

Novell Access Manager 3.0

Novell System Test Report

Performance, Reliability, and Scalability Testing

Disclaimer	<p>Novell, Inc. makes no representations or warranties with respect to the contents or use of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.</p>	
Trademarks	<p>Novell is a registered trademark of Novell, Inc. in the United States and other countries.</p> <p>* All third-party trademarks are property of their respective owner.</p>	
	<p>Copyright 2008 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of Novell, Inc.</p>	
	<p>Novell, Inc. 1800 South Novell Place Provo, UT 84606 USA</p>	<p>Novell UK Limited Novell House 1 Arlington Square Downshire Way Bracknell Berkshire RG12 1WA</p>
Prepared By	<p>Novell System Test Provo/Bangalore</p>	
	<p>Novell Access Manager - White Paper June 2008</p>	

Contents

The Focus of System Testing.....	4
Access Manager 3.0 Test Plan	5
Components	5
Final Test Plan.....	5
Server Hardware	7
Details of Configuration.....	8
Performance/Reliability/Stress Tools.....	8
Test Results.....	10
Identity Server.....	10
Linux Access Gateway.....	10
SSL VPN in HB Enterprise Mode.....	11
SSL VPN in HB Kiosk Mode.....	11
User Stores.....	11
Scalability.....	12
Hardware Comparisons.....	12
Suggested Guidelines.....	14
Use Case for a Linux Access Gateway and an Identity Server.....	14
Use Case for a SSL VPN Server, a Linux Access Gateway, and an Identity Server.....	15

The Focus of System Testing

Novell System Test has provided this report so that customers can determine the required levels of hardware to meet their specific business goals. To ensure accurate benchmark results, System Test focused on reliability testing, performance testing, and scalability testing.

Although System Test has provided this performance information, other factors in a network impact overall performance. These include the following:

- **L4 Switches:** If the switch is slow or misconfigured, it can severely impact performance. If possible, System Test recommends that clustered Access Manager components be plugged directly into the switch or segmented accordingly.
- **Network bandwidth:** Gigabit copper networking was tested throughout the process, so this is a requirement for internal communication of high performing systems.
- **Web Servers:** The application servers are a major cause of performance problems, because they are processing the most information. The following tests used static and dynamic pages with 100+ images. The tests were based upon real-world traffic to give a general idea of response times that are less than a second. The public requests can be vary widely based upon size of the page, caching settings and content.
- **LDAP User Stores:** This critical component can be another major cause of performance problems, 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 are going to be used in the environment. Expect adjustments if you are attempting to get the maximum speed out of the cluster.

Access Manager 3.0 Test Plan

Components

The following components were included in the test:

- Linux Access Gateways
- Identity Servers
- Multiple User Stores
- SSL VPN Servers

Final Test Plan

The following sections provide a high-level view of the tests performed. For each of the components, there are subsections that discuss the type of testing and the goals of the test.

Access Gateway

Performance Testing

- 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 1 week through a stress test

Scalability (Clustering) Testing

- 1 x 4 x 4 (1 Administration Console, an Identity Server cluster with 4 members, and a Linux Access Gateway cluster with 4 members). We did test with 2 Administration Consoles in failover tests, but because of the number of different hardware environments, the scalability and performance tests only included 1.

Failover Testing

- HTTP/HTTPS traffic continues after a component failover

Identity Server

Performance Testing

- Authentication redirect from the Access Gateway

Reliability Testing

- Authentication redirect from the Access Gateway

Scalability Testing

- Authentication redirect from the Access Gateway

User Stores

Performance Testing

- Tested an authentication request from the Identity Server, following an authentication redirect from the Access Gateway
- Verified individual eDirectory tests at 40 logins per second for 4 days

Stress Testing

- Tested 100 threads HTTP/HTTPS traffic through a login

Reliability Testing

- Tested an authentication request from the Identity Server, following an authentication redirect from the Access Gateway

Scalability Testing

- Configured and tested in clusters of 30 Identity Servers

Failover

- Verified that logins were successful as 3 Identity Servers were enabled and disabled.

SSL VPN

Performance Testing

Enterprise mode with 500 connections to a high bandwidth server

- Initiated SSL VPN connections from multiple clients in Enterprise mode from a mix of Windows and SLED clients.

