Netegrity SiteMinder 4.51 AuthMark Performance Details

By Bruce Weiner
(PDF version, 96 KB)

March 22, 2001

Contents

Test Methodology

Mindcraft® tested the performance of Netegrity SiteMinder 4.51 using our iLOAD MVP™ tool to run the AuthMark ™ Benchmark Login and Extranet Scenarios. In this section, we describe these tools so that you will be able to understand the performance results discussed in the Result Analysis section below.

iLOAD MVP Overview

iLOAD MVP is a general-purpose, script-driven capacity planning, benchmarking, and regression testing tool. The major components of iLOAD MVP are:

- A Control Center that manages client systems, controls test script execution, and reports on test results.
- Multi-threaded client load generators that execute test scripts to simulate users accessing a server.
- Test script generation programs.
- Test data generation programs.

iLOAD MVP provides the capabilities needed to test high-performance servers with a small number of client systems. Its capabilities include:

- The ability to simulate a large number of simultaneous user sessions. The number of user sessions is limited only by the client OS, the amount of memory and the performance of the client systems.
- Support for HTTP 1.0 and 1.1 as well as LDAP V3.
- Support for authentication and authorization.
- Support for SSL.
- Custom test scripts.

The AuthMark Benchmark

The AuthMark Benchmark is designed to test the performance of products that provide authentication and authorization services in support of Web servers. *Authentication* is the process of verifying who a user is; it typically occurs when a user logs in. *Authorization* is the process of verifying that an authenticated user is allowed to see or to use a particular resource. In the case of a

Web server such resources include HTML files, graphic files, and programs that generate Web pages dynamically.

AuthMark simulates a large number of users accessing Web servers via their browsers. This approach permits AuthMark to test authentication and authorization performance independent of the technology used to provide those services.

AuthMark consists of several test scenarios to determine various aspects of performance for authentication and authorization systems under different circumstances. For the SiteMinder tests we used the AuthMark Login and Extranet Scenarios.

AuthMark Login Scenario

The AuthMark Login Scenario focuses on testing authentication. We call it the Login Scenario because authentication is done the first time a user accesses a protected part of a Web site, just like a login. The HTTP 1.0 and 1.1 protocols define the steps a browser follows for authentication. Some of the steps are visible to you and others are not. It is important to understand what happens during a login in order to understand what the Login Scenario measurements mean.

Login Process

The following simplified sequence will walk you through the login process to show you how it works using the HTTP 1.0 and 1.1 protocols:

1. When you click on a link or enter a URL in your browser your browser sends the requested URL to the Web server.
2. The Web server determines that you must be authenticated before it returns the resource at the requested URL. Typically, the authentication requirement is specified as part of the Web server's configuration or via an authentication/authorization product connected to the Web server.
3. The Web server sends back a "401" HTTP response to your browser indicating that you are not authorized to see that requested resource.
4. Your browser pops open a window and asks you to enter your user ID and a password.
5. After you enter your user ID and password, your browser stores them in memory and associates them with the protected space (called a *realm*) containing the URL you requested.
6. Your browser then resends a request for the same URL but this time it includes an HTTP authorization header containing your user ID and password.
7. This time the Web server checks your user ID and password to see if they match the authentication information in the authentication system. If they do, you are authenticated.

8. Now that you have been authenticated, the authorization system checks whether or not you are authorized to access Web pages in the realm. If you are authorized, the Web server sends the Web page you requested.

Notice that the URL you clicked on or entered is actually sent twice (in steps 1 and 6). This means that the authentication system is used twice—first, it finds out that the requested URL requires the user be authenticated, then it processes the authorization header when the request is resent.

Once a user has been authenticated, the Web browser automatically sends the authorization header whenever the user requests a URL in the same realm requiring authentication.

Login Scenario Configuration

Table 1 shows the AuthMark Login Scenario configuration parameters we used.

Table 1: AuthMark Login Scenario Configuration Parameters