.out file.

  ```
  JAVA_OPTS="${JAVA_OPTS} -Dnids.freemem.threshold=10"
  ```

Note: In the Access Manager Service for Windows, the preceding values can be set by executing the Tomcat7w.exe file located at C:\Program Files (x86)\Novell\Tomcat\bin. Select the Java tab for setting the Initial memory pool and Maximum memory pool values.

LDAP Load Threshold Configuration

In /opt/novell/nam/idp/webapps/nidp/WEB-INF/web.xml, set ldapLoadThreshold to 600.

```
<context-param>

        <param-name>ldapLoadThreshold</param-name>

        <param-value>600</param-value>

 </context-param>
```

This configuration entry enables the Identity Server to make up to 600 connections to the LDAP user store.

Note: In the Access Manager Service for Windows the preceding value can be set in C:\Program Files (x86)\Novell\Tomcat\webapps\nidp\WEB-INF\web.xml file.

3.2 Access Gateway

This section is applicable for Access Gateway Appliance and Access Gateway Service on SLES and Access Manager Appliance.

AJP Connector Maximum Thread Setting

In /opt/novell/nam/mag/conf/server.xml, set maxThreads="1000" for the port 9009 connector.

This parameter enables the Access Gateway ESP to handle more threads simultaneously to improve the performance. The thread number needs to be fine-tuned for every customer environment based on the number of attributes attached to a user session. When each user session is holding large number of attributes, each user session needs more heap memory. The available stack memory reduces as a result. If number of threads configured in this scenario is high, Tomcat will try to spawn more threads and fails due to non-availability of the stack memory. Customer has to fine-tune the number of threads based on the attribute usage.

Note: In the Access Gateway Service for Windows, the server.xml file is located at C:\Program Files\Novell\Tomcat\conf\server.xml.

Java Memory Allocations

The Tomcat configuration file controls the amount of memory that Tomcat can allocate for Java.

- If you have installed your Access Gateway on a machine with the minimum 4 GB of memory, you can modify two parameters in this file to improve performance under heavy load:

  In /opt/novell/nam/mag/conf/tomcat7.conf, set the following parameters:

  Replace the Xms and Xmx values to 2048:

  JAVA_OPTS="-server -Xms2048m -Xmx2048m -Xss128k "

  This enables the Tomcat process to come up with 2 GB pre-allocated memory.

- If your Access Gateway Appliance machine has more than 4 GB memory, recommendation is to allocate 50% to 75% of the memory to the ESP Tomcat. This needs to be fine-tuned based on each customer environment.

- The performance results in this white paper are achieved by setting ESP Tomcat to 12288 for both Xms and Xmx where physical memory available was 16 GB.

  Note: Due to a bug in the throttling code, ESP was not able to go beyond the Xms value and used to ignore the Xmx value. This bug will be fixed in a later release. Until it gets fixed, recommendation is to keep Xms value same as Xmx value.

- Change the -Dnids.freemem.threshold value to a value between 5 and 15.

  This parameter prevents user sessions from using up all memory and ensures that there is free memory available so that the other internal Java processes can continue to function. When this threshold is reached, the user receives a 503 server busy message and a threshold error message is logged to the catalina.out file. JAVA_OPTS="${JAVA_OPTS} -Dnids.freemem.threshold=10"

Note: In the Access Gateway Service for Windows, the preceding values can be set by executing the Tomcat7w.exe file located at C:\Program Files (x86)\Novell\Tomcat\bin directory. Select the Java tab for setting the Initial memory pool and Maximum memory pool values.

Advanced Options

Add a new advanced option as follows:

NAGGlobalOptions ESP_Busy_Threshold=5000

Apache MPM settings

Use the following configuration for the Access Gateway Appliance, Access Gateway Service on SLES, and Access Manager Appliance:

In /etc/opt/novell/apache2/conf/extra/httpd-mpm.conf, mpm_worker_module is by default configured with following settings:

```
<IfModule mpm_worker_module>
        ThreadLimit             300
        StartServers            3
        MaxClients              3000
        MinSpareThreads         3000
        MaxSpareThreads         3000
        ThreadsPerChild         300
        ServerLimit             10
        MaxRequestsPerChild     0
</IfModule>
```

If the Access Gateway server has more memory than 6 GB, set the mpm_worker_module to match the following configuration.

```
<IfModule mpm_worker_module>
        ThreadLimit             1000
        StartServers            9
        ServerLimit             10
        MaxClients              9000
        MinSpareThreads         9000
        MaxSpareThreads         9000
        ThreadsPerChild         1000
        MaxRequestsPerChild     0
</IfModule>
```

The performance tests were conducted with the above configuration when the Access Gateway Appliance and Gateway Service had 16 GB memory available and Access Manager Appliance had 32 GB memory.

If the memory available is less or more, customers must fine-tune each of these configurations based on their environment.

Use the following configuration for the Access Gateway Service for Windows:

The mpm_winnt_module located at C:\Program Files\Novell\apache\conf\extra\httpd-mpm, is by default configured with the following settings:

```
<IfModule mpm_winnt_module>

    ThreadsPerChild   1920

    MaxRequestsPerChild    0

</IfModule>
```

The performance tests were conducted with the default settings. Modifying the default values did not have any impact on the performance.