- After the connection was established, initiated continuous traffic over the tunnel using FTP scripts
- Ran the test for 8 hours, monitoring utilization and connection failures

Performance Testing

Kiosk mode with 500 connections to a high bandwidth server

- Initiated SSL VPN connections from multiple clients in Kiosk mode from a mix of Windows and SLED clients.
- After the connection was established, initiated continuous traffic over the tunnel using FTP scripts
- Ran the test for 8 hours, monitoring the utilization and connection failures

Server Hardware

The clustered tests were run with the following physical hardware:

- 1 Administration Console (Dell Poweredge 1850: Dual 2.8 GHz, 2 GB RAM)
- 4 Identity Servers (Dell Poweredge 1850: Dual 2.8 GHz, 2 GB RAM)
- 4 Access Gateways (Dell Poweredge 1850: Dual 2.8 GHz, 2 GB RAM)
- 3 external eDirectory user stores with 100,000 users (Clone: Dual 2.8 GHz, 2 GB RAM)
- 1 Apache 2 Web server running on SLES 9 SP3 (Clone: Dual 2.8 GHz, 2 GB RAM)
- 4 client machines running Loadrunner (Dell Poweredge 2850: Dual 2.8 GHz, 2 GB RAM)

The machines were all connected through Gigabit Ethernet on a gigabit network switch and a 100 MB Foundry L4 switch with a gigabit fiber connection to clients. In this configuration, System Test also compared the results when additional eDirectory servers and Web servers were added to the configuration and discovered that these additional machines caused no impact to performance.

The hardware comparisons were based upon two configurations with similar parameters.

IDP/LAG Environment 1

- Single processor
- Pentium 4, 3.6GHz
- 2 GB RAM
- SATA 150 GB drives

- Gigabit copper

IDP/LAG Environment 2

- Dual core
- AMD 64 dual core processor 5200+
- 2 GB RAM
- SATA 200 GB drives
- Gigabit copper

SSLVPN Environment

- Dual CPU
- Xeon 3.0 GHz
- 4 GB RAM
- SCSI 225 GB drives
- Gigabit copper

SSLVPN Client Environments

- 500 Clients ranging from 2 GHz to 3.2 GHz
- 1-2 GB of RAM
- 80-160 GB hard drives
- Gigabit copper network

Details of Configuration

- HTML pages were approximately 50 KB with 50 small images embedded.
- User stores had 20 threads with 100,000 users in a single container.
- Alteon and Foundry 10/100 L4 switches with the sticky bit enabled and with 2 virtual IP addresses.

Performance/Reliability/Stress Tools

The selected test tool for Identity Server and Linux Access Gateway testing was Mercury's Loadrunner because it is able to correctly replicate large IP ranges between multiple clients in a clustered environment. This allowed System Test to more closely simulate real-world environments and real browser interaction with Internet Explorer and Firefox.

The SSL VPN tests were done using SLATH (Novell's Superlab test automation tool), with the help of tools like FTP script, HTTP torture, LTFX, Iperf, etc. The main focus of the test was to exercise the scalability of the product.

Test Results

The results were compiled from the final results that System Test achieved with Novell Access Manager 3.0. The tests were ran multiple times to verify that the results were as accurate as possible.

Identity Server

Because the Identity Server is required for authentication, it was involved in the majority of test cases. Its performance results have been incorporated into the Linux Access Gateway tests.

Multiple Identity Servers were tested in a fault tolerant configuration.

Failover Test: **Pass**

Linux Access Gateway

The majority of the testing was done with the Access Gateway, which is the most visible portion of the product to the customer. So the focus was first upon performance, then stress, reliability, and finally scalability.

Comparisons results are based upon a cluster of 4 Access Gateways and a cluster of 4 Identity Servers.

Test Scenario	Results
Concurrent Users per Cluster	4 * 5000 (20000 users)
HTTPS Public	160 requests (5000 hits per second)
HTTPS Authentications	55 logins
HTTPS Authorizations	120 authorized pages
HTTPS Login with Identity Injection	42 logins
HTTPS Login with Form Fill	45 logins
HTTPS Login with Roles/AGA	47 logins
HTTPS Login with II, FF, Roles/AGA	40 logins
HTTPS Login with 10 page requests	15 logins (105 Authorizations)
<i>*Numbers listed are logins per second.</i>	
<i>*AGA is Access Gateway Authorization.</i>	

Failover Results

Linux Access Gateway Failover Test: **Pass**

Reliability Results (15 million authentications)

Linux Access Gateway Seven-Day Reliability Test: **Pass**

SSL VPN in HB Enterprise Mode

Achieve 500 concurrent SSL VPN connections in Enterprise mode using a single high bandwidth SSL VPN server.

