

Novell Access Manager 3.1

Performance and Sizing Guidelines

Performance, Reliability, and Scalability Testing

| | | |
|-------------|--|--|
| Disclaimer | 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. | |
| Trademarks | Novell is a registered trademark of Novell, Inc. in the United States and other countries. * All third-party trademarks are property of their respective owner. | |
| | Copyright 2009 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. | |
| | Novell, Inc. 404 Wyman Street, Suite 500 Waltham, MA 02451 U.S.A. www.novell.com | Novell UK Limited Novell House 1 Arlington Square Downshire Way Bracknell Berkshire RG12 1WA |
| Prepared By | Jeremy Brown | |
| | Novell Access Manager - White Paper March 2009 | |

Contents

| | |
|--|----|
| Introduction..... | 4 |
| Test Setup..... | 5 |
| Access Gateway..... | 5 |
| SSL VPN..... | 6 |
| Server Hardware | 6 |
| Load Balancers..... | 7 |
| Details of Configuration..... | 7 |
| Performance/Reliability/Stress Tools..... | 7 |
| Other Factors Influencing Performance Information..... | 8 |
| Results..... | 9 |
| Linux Access Gateway Performance..... | 9 |
| SSL VPN..... | 10 |
| Scalability..... | 10 |
| Reliability..... | 11 |
| Sizing Guidelines..... | 12 |
| Use Case for Linux Access Gateway and Identity Server..... | 12 |
| Recommendations..... | 12 |
| Use Case for SSL VPN, Linux Access Gateway, and Identity Server..... | 12 |
| Recommendations | 13 |
| Conclusion..... | 14 |

Introduction

Novell® Access Manager is a comprehensive access management solution that provides secure access to Web and enterprise applications. Access Manager also provides seamless single sign-on across technical and organizational boundaries, and uses industry standards including SAML (Secure Assertions Markup Language) and Liberty Alliance protocols.

This white paper details the performance, reliability, and scalability of the product so that you can deploy the correct configuration in your environment. The test results are artificial, and every environment is different, but the data should help in determining the design of your system. This paper specifically refers to the 3.1.0 release of Novell Access Manager that shipped in December 2008.

Key Features of Novell Access Manager

- 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 for remote users
- Delivers roles-based access control for Web-based and enterprise applications
- Establishes federated links with trusted business partners

Test Strategy

The test was designed to represent a medium-sized business with heavy traffic, in order 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 in order 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.

Test Setup

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 Novell Access Manager.
- The authorization requests test 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 a cluster of 4 Access Gateways. The number of users and the amount of traffic determine the size of the cluster.

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 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).

Failover Testing

- HTTP/HTTPS traffic continues after a component failover

SSL VPN

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

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

Server Hardware

The Linux Access Gateway clustered tests were run with the following physical hardware:

- 1 Administration Console (Dell PowerEdge 1850: Dual 2.8 GHz, 2GB RAM)
- 4 Identity Servers (Dell PowerEdge 1850: Dual 2.8 GHz, 2GB RAM)
- 4 Access Gateway Servers (Dell PowerEdge 1850: Dual 2.8 GHz, 2GB RAM)
- 3 external eDirectory™ user stores with 100,000 users (Clone: Dual 2.8 GHz, 2 GB RAM)
- 1 Apache2 Web server running on SLES 9 SP3 (Clone: Dual 2.8 GHz, 2 GB RAM)
- 4 client machines running LoadRunner (Clone: 3.2 GHz, 2GB RAM)

The SSL VPN servers were run with the following physical hardware:

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

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

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

Load Balancers

The following L4 switches were used as load balancers:

- Zeus ZXTM LB (software L4 switch)
- Foundry ServerIron XL (hardware L4 switch)
- Alteon 2424 (hardware L4 switch)

Details of Configuration

- HTML pages were approximately 50 KB with 50 small images embedded for all the tests.
- Access Manager user store configurations had 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 less performance. The primary user store we used in the tests was eDirectory 8.8.3.

Performance/Reliability/Stress Tools

The HP Mercury LoadRunner tool was used for 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 specifics of the LoadRunner tests:

- The virtual users had 100 threads between 4 clients. This was the optimal amount of threads before the system started to receive excessive login times.
- The scripts that we use 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, then you must use sslid load balancing on the Layer 4 switch. You must have parameters for the users so you aren't using the same user for every connection.