4 Results

The tests results are divided into the Access Gateway Appliance, Access Gateway Service on SLES, Access Manager Appliance, and Access Gateway Service for Windows sections. These performance numbers are classified by per minute and per second to show how the system performs. Note that 3.2 performance numbers are updated only for the Access Gateway Appliance and Access Gateway Service on SLES.

4.1 Access Gateway Appliance

The following performance numbers are recorded per minute to show how the system performs:

Test Scenario	Results
HTTPS Public (user accessing single page in a session)	1,599,600 requests per minute (1,585,800 hits per minute) and throughput 2,367,311,760 bytes per minute
HTTPS Public (user accessing 10 pages in a session)	957,120 requests per minute (940,020 hits per minute) and throughput 3,730,304,340 bytes per minute
HTTPS Authentications using secure name/password - form	28980 logins per minute
HTTPS Authorizations	20520 authorized pages per minute
HTTPS Authorization with 10 page requests	85500 authorizations per minute

The following performance numbers are recorded per second to show how the system performs:

Test Scenario	Results
Concurrent Sessions in a 4-node Access Gateway cluster	192180 sessions in cluster (approximately 48000 sessions per server)
Concurrent Sessions in a 4-node Identity Server cluster	187531 sessions in cluster (approximately 46000 sessions per server)
HTTP Public	26748 requests (26531 hits per second)
HTTPS Public	26660 requests (26430 hits per second)
HTTPS Authentications using Name/Password – Basic	514 logins per second
HTTPS Authentications using Secure Name/Password – Basic	488 logins per second
HTTPS Authentications using Name/Password – Form	456 logins per second
HTTPS Authentications using Secure Name/Password – Form	483 logins per second
HTTPS Login with Roles/AGA	342 logins per second
HTTPS Login with Identity Injection	245 logins per second
HTTPS Login with Form Fill	241 logins per second
HTTPS Authorizations	1425 authorized pages per second
AGA is Access Gateway Authorization	

4.2 Access Gateway Service on SLES

The following performance numbers are recorded per minute to show how the system performs:

Test Scenario	Results
HTTPS Public (user accessing single page in a session)	1,168,200 requests per minute (1,144,080 hits per minute) and throughput 1,700,436,720 bytes per minute
HTTPS Public (user accessing 10 pages in a session)	967,800 requests per minute (954,000 hits per minute) and throughput 3,784,045,320 bytes per minute
HTTPS Authentications using secure name/password - form	26160 logins per minute
HTTPS Authorizations	25620 authorized pages per minute
HTTPS Authorization with 10 page requests	81300 authorizations per minute

The following performance numbers are recorded per second to show how the system performs:

Test Scenario	Results
Concurrent Sessions in a 4-node Access Gateway cluster	196258 sessions in cluster (approximately 48000 sessions per server)
Concurrent Sessions in a 4-node Identity Server cluster	193851 sessions in cluster (approximately 48000 sessions per server)
HTTP Public	26170 requests (25057 hits per second)
HTTPS Public	19580 requests (18911 hits per second)
HTTPS Authentications using Name/Password – Basic	512 logins per second
HTTPS Authentications using Secure Name/Password – Basic	502 logins per second
HTTPS Authentications using Name/Password – Form	468 logins per second
HTTPS Authentications using Secure Name/Password – Form	436 logins per second
HTTPS Login with Roles/AGA	427 logins per second
HTTPS Login with Identity Injection	247 logins per second
HTTPS Login with Form Fill	252 logins per second
HTTPS Authorizations	1355 authorized pages per second
AGA is Access Gateway Authorization	

4.3 Access Manager Appliance

The following performance numbers are recorded per minute to show how the system performs:

Test Scenario	Results
HTTPS Public (user accessing single page in a session)	2110800 requests per minute (2022480 hits per minute) and throughput 3003406320 bytes per minute
HTTPS Public (user accessing 10 pages in a session)	1669800 requests per minute (1512780 hits per minute) and throughput 5970431700 bytes per minute
HTTPS Authentications using secure Name/Password - Form	17400 logins per minute
HTTPS Authorizations	18840 authorized pages per minute
HTTPS Authorization with 10 page requests	110940 authorizations per minute

The following performance numbers are recorded per second to show how the system performs:

Test Scenario	Results
Concurrent Sessions in a 4-node Access Gateway cluster	717351 sessions in cluster (approximately 139427sessions per server)
Concurrent Sessions in a 4-node Identity Server cluster	708882 sessions in cluster (approximately 177220 sessions per server)
HTTP Public	29310 requests (28491 hits per second)
HTTPS Public	27830 requests (25213 hits per second)
HTTPS Authentications using Name/Password – Basic	499 logins per second
HTTPS Authentications using Secure Name/Password – Basic	376 logins per second
HTTPS Authentications using Name/Password – Form	301 logins per second
HTTPS Authentications using Secure Name/Password – Form	290 logins per second
HTTPS Login with Roles/AGA	314 logins per second
HTTPS Login with Identity Injection	196 logins per second
HTTPS Login with Form Fill	199 logins per second
HTTPS Authorizations	1849 authorized pages per second
AGA is Access Gateway Authorization	

