NetIQ Access Manager 4.1

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	31-07-2015	Updated the document with the inputs received from field.
1.3	14-07-2015	Added Test results for Access Gateway Services for Windows
1.2	30-06-2015	Added Test results for Access Manager Appliance
1.1	17-06-2015	Added Test results for Access Gateway Services for SLES12
1.0	02-06-2015	Initial document for Access Manager 4.1 performance test results of Access Gateway Appliance.

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 Access Manager to help you deploy the correct configuration in your environment. The test results are artificial and may differ depending on environments. However, the data should help in determining the design of your system. This document refers to the 4.1 release of Access Manager shipped in March 2015.

1.1 Key Features of NetIQ Access Manager

The following are the key features of Access Manager:

- Basic and advanced authentication methods
- Federation-based architecture
- Single sign-on to all web-based applications
- Corporate policies for required software remote users
- Roles-based access control for web-based and enterprise applications
- 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 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 four Identity Servers and four Access Gateways. The number of users and the amount of traffic determine the size of the cluster.

2.1 Access Gateway

Performance Testing:

It includes the following tasks (or setup or scenarios):???

- 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 2 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 Test Setup

- This Section includes:
- Server Hardware for Access Gateway Appliance Tests
- Server Hardware for Access Gateway Service on SLES Tests
- Client Hardware
- Load Balancers
- Configuration Details
- Performance/Reliability/Stress Tools
-

2.2.1 Server Hardware for Access Gateway Appliance Tests

The Access Gateway clustered tests are run on virtualized environment setup on the following servers:

- Dell PowerEdge R730xd running ESXi 5.5
- Dell PowerEdge R720xd running ESXi 5.5
- Dell PowerEdge R710 running ESXi 5.5
- Dell PowerEdge R710 running ESXi 3.5

The Virtual Machine design is as follows:

Server Components	Operating System	Hardware
• Administration Console (2 nodes)	• SLES11 SP3	• CPU: 2 x 3 GHz • Memory : 4GB
• Identity Servers (4 nodes)	• SLES11 SP3	• CPU: 4 x 3 GHz • Memory : 16GB
• Access Gateway Appliance (4 nodes)	• SLES11 SP3	• CPU: 4 x 2.6 GHz

Server Components	Operating System	Hardware
		• Memory : 16GB
• External eDirectory user store (3 nodes)	• SLES11 SP1	• CPU: 2 x 3 GHz • Memory : 4GB
• Apache2 Web Server (3 nodes)	• SLES11 SP1	• CPU: 2 x 3 GHz • Memory : 4GB

2.2.2 Server Hardware for Access Gateway Service on SLES12 Tests

The Access Gateway clustered tests are run on virtualized environment setup on the following servers:

- Dell PowerEdge R730xd running ESXi 5.5
- Dell PowerEdge R720xd running ESXi 5.5
- Dell PowerEdge R710 running ESXi 5.5
- Dell PowerEdge R710 running ESXi 3.5

The Virtual Machine design is as follows:

Server Components	Operating System	Hardware
• Administration Console (2 nodes)	• SLES 12	• CPU: 2 x 3 GHz • Memory : 4GB
• Identity Servers (4 nodes)	• SLES12 •	• CPU: 4 x 3 GHz • Memory : 16GB

Server Components	Operating System	Hardware
• Access Gateway Service (4 nodes)	• SLES12	• CPU: 4 x 2.6 GHz • Memory : 16GB
• External eDirectory user store (3 nodes)	• SLES11 SP1	• CPU: 2 x 3 GHz • Memory : 4GB
• Apache2 Web Server (3 nodes)	• SLES11 SP1	• CPU: 2 x 3 GHz • Memory : 4GB

Note: In the performance testing, Access Gateways were installed on SLES12 servers with BTRFS as a file system. Whereas the Identity servers were installed on SLES12 with EXT3 as file system (upgraded from SLES11 SP3 to SLES12)

2.2.3 Server Hardware for Access Manager Appliance Tests

The Access Gateway clustered tests are run on virtualized environment setup on the following servers:

- Dell PowerEdge R730xd running ESXi 5.5
- Dell PowerEdge R720xd running ESXi 5.5
- Dell PowerEdge R710 running ESXi 5.5
- Dell PowerEdge R710 running ESXi 3.5

The Virtual Machine design is as follows:

Server Components	Operating System	Hardware
• Access Manager Appliance (4 nodes)	• SLES11 SP3	• CPU: 8 x 3 GHz • Memory : 32GB
• External eDirectory user store (3 nodes)	• SLES11 SP1	• CPU: 2 x 3 GHz • Memory : 4GB
• Apache2 Web Server (3 nodes)	• SLES11 SP1	• CPU: 2 x 3 GHz • Memory : 4GB

2.2.4 Server Hardware for Access Gateway Service on Windows Tests

The Access Gateway clustered tests are run on virtualized environment setup on the following servers:

- Dell PowerEdge R730xd running ESXi 5.5
- Dell PowerEdge R720xd running ESXi 5.5
- Dell PowerEdge R710 running ESXi 5.5
- Dell PowerEdge R710 running ESXi 3.5

The Virtual Machine design is as follows:

Server Components	Operating System	Hardware
• Administration Console (2 nodes)	• Windows Server 2012 R2 Standard	• CPU: 2 x 3 GHz • Memory : 4GB
• Identity Servers (4 nodes)	• Windows Server 2012 R2 Standard	• CPU: 4 x 3 GHz • Memory : 16GB
• Access Gateway Service (4 nodes)	• Windows Server 2012 R2 Standard	• CPU: 4 x 2.6 GHz • Memory : 16GB
• External eDirectory user store (3 nodes)	• SLES11 SP1	• CPU: 2 x 3 GHz • Memory : 4GB
• Apache2 Web Server (3 nodes)	• SLES11 SP1	• CPU: 2 x 3 GHz • Memory : 4GB

2.2.5 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)

2.2.6 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 200B with one hyperlink in it. These tests focus on the authentication, authorization, identity injection, and form fill performance rather than the page rendering performance.
- Access Manager user stores configurations 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, performance will decrease. The primary user store used in the tests was eDirectory 8.8.6.

2.2.7 Performance/Reliability/Stress Tools

The HP Mercury LoadRunner tool is used for the Identity Server and Access Gateway testing because it correctly replicates large IP ranges between multiple clients in a clustered environment. This allowed the tests to more closely simulate real-world environments with real browser interaction with 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 so that you do not use the same user for every connection.

2.3 Other Factors Influencing Performance Information

We have provided description of the hardware and of the test configuration. However, other factors in a network also affect overall performance. These include the following factors:

Customized Login Pages: Login and landing pages play an important role in the overall user experience while accessing the resources protected by Access Manager. You should consider the performance aspect of the page loading and rendering while developing the custom login JSP pages.

- **L4 Switches:** If the switch is slow or misconfigured, it can severely affect 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 Performance 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 one second. The public requests can vary widely based upon size of the page, caching settings, and content.

- **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 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 consider this while planning for capacity testing on a cluster.
  Configuring the session timeout for a resource is 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 a short duration and leave the session idle after accessing few pages, configuring short 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 duration, 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.

3 Tuning Parameters

The following parameters were tuned during the performance 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 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/idp/conf/tomcat.conf, set the following parameters:

  Replace the Xms and Xmx values to 2048:

  JAVA_OPTS="-server -Xms2048m -Xmx2048m –Xss256k "

  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.

- 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"

- **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 enables the Identity Server to make connections to the LDAP user store up to 600.

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

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 Appliances 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/tomcat.conf, set the following parameters:

  Replace the Xms and Xmx values to 2048:

  JAVA_OPTS="-server -Xms2048m -Xmx2048m –Xss256k "

  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.

  In the performance tests, ESP Tomcat was set to 12288 for both Xms and Xmx.

- 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 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.

Access Gateway Appliance Advanced Options

Add a new advanced option as follows:

NAGGlobalOptions ESP_Busy_Threshold=5000

Apache MPM settings

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

<IfModule mpm_worker_module>

ThreadLimit 300

StartServers 3

MaxClients 3000

MinSpareThreads 3000

MaxSpareThreads 3000

ThreadsPerChild 300

ServerLimit 10

MaxRequestsPerChild 0

</IfModule>

This configuration is for the appliance machine, which has the minimum 4GB memory available. If the appliance machine has more memory than 6GB, set the mpm_worker_module to match the following configuration.

The performance tests were conducted with the following configuration when the appliance machine has 16 GB memory available:

<IfModule mpm_worker_module>

ThreadLimit 1000

StartServers 9

ServerLimit 10

MaxClients 9000

MinSpareThreads 9000

MaxSpareThreads 9000

ThreadsPerChild 1000

MaxRequestsPerChild 0

</IfModule>

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 Test 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.

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)	1700K requests per minute with a throughput of 2000 Megabits per minute
HTTPS Public (user accessing 10 pages in a session)	1400K requests per minute with a throughput of 5000 Megabits per minute
HTTPS Authentications using secure name/password - form	42K logins per minute

Test Scenario	Results
HTTPS Authorizations	30K authorized pages per minute
HTTPS Authorization with 10 page requests	150K authorizations per minute