Time Duration	Connections	Total Data Transferred
1.5 hours	512	58GB
3 hours	509	176GB
17.5 hours	371	1052 GB

SSL VPN in HB Kiosk Mode

Achieve 500 concurrent SSL VPN connections in Kiosk mode using a single high bandwidth SSL VPN server.

Time duration	Connections	Total Data Transferred
30 minutes	521	28GB
1.5 hours	518	121GB
4 hours	513	366GB
8 hours	505	768GB
12 hours	501	1192GB
17.5 hours	492	1689GB

User Stores

User stores were a key component of all the failover, reliability, and performance tests.

Failover Results

Active Directory: **Pass**

eDirectory: **Pass**

SunOne: **Pass**

Reliability Results Seven-Day Test (15 million authentications)

Active Directory: **Pass**

eDirectory: **Pass**

SunOne: **Pass**

Scalability

The goal of the scalability testing was to validate the architecture.

Component	Number of Devices/Items
Identity Servers	4
Linux Access Gateways	4
LDAP Servers	8
Web Servers	101
Policies/Roles	101
Accelerators	51
Concurrent Users on NAM	5000+ (per Access Gateway/Identity Server)

Hardware Comparisons

The hardware comparisons show how well a system runs with the different types of hardware and give a basic idea of how the product works. Each environment was set up with 1 Administration Console, 1 Linux Access Gateway, 1 Identity Server, 2 eDirectory servers (user stores), 1 Web server, and 1 client. The configuration used SSL between the Access Gateway and Identity Server, between the Identity Server and eDirectory (user store), and between the client and the Access Gateway.

The stress test used a worst possible test, running full speed with no delays against the system, which is not realistic in a business case. However, it helps to provide raw data to compare hardware platforms.

Environment 1: Single Processor Pentium 4, 3.6 GHz, 2 GB RAM

Environment 1	Results
HTTPS Public	65 requests
HTTPS Authentications	32 logins
HTTPS Login with 10 page requests	9 logins with 80 requests
HTTPS Login with Identity Injection	22 logins
HTTPS Login with Form Fill	19 logins
HTTPS Login with Roles/AGA	16 logins

Environment 2: AMD 64 Dual Core Processor 5200+, 2 GB RAM

Environment 2	Results
HTTPS Public	98 requests
HTTPS Authentications	43 logins
HTTPS Login with 10 page requests	18 logins with 90 requests
HTTPS Login with Identity Injection	30 logins
HTTPS Login with Form Fill	26 logins
HTTPS Login with Roles/AGA	22 logins

Suggested Guidelines

Use Case for a Linux Access Gateway and an Identity Server

The use case is based upon a user that logs in once, requests 30 pages (approximately 1000 hits) during a 30 minute time period, then drops 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 because we only care about how many are using the system at the same time. There can be 10 million or 10,000 users, but the recommendation is based upon the simultaneous users on the cluster at any one point in time.

Recommendations

When two numbers are listed in the cluster setup, the required number of machines depends upon traffic spikes within the network. When usage is high for accessing Web servers and applications, more Access Gateways are required. When usage is high for users and authentication, more Identity Servers are required. The setup needs to be evaluated in a real-world situation. The following are general recommendations and are based upon a test environment and setup, so the actual requirements will be different for each business.

Simultaneous Users	Cluster Setup
5000 Users	1-2 Access Gateways, 1-2 Identity Servers. 2 are required for fault tolerance/load balancing.
10,000 Users	2 Access Gateways, 2 Identity Servers
15,000 Users	3 Access Gateways, 2 Identity Servers
20,000 Users	4 Access Gateways, 2-3 Identity Servers
50,000 Users*	10 Access Gateways, 3 Identity Servers
100,000 Users*	20 Access Gateways, 4 Identity Servers
*Expanded the time to 1 hour for the use case.	

Use Case for a SSL VPN Server, a Linux Access Gateway, and an Identity Server

The use case is based upon 500 users that log in once and continually make a series of actions over an eight hour period. The test is used to validate that 500 users can concurrently be logged into the system and perform work.

Recommendations

The following are general recommendations and are based upon a test environment. The results can vary due to bandwidth and the applications that are attempting to pass through the server.

Simultaneous Users	Cluster Setup
500 Users in Enterprise Mode	1 SSL VPN Server with High Bandwidth
500 Users in Kiosk Mode	1 SSL VPN Server with High Bandwidth