4.4 Access Gateway Service for Windows

The following performance numbers are recorded per minute to show how the system performs:

Test Scenario	Results
HTTPS Public (user accessing single page in a session)	1,336,800 requests per minute (1,136,820 hits per minute) and throughput 1,686,406,680 bytes per minute
HTTPS Public (user accessing 10 pages in a session)	1,167,000 requests per minute (856,400 hits per minute) and throughput 3,394,894,380 bytes per minute
HTTPS Authentications using secure name/password - form	14580 logins per minute
HTTPS Authorizations	15000 authorized pages per minute
HTTPS Authorization with 10 page requests	82740 authorizations per minute

The following performance numbers are recorded per second to show how the system performs:

Test Scenario	Results
Concurrent Sessions in a 4-node Access Gateway cluster	123439 sessions in cluster (approximately 30860 sessions per server)
Concurrent Sessions in a 4-node Identity Server cluster	120139 sessions in cluster (approximately 30034 sessions per server)
HTTP Public	15770 requests (12961 hits per second)
HTTPS Public	18500 requests (15781 hits per second)
HTTPS Authentications using Name/Password – Basic	324 logins per second
HTTPS Authentications using Secure Name/Password – Basic	300 logins per second
HTTPS Authentications using Name/Password – Form	243 logins per second
HTTPS Authentications using Secure Name/Password – Form	243 logins per second
HTTPS Login with Roles/AGA	250 logins per second
HTTPS Login with Identity Injection	157 logins per second
HTTPS Login with Form Fill	250 logins per second
HTTPS Authorizations	1379 authorized pages per second
AGA is Access Gateway Authorization	

4.5 Scalability

The goal of the scalability tests is to validate the architecture and show the size of clusters/components that were used.

Component	No of Devices/Items
Identity Servers	12
Access Gateway Appliance	18
Linux Access Gateways	8
LDAP Servers	8
Web Servers	101
Policies/Roles	101
Accelerators	51
SSL VPN	500 connections per server
Concurrent users on Access Manager	40000 sessions per Access Gateway

4.6 Reliability

The goal of the reliability tests is to run the system with a high load and allow the test to run for a specified length of time to check if Access Manager can sustain that load and continue to work correctly. The main goal is to demonstrate that the product can process sustained loads for a substantial amount of time.

Linux Access Gateway

- Linux Access Gateway Fourteen Day Reliability Test: Pass
- (60 million authentications)

SSL VPN

- SSL VPN 8 hour Reliability Test: Pass

5 Sizing Guidelines

This section discusses the use case for the following:

- Access Gateway and Identity Server
- SSL VPN, Linux Access Gateway, and Identity Server

5.1 Access Gateway and Identity Server

This use case is based on a user that logs in, requests 30 pages (approximately 1000 hits) during a 30 minute period, and then ends the session. The total number of users is irrelevant in this situation. There can be 1 million or 10,000 users configured in the user stores, but this recommendation is based upon the simultaneous users on the cluster at any one point in time.

Recommendations

When two numbers are listed in a cluster setup, the required number of machines depends upon traffic spikes within the network.

When usage is high on accessing Web servers and applications, more Access Gateways are required. When usage is high on users and authentication, more Identity Servers are required. The setup needs to be evaluated in a real-world usage of the use case.

The following are general recommendations based on a test environment and setup. Each business setup requires some modifications to the recommendations.

Concurrent Users	Cluster Setup
25,000 Users	1-2 Access Gateway, 1-2 Identity Servers 2 are required for fault tolerance/load balancing
50,000 Users	2 Access Gateways, 2 Identity Servers
100,000 Users	4 Access Gateways, 4 Identity Servers

5.2 SSL VPN, Linux Access Gateway, and Identity Server

This use case is based on a user that logs in and performs a series of actions continually to achieve 500 users in eight hours. The system is used to validate the concurrency and to show that they all can work together on the system.

Recommendations

The concurrent users are based on concurrency and the server supports recommendation for a standard user. The results vary because of bandwidth and the applications that pass through the server.

Concurrent Users	Cluster Setup
500 Users	1 SSL VPN Enterprise Mode with High Bandwidth
500 Users	1 SSL VPN Kiosk Mode

6 Conclusion

The testing results confirm that NetIQ Access Manager can be successfully deployed in a high availability environment. The performance of the product has improved a lot compared to the previous version and is capable of handling the Web access management and VPN requirements. The solution provides a fast enterprise level of service for your group and simplifies working with external groups. The product provides superior performance and reliability that simplifies access for remote users.

The results of this test are based on an isolated lab and considered an optimal set of results for NetIQ Access Manager. You can increase the results with changes in hardware, but on similar hardware in real environments you will have different results. You can take this into consideration as you attempt to configure your own cluster. You must also take into account the external items that interact with NetIQ Access Manager

7 Appendix

This appendix discusses:

- Tests with Shared Secrets
- Linux Access Gateway Performance
- SSL VPN Performance

7.1 Tests with Shared Secrets

The objective for this test was to compare the responsiveness of user requests accessing the policies for which shared secrets are configured.