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

Test Scenario	Results
Concurrent Sessions in 4-node AG Cluster	240K sessions in cluster (approximately 60K sessions per server)
Concurrent Sessions in 4-node IDP Cluster	240K sessions in cluster (approximately 60K sessions per server)
HTTP Public	35K requests per second
HTTPS Public	28K requests per second
HTTPS Authentications using Name/Password – Basic	700 logins per second
HTTPS Authentications using Secure Name/Password – Basic	700 logins per second
HTTPS Authentications using Name/Password – Form	700 logins per second
HTTPS Authentications using Secure Name/Password – Form	700 logins per second
HTTPS Login with Roles/AGA	500 logins per second
HTTPS Login with Identity Injection	425 logins per second
HTTPS Login with Form Fill	350 logins per second
HTTPS Authorizations with 10 page requests	2500 authorized pages per second
AGA is Access Gateway Authorization	

4.2 Access Gateway Service on SLES12

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)	2600K requests per minute with a throughput of 2700 Megabits per minute

Test Scenario	Results
HTTPS Public (user accessing 10 pages in a session)	1600K requests per minute with a throughput of 6200 Megabits per minute
HTTPS Authentications using secure name/password - form	39K logins per minute
HTTPS Authorizations	30K authorized pages per minute
HTTPS Authorization with 10 page requests	150K authorizations per minute

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

Test Scenario	Results
Concurrent Sessions in 4-node AG Cluster	260K sessions in cluster (approximately 65K sessions per server)
Concurrent Sessions in 4-node IDP Cluster	280K sessions in cluster (approximately 70K sessions per server)
HTTP Public	37K requests per second
HTTPS Public	43K requests per second
HTTPS Authentications using Name/Password – Basic	700 logins per second
HTTPS Authentications using Secure Name/Password – Basic	650 logins per second
HTTPS Authentications using Name/Password – Form	650 logins per second
HTTPS Authentications using Secure Name/Password – Form	650 logins per second
HTTPS Login with Roles/AGA	500 logins per second
HTTPS Login with Identity Injection	400 logins per second
HTTPS Login with Form Fill	450 logins per second
HTTPS Authorizations with 10 page request	2500 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)	2808K requests per minute with a throughput of 3000 Megabits per minute
HTTPS Public (user accessing 10 pages in a session)	1800K requests per minute with a throughput of 6600 Megabits per minute
HTTPS Authentications using secure name/password - form	33K logins per minute
HTTPS Authorizations	24K authorized pages per minute
HTTPS Authorization with 10 page requests	168K authorizations per minute

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

Test Scenario	Results
Concurrent Sessions in 4-node AG Cluster	560K sessions in cluster (approximately 140K sessions per server)
Concurrent Sessions in 4-node IDP Cluster	720K sessions in cluster (approximately 180K sessions per server)
HTTP Public	48K requests per second
HTTPS Public	47K requests per second
HTTPS Authentications using Name/Password – Basic	650 logins per second
HTTPS Authentications using Secure Name/Password – Basic	660 logins per second
HTTPS Authentications using Name/Password – Form	550 logins per second
HTTPS Authentications using Secure Name/Password – Form	560 logins per second
HTTPS Login with Roles/AGA	400 logins per second
HTTPS Login with Identity Injection	300 logins per second
HTTPS Login with Form Fill	290 logins per second
HTTPS Authorizations with 10 page request	2800 authorized pages per second

Test Scenario	Results
AGA is Access Gateway Authorization	

4.4 Access Gateway Service on 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)	1700K requests per minute with a throughput of 1800 Megabits per minute
HTTPS Public (user accessing 10 pages in a session)	1340K requests per minute with a throughput of 5000 Megabits per minute
HTTPS Authentications using secure name/password - form	28K logins per minute
HTTPS Authorizations	27K authorized pages per minute
HTTPS Authorization with 10 page requests	114K authorizations per minute

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

Test Scenario	Results
Concurrent Sessions in 4-node AG Cluster	160K sessions in cluster (approximately 40K sessions per server)
Concurrent Sessions in 4-node IDP Cluster	400K sessions in cluster (approximately 100K sessions per server)
HTTP Public	27K requests per second
HTTPS Public	28K requests per second
HTTPS Authentications using Name/Password – Basic	530 logins per second
HTTPS Authentications using Secure Name/Password – Basic	520 logins per second
HTTPS Authentications using Name/Password – Form	470 logins per second
HTTPS Authentications using Secure Name/Password – Form	460 logins per second
HTTPS Login with Roles/AGA	450 logins per second
HTTPS Login with Identity Injection	380 logins per second

Test Scenario	Results
HTTPS Login with Form Fill	450 logins per second
HTTPS Authorizations with 10 page requests	1900 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	Number 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
Concurrent Users on Access Manager	40000 sessions per Access Gateway

5 Sizing Guidelines

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 duration, and then ends the session. This is the basis for the recommendations and how the system will be used. 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 point of 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 in the recommendations.

Concurrent Users	Cluster Setup
25000 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

6 Conclusion

The testing results confirm that the NetIQ Access Manager product can be successfully deployed in a high availability environment. The performance of the product has improved a lot compared to the previous version and it 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 consider this as you attempt to configure your own cluster. You must also consider the external items that interact with NetIQ Access Manager.