The SSL VPN tests were done with the Novell Superlab test automation tool, SLATH, with the help of tools such as ftp-script, HTTP torture, LTFX, and iperf. The main focus of the testing was to exercise the scalability of the product across multiple protocols and high bandwidth. The combinations of tools allowed us to increase the performance from the clients instead of trying to use one tool for everything.

Other Factors Influencing Performance Information

We have provided a description of the hardware and of the test configuration. However, other factors in a network also 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. 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 than when persistence is enabled.
- **Network Bandwidth:** Gigabit copper networking was used throughout the testing process, so this is a requirement for the product to meet the testing results. If you are only 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 are processing the most information. The tests used static and dynamic pages with 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 are going to 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 was used primarily throughout the testing to give a baseline for the product.
- **Timeout:** If you are going to run a performance test, you need to factor in sessions being stored on the server. The tests have 2 minute timeouts so that the tests did not overrun the total users on the system of 20,000 active sessions on the cluster. You need to take this into account when planning capacity testing on a cluster.
- **Users:** Do not attempt to run a performance test without ensuring that you have enough users on the system to run the 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 unusual scenario has a negative effect on performance and invalidates the test.

Results

The tests results are divided into a Linux Access Gateway section (which includes the Identity Server) and an SSL VPN section. Each section contains the results of the performance, scalability, and reliability tests.

Linux Access Gateway Performance

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 broken out by minute to show how the product performs.

| Test Scenario | Results |
|-----------------------------------|--|
| HTTPS Public | 13200 requests (480,000 hits) per minute |
| HTTPS Authentications | 5220 logins per minute |
| HTTPS Authorizations | 11520 authorized pages per minute |
| HTTPS Login with 10 page requests | 2460 logins (9000 Authorizations) per minute |

These performance numbers are broken out by second to show how the system performs.

| Test Scenario | Results |
|-------------------------------------|--|
| Concurrent Users per Cluster | 4 servers with 5000 users each (20000 users per cluster) |
| HTTPS Public | 220 requests (8000 hits per second) |
| HTTPS Authentications | 87 logins per second |
| HTTPS Authorizations | 192 authorized pages per second |
| HTTPS Login with Identity Injection | 62 logins per second |
| HTTPS Login with Form Fill | 64 logins per second |
| HTTPS Login with Roles/AGA | 81 logins per second |

| Test Scenario | Results |
|--|---|
| HTTPS Login with II, FF, Roles/AGA | 60 logins per second |
| HTTPS Login with 10 page requests | 41 logins (150 authorizations) per second |
| <i>AGA is Access Gateway Authorization, II is Identity Injection, and FF is Form Fill.</i> | |

SSL VPN

High Bandwidth Enterprise SSL VPN Mode

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

Enterprise Server Performance

| Time Duration | Connections | Throughput |
|---------------|-------------|-------------------|
| 8 hours | 500 | 15 MB/sec average |

High Bandwidth Kiosk Mode

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

Kiosk Server Performance

| Time Duration | Connections | Throughput |
|---------------|-------------|-------------------|
| 8 hours | 500 | 26 MB/sec average |

Scalability

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

| Component | Number of Devices/Items |
|-----------------------|-------------------------|
| Identity Servers | 8 |
| Linux Access Gateways | 8 |

| Component | Number of Devices/Items |
|------------------------------------|----------------------------------|
| LDAP Servers | 8 |
| Web Servers | 101 |
| Policies/Roles | 101 |
| Accelerators | 51 |
| SSL VPN | 500 connections per server |
| Concurrent Users on Access Manager | 5000 sessions per Access Gateway |

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 see if Access Manager can sustain that load and still 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**

Sizing Guidelines

Use Case for Linux Access Gateway and Identity Server

This 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. 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 the 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 and are based upon a test environment and setup. Each business setup requires some modifications to the recommendations.

| Simultaneous Users | Cluster Setup |
|--------------------|---|
| 5000 Users | 1-2 Access Gateway, 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 |

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

This use case is based upon a user that logs in once and makes a series of actions continually to achieve 500 users over an eight hour period. The system is used to validate the concurrency and to show that they can all be working together on the system.

Recommendations

The simultaneous users are based upon concurrency and the server will support the recommendation for a standard user. The results might vary because of bandwidth and the applications that are attempting to pass through the server.

| Simultaneous Users | Cluster Setup |
|---------------------------|---|
| 500 Users | 1 SSL VPN Enterprise Mode with High Bandwidth |
| 500 Users | 1 SSL VPN Kiosk Mode |

Conclusion

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

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