7.1.1 Test Setup

The tests were conducted on Windows Server 2008 R2 and SLES11 SP1 with the configuration as mentioned in the section 2.3.2 *Server Hardware for Access Gateway Service on SLES Tests.*

Test with the Access Gateway Service on Windows 2008 R2 (run with attributes and shared secrets sent at authentication):

- Objective of the test was to simulate a real-life environment where a user accesses 3 different applications.
- The Administration Console is populated with 30000 users each with 5 shared secrets (150,000 shared secrets).
- Test was to access 3 protected resources one after the other each configured with three different form fill policies, which will retrieve 2, 1, and 2 shared secrets respectively.
- Test was done with 50 Load Runner users with users randomly picked from a block of 10000 users.
- Test completed with an average response time of 15 seconds for first application access and 0.5 seconds each for the subsequent two applications.
- Because the shared secrets and attributes are cached in ESP, subsequent requests are faster.

7.1.2 Test with Access Gateway Service on Windows 2008 R2

Run without sending attributes and shared secrets at authentication:

- Objective of the test was to simulate a real-life environment where a user accesses 3 different applications.
- The Administration Console is populated with 30,000 users, each with 5 shared secrets (150,000 shared secrets).
- Test was to access 3 protected resources one after the other, each configured with three different form fill policies, which will retrieve 2, 1, and 2 shared secrets respectively.
- Test was done with 50 Load Runner users with users randomly picked from a block of 10,000 users.
- Test completed with an average response time of 15 seconds for first application access and 6 seconds each for the subsequent two applications***.***

7.1.3 Test with Access Gateway service on SLES11SP1

- Objective of the test was to simulate a real-life environment where a user accesses 3 different applications.
- The Administration Console is populated with 10000 users, each with 5 shared secrets (50,000 shared secrets).
- Test was to access a protected resource configured with a form fill policy, which will retrieve 5 shared secrets.
- Test was done with 50 Load Runner users with users randomly picked from a block of 10,000 users.
- Test completed with an average response time of *11 seconds.*

7.1.4 Summary

- First login with attribute requests takes approximately 10 - 15 seconds depending upon the platform.
- SLES 11 gives slightly better performance compared to Windows.
- If the tests are done keeping the real life use case where a user will access multiple applications or pages in one session, subsequent requests from same application or requests to subsequent applications will take less than a second.

  Note: Attributes need to be sent with authentication to reap the caching benefits.

7.2 Linux Access Gateway Performance

This section describes the Linux Access Gateway performance tuning and test results. These test results are from NetIQ Access Manager 3.1 SP3.

Tomcat Connector Maximum Thread Setting

In /var/opt/novell/tomcat5/conf/server.xml, set maxThreads="500" for the port 8080 connector.

This parameter enables the Linux Access Gateway ESP to handle more threads simultaneously to improve the performance. The thread number must be fine-tuned for every customer environment based on the number of attributes attached to a user session. When the user sessions are holding large number of attributes, each user session requires more heap memory. The available stack memory reduces as a result. If number of threads configured in this scenario is high, Tomcat will try to spawn more threads and fails due to non-availability of the stack memory. Customer must fine-tune the number of threads based on the attribute usage.

7.2.1 Java Memory Allocations

The Tomcat configuration file controls the amount of memory that Tomcat can allocate for Java.

- If you have installed the Access Gateway on a machine with the minimum 4 GB of memory, you can modify two parameters in this file to improve performance under heavy load:
  In /var/opt/novell/tomcat5/conf/tomcat5.conf, set the following parameters:

  Replace the -Xmx value (default is 1024) with 1800.
  JAVA_OPTS="${JAVA_OPTS} server -Xmx1800m -Xms1024m -Xss128k -XX:+UseConcMarkSweepGC"

- Change the -Dnids.freemem.threshold value from 0 to a value between 5 and 15. This parameter prevents user sessions from using up all memory and ensures that there is free memory available so that the other internal Java processes can run. When this threshold is reached, the user receives a 503 server busy message and a threshold error message is logged to the catalina.out file.

  JAVA_OPTS="${JAVA_OPTS} -Dnids.freemem.threshold=10"

7.2.2 Linux Access Gateway Test Result

The performance testing for the Identity Server was done in conjunction with the Access Gateway. Because users interact with the Identity Server when requesting access to an Access Gateway resource, the login authentication performance is more accurately tested from the Access Gateway rather than directly to the Identity Server.

These performance numbers are recorded in minute to show how the project performs:

Test Scenario	Results
HTTPS Public	298,320 requests per minute (461,040 hits per minute) and throughput 1,666,706,760 bytes per minute
HTTPS Authentications	13440 logins per minute
HTTPS Authorizations	12660 authorized pages per minute
HTTPS Login with 10 page requests	10860 logins (108660 Authorizations) per minute

These performance numbers are recorded in second to show how the system performs:

Test Scenario	Results
Concurrent Users per Cluster	4 servers with 16,000 users each (67,200 users per cluster)
HTTPS Public	4972 requests (7684 hits per second)
HTTPS Authentications	224 logins per second
HTTPS Authorizations	211 authorized pages per second
HTTPS Login with Identity Injection	130 logins per second
HTTPS Login with Form Fill	144 logins per second
HTTPS Login with Roles/AGA	165 logins per second
HTTPS Login with 10 page requests	181 logins (1810 authorizations) per second
AGA is Access Gateway Authorization	

7.3 SSL VPN

These test results are from NetIQ Access Manager 3.1.3.

7.3.1 Server Hardware for SSL VPN Tests

The SSL VPN servers were run with the following hardware:

- 1 SSL VPN server (Clone: Dual CPU Xeon 3.0 GHz, 4 GB RAM)

The SSL VPN clients run from this hardware to provide the connection information:

- 500 clients ranging from 2 GHz to 3.2 GHz and 1 to 2GB of RAM

7.3.2 Enterprise Server Performance

The test achieved 500 concurrent SSL VPN connections in the Kiosk mode, using a single high bandwidth SSL VPN server. The SSL VPN connections are initiated from multiple Windows XP and SLED clients. The test was run from the clients over an eight-hour period.

Enterprise Server Performance: Duration	Connections	Throughput
8 hours	500	15 MB/sec average

7.3.3 High Bandwidth Kiosk Mode

The test achieved 500 concurrent SSL VPN connections in the Kiosk mode, using a single high bandwidth SSL VPN server. The SSL VPN connections are initiated from multiple Windows XP and SLED clients. The test was run from the clients over an eight-hour period.

Kiosk Server Performance:

Duration	Connections	Throughput
8 hours	500	26 MB/sec average

NetIQ® Access Manager 3.2
License Agreement

PLEASE READ THIS AGREEMENT CAREFULLY. BY INSTALLING, DOWNLOADING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE WITH THESE TERMS, DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE AND, IF APPLICABLE, RETURN THE ENTIRE UNUSED PACKAGE TO THE RESELLER WITH YOUR RECEIPT FOR A REFUND. THE SOFTWARE MAY NOT BE SOLD, TRANSFERRED, OR FURTHER DISTRIBUTED EXCEPT AS AUTHORIZED BY NETIQ.

This NetIQ License Agreement (“Agreement”) is a legal agreement between You (an entity or a person) and NetIQ Corporation or an affiliate (“NetIQ”). The software product identified in the title of this Agreement for which You have acquired licenses, any media and accompanying documentation (collectively the “Software”) is protected by the copyright laws and treaties of the United States (“U.S.”) and other countries and is subject to the terms of this Agreement. Any update or support release to the Software that You may download or receive that is not accompanied by a license agreement expressly superseding this Agreement is Software and governed by this Agreement. If the Software is an update or support release, then You must have validly licensed the version and quantity of the Software being updated or supported in order to install or use the update or support release.
The Software may include or be bundled with other software programs licensed under different terms and/or licensed by a licensor other than NetIQ. Use of any software programs accompanied by a separate license agreement is governed by that separate license agreement. Any third party software that may be provided with the Software is included for use at Your option.

GRANT. Subject to your acceptance of and compliance with this Agreement, timely payment of required payments, and your adherence to the license restrictions set forth herein, in the Documentation accompanying the Software and in the Order Documentation (the “License Restrictions”), NetIQ hereby grants to You as licensee, a nonexclusive, nontransferable license, without right of sublicense, to use the software, together with any adapters, modules, updates and modifications to the foregoing, if any, provided to You by NetIQ subject to the License Restrictions (collectively "Software"). The Software is licensed solely in object code format and solely for Your internal business use. For purposes hereof, Order Documentation "Order Documentation” means the software license schedule, purchase order, purchase letter or other similar document provided by NetIQ by which You place an order for the Software.

LICENSED USE

Commercial Software

"Instance" means the initial copy of the Software necessary for execution of the Software and each additional copy (or partial copy) of the Software stored or loaded in memory or virtual memory.

"User" means a user object in a single directory tree (or other class of object that contains data representing a person, such as objects containing credit card information or PIN numbers) that has (a) access or use rights to any portion of the Software, or (b) access or use rights to products (devices, hardware, or software) being managed by the Software, regardless of whether the user object is assigned to a person or device. User objects (or other classes of objects) representing the same person that are linked to each other within a single tree and/or linked across multiple trees count as only one User.

"Access Gateway Software" means the gateway software that performs access management services to protected web applications, including role based authorization, web single sign-on and data encryption.

"Identity Server" means the server software that performs authentication, federation, role definition and policy distribution.

"SSLVPN" means the server software that performs access management services to protected enterprise applications, including role based authorization and client integrity checking.
The following licenses apply to Your use of the Software depending on whether You have purchased licenses to the Software under a User license model or an Instance license model. If You have received the Software as an entitlement under upgrade protection You purchased for the Novell iChain product, then You are licensed to use the Software under the User Model specified below in a quantity equivalent to the number of Your Novell iChain user licenses covered by the applicable upgrade protection. For evaluation rights, please see the Evaluation Software paragraph below.

User Model. You must acquire a user license for each User. Each person who accesses or uses the Software must have at least one user object uniquely assigned to that person and access the Software through the user object.

Instance Model. The Access Gateway component of the Software and the Identity Server component of the Software are licensed separately. Use of each requires purchase of the applicable quantity of Access Manager instance licenses.

> **Access Gateway**. You must acquire an Access Manager instance license for each Instance of the Access Gateway Software. You may install and use one Instance of the SSLVPN for each Instance of the Access Gateway Software You have licensed.
>
> **Identity Server**. You must acquire an Access Manager instance license for each Instance of the Identity Server Software.
>
> **NetIQ Access Manager Appliance**. If You deploy the Software as an appliance, then You will have installed an Instance of the Access Gateway Software as well as an Instance of the Identify Server Software. Consequently, You must acquire two (2) Access Manager Instance licenses for each appliance.

SLES® Appliance License. If the Software is deployed as an appliance and includes the SUSE® Linux Enterprise Server product (SLES), then You are subject to the following restriction with respect to use of SLES. Notwithstanding the license rights in the license agreement accompanying the copy of SLES You received with the Software, You agree to use. SLES solely for the purpose of running the Access Manager Software. SLES includes components that are open source packages accompanied by separate license terms. Your license rights with respect to individual components accompanied by separate license terms are defined by those terms; nothing in this Agreement shall restrict, limit, or otherwise affect any rights or obligations You may have, or conditions to which You may be subject, under such license terms.

eDirectory™ Software License. The quantity of licenses for the eDirectory software included with Your lawfully acquired user licenses of the Access Manager Software is equal to the greater of (1) the quantity of User licenses You have lawfully acquired for the Access Manager Software, or (2) 250,000 Users per company/entity. If You have licensed the Software on an Instance model, then You may use an equivalent number of Instance licenses of the eDirectory software, but Your use of eDirectory software is limited to use only with the Software. The foregoing eDirectory licenses are not upgradeable and are otherwise subject to the license agreement accompanying the eDirectory software.

Audit Software License. Your use of the Audit Software included with Access Manager is limited to use solely in connection with Access Manager. Any other use of the Audit Software requires the purchase of the applicable Audit Software licenses.

Staging Software License

Provided that You are in compliance with the terms of this Agreement, You are authorized to use the Software in Your internal, non-production environment solely for testing purposes in a quantity equal to that of Your Instance or User commercial licenses.

Evaluation Software

In the event that the Software is licensed only for Evaluation Use, the terms of this paragraph shall apply. Your license to use the Software commences on installation of the Software and, unless you and NetIQ agree to a different period, will terminate after a period of 30 days (the “Evaluation Period”). You may use the Software in a non-production environment during the Evaluation Period. At the end of the Evaluation Period, your license to use the Evaluation version of the Software is automatically terminated. You may not extend the time limits of the Software in any manner. At the end of the Evaluation Period You agree to de-install the Software and if required by NetIQ, return all copies or partial copies of the Software or certify to NetIQ that all copies or partial copies of the Software have been deleted from Your computer libraries and/or storage devices and have been destroyed. If You desire to continue Your use of the Software beyond the Evaluation Period, You must contact NetIQ to acquire a license to the Software for the applicable fee. The Software may contain an automatic disabling mechanism that prevents its use after a certain period of time, so You should back up Your system and take other measures to prevent any loss of files or data.

EVALUATION SOFTWARE IS PROVIDED ON AN “AS IS” BASIS, WITHOUT WARRANTIES OR REPRESENTATIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR REPRESENTATIONS OF TITLE OR NON-INFRINGEMENT.

RESTRICTIONS

License Restrictions. NetIQ reserves all rights not expressly granted to You. You may not (1) reverse engineer, decompile, or disassemble the Software except and only to the extent it is expressly permitted by applicable law; (2) modify, alter, rent, timeshare host or lease the Software or sublicense any of Your rights under this Agreement; (3) transfer the Software or Your license rights under this Agreement, in whole or in part, without written permission by NetIQ; (4) copy the Software (except for back-up purposes); (5) remove any patent, trademark, copyright, trade secret or other proprietary notices or labels on the Software or documentation; (6) you may not transfer, lease, assign, sublicense, pledge, rent, share or distribute the Software or make it available for timesharing, service bureau or on-line use, unless previously agreed to in writing by NetIQ; and (7) you may not disclose the results of any performance, functional or other evaluation or benchmarking of the Software to any third party without the prior written permission of NetIQ.

Suite Licenses. If Your license to use the Software is for a suite of products, then for each license only one user may use the products in the suite. The suite license does not allow use of individual products in the suite by multiple users if licensed on a user basis or multiple devices if licensed on a device or server basis.

Upgrade Protection. If You purchased upgrade protection or maintenance under a NetIQ program for this Software, the upgrade protection or maintenance only entitles You to upgrades of the Software as a whole and does not entitle You to upgrades of any component programs or products bundled with the Software or any individual products included in a suite if the Software is licensed as a suite of products. You may separately purchase upgrade protection for individual components of the Software if permitted by the applicable NetIQ policies and programs.
Upgrade Software. This section applies to You if You have purchased the Software based upon upgrade pricing. “Original Product” means the product from which You are upgrading. You are authorized to use the Software only if You are the authorized user of the Original Product and You meet the following conditions: (1) You have acquired the right to use the Software solely to replace the Original Product that You acquired legally and that is qualified to be upgraded with the Software under the NetIQ policies existing at the time You acquired the Software; (2) You installed and used the Original Product in accordance with the terms and conditions of the applicable license agreement; and (3) You will not sell or otherwise transfer possession of the Original Product.

Support. NetIQ has no obligation to provide support unless You purchase an offering that expressly includes support services. If You make such a purchase and no separate agreement specifically applies to the support services, then the terms of this Agreement will govern the provision of such support services (“Services”). For more information on NetIQ's current support offerings, see http://netiq.com/support/process.asp

OWNERSHIP

No title to or ownership of the Software is transferred to You. NetIQ and/or its licensors retain all right, title and interest in and to all intellectual property rights in the Software and Services, including any adaptations or copies thereof. You acquire only a conditional license to use the Software.

LIMITED WARRANTY

For ninety (90) days from Your date of purchase, NetIQ warrants that any media on which the Software is delivered is free from physical defects. If the defective items are returned to NetIQ within ninety (90) days from the date of purchase, NetIQ will at its sole discretion either resolve the nonconformity or refund the license fees You paid for the Software. Any unauthorized use or modification to the Software voids this warranty. THE FOREGOING WARRANTY IS YOUR SOLE AND EXCLUSIVE REMEDY AND IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED. (The foregoing warranty does not apply to Software provided free of charge. SUCH SOFTWARE IS PROVIDED “AS IS” WITHOUT ANY WARRANTIES OF ANY KIND.)

THE SOFTWARE IS NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR DISTRIBUTION WITH ON-LINE CONTROL EQUIPMENT IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION, COMMUNICATION, OR CONTROL SYSTEMS, DIRECT LIFE SUPPORT MACHINES, WEAPONS SYSTEMS, OR OTHER USES IN WHICH FAILURE OF THE SOFTWARE COULD LEAD DIRECTLY TO DEATH, PERSONAL INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE.

THE SOFTWARE IS ONLY COMPATIBLE WITH CERTAIN COMPUTERS AND OPERATING SYSTEMS. THE SOFTWARE IS NOT WARRANTED FOR NON-COMPATIBLE SYSTEMS. Call NetIQ or Your reseller for information about compatibility.

Non-NetIQ Products. The Software may include or be bundled with hardware or other software programs or services licensed or sold by an entity other than NetIQ. NETIQ DOES NOT WARRANT NON-NETIQ PRODUCTS OR SERVICES. ANY SUCH PRODUCTS OR SERVICES ARE PROVIDED ON AN “AS IS” BASIS. WARRANTY SERVICE IF ANY FOR NON-NETIQ PRODUCTS IS PROVIDED BY THE PRODUCT LICENSOR IN ACCORDANCE WITH THE APPLICABLE LICENSOR WARRANTY.

EXCEPT AS OTHERWISE RESTRICTED BY LAW, NETIQ DISCLAIMS AND EXCLUDES ANY AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT. NETIQ MAKES NO WARRANTY, REPRESENTATION OR PROMISE NOT EXPRESSLY SET FORTH IN THIS LIMITED WARRANTY. NETIQ DOES NOT WARRANT THAT THE SOFTWARE OR SERVICES WILL SATISFY YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE OR SERVICES WILL BE UNINTERRUPTED. Some jurisdictions do not allow certain disclaimers and limitations of warranties, so portions of the above limitations may not apply to You. This limited warranty gives You specific rights and You may also have other rights which vary by state or jurisdiction.

LIMITATION OF LIABILITY

Consequential Losses. NEITHER NETIQ NOR ANY OF ITS LICENSORS, SUBSIDIARIES, OR EMPLOYEES WILL IN ANY CASE BE LIABLE FOR ANY SPECIAL, INCIDENTAL,

CONSEQUENTIAL, INDIRECT, TORT, ECONOMIC OR PUNITIVE DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR SERVICES, INCLUDING WITHOUT LIMITATION LOSS OF PROFITS, BUSINESS OR DATA, EVEN IF ADVISED OF THE POSSIBILITY OF THOSE DAMAGES.
Direct Damages. IN NO EVENT WILL NETIQ'S OR ITS LICENSOR(S)' AGGREGATE LIABILITY FOR DIRECT DAMAGES TO PROPERTY OR PERSON (WHETHER IN ONE INSTANCE OR A SERIES OF INSTANCES) EXCEED 1.25 TIMES THE AMOUNT PAID BY YOU FOR THE SOFTWARE OR SERVICES OUT OF WHICH SUCH CLAIM AROSE (OR $50 (U.S.) IF YOU RECEIVED THE SOFTWARE FREE OF CHARGE). The above exclusions and limitations will not apply to claims relating to death or personal injury. In those jurisdictions that do not allow the exclusion or limitation of damages, NetIQ's and its Licensors' liability shall be limited or excluded to the maximum extent allowed within those jurisdictions.

GENERAL TERMS

Term. This Agreement becomes effective on the date You legally acquire the Software and will automatically terminate if You breach any of its terms. If the Software is provided to You on a subscription basis, then Your right to possess or use the Software will terminate at the end of the applicable subscription period. Upon termination of this Agreement or any applicable subscription period, You must destroy the original and all copies of the Software or return them to NetIQ and delete the Software from Your systems.

Verification; Audit Rights. NetIQ may, upon fifteen (15) days' advance notice and at its expense, conduct an annual audit, during your normal business hours, of your use of the Software and Documentation to verify compliance with this Agreement. You agree to implement internal safeguards to prevent any unauthorized copying, distribution, installation, or use of, or access to, the Software. You further agree to keep records sufficient to certify your compliance with this Agreement (including its License Restrictions), and, upon request of NetIQ, provide and certify metrics and/or reports based upon such records and accounting both numbers of copies (by product and version) and network architectures as they may reasonably relate to your licensing and deployment of the Software. You shall provide NetIQ or an authorized representative with access to records, hardware and employees in order to perform the audit. Upon NetIQ's or its authorized representative's presentation of their reasonable written commitment(s) to safeguard your confidential information, you shall fully cooperate with such audit and provide any necessary assistance and access to records and computers. If an audit reveals that you have or at any time have had unlicensed installation, use of, or access to the Software, You will promptly acquire sufficient licenses to cover any shortage. If a material license shortage of 5% or more is found, you must reimburse NetIQ for the costs incurred in the audit and acquire the necessary additional licenses within 30 days without the benefit of any otherwise applicable discount.

Benchmark Testing. This benchmark testing restriction applies to You if You are a software developer or licensor or if You are performing testing on the Software at the direction of or on behalf of a software developer or licensor. You may not, without NetIQ's prior written consent not to be unreasonably withheld, publish or disclose to any third party the results of any benchmark test of the Software.

Open Source. The software may contain or be distributed with third party software covered by an open source software license ("Open Source Software") or other third party software ("Third Party Software") covered by a different license. If Open Source Software is included the terms and conditions of this license do not apply to the Open Source Software. If Third Party Software is included the terms and conditions of this license may not apply to Third Party Software. Information concerning the inclusion of the Open Source Software and Third Party Software not covered by this license, if any, and the notices, license terms and disclaimers applicable to such software is contained in the About Box and/or ThirdPartySoftware.txt file or available upon request from NetIQ. Nothing in this Agreement shall restrict, limit or otherwise affect any rights or obligations You may have, or conditions to which

You may be subject, under any applicable open source licenses to any open source code contained in the Software.

Transfer. This Agreement may not be transferred or assigned without the prior written approval of NetIQ.

Law and Jurisdiction. This Agreement is governed by the laws of the State of Texas, U.S. Any action at law relating to this Agreement may only be brought before the courts of competent jurisdiction of the State of Texas. If, however, Your country of principal residence is a member state of the European Union or the European Free Trade Association, this Agreement is governed by the laws of that country, and any action at law may only be brought before a court of competent jurisdiction of that country.

Entire Agreement. This Agreement, together with any Order Documentation, sets forth the entire understanding and agreement between You and NetIQ and may be amended or modified only by a written agreement agreed to by You and an authorized representative of NetIQ. NO LICENSOR, DISTRIBUTOR, DEALER, RETAILER, RESELLER, SALES PERSON, OR EMPLOYEE IS AUTHORIZED TO MODIFY THIS AGREEMENT OR TO MAKE ANY REPRESENTATION OR PROMISE THAT IS DIFFERENT FROM, OR IN ADDITION TO, THE TERMS OF THIS AGREEMENT.

Waiver. No waiver of any right under this Agreement will be effective unless in writing, signed by a duly authorized representative of the party to be bound. No waiver of any past or present right arising from any breach or failure to perform will be deemed to be a waiver of any future right arising under this Agreement.

Severability. If any provision in this Agreement is invalid or unenforceable, that provision will be construed, limited, modified or, if necessary, severed, to the extent necessary, to eliminate its invalidity or unenforceability, and the other provisions of this Agreement will remain unaffected.

Export Compliance. Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. The parties agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. The parties agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. The parties will not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. Please consult the Bureau of Industry and Security web page www.bis.doc.gov before exporting NetIQ products from the U.S. Upon request, NetIQ will provide You specific information regarding applicable restrictions. However, NetIQ assumes no responsibility for Your failure to obtain any necessary export approvals and you agree to indemnify and hold harmless NetIQ from any claims or damages arising from your noncompliance with U.S. export laws.

U.S. Government Restricted Rights. Use, duplication, or disclosure by the U.S. Government is subject to the restrictions in FAR 52.227-14 (June 1987) Alternate III (June 1987), FAR 52.227-19 (June 1987), or DFARS 252.227-7013 (b) (3) (Nov 1995), or applicable successor clauses. Contractor/Manufacturer is NetIQ Corporation, 1233 West Loop South, Houston, TX 77027.
Other. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded.

Communication. By registering or downloading this product, you make the registered e-mail address available to receive information about NetIQ Corporation and our products. To remove yourself from this mailing list, please visit: http://www.netiq.com/Account/lists.asp

Payment. You are responsible for making full and timely payment for the Software license. You shall pay all of NetIQ’s reasonable fees, costs and expenses (including reasonable attorneys’ fees) if legal action is required to collect outstanding balances.

Force Majeure. NetIQ and its suppliers shall not be liable in any respect for failures to perform hereunder due wholly or substantially to the elements, acts of God, labor disputes, acts of terrorism, acts of civil or military authority, fires, floods, epidemics, quarantine restrictions, armed hostilities, riots and other unavoidable events beyond the control of NetIQ or its suppliers, and the time for performance of obligations hereunder by NetIQ or its suppliers subject to such event shall be extended for the duration of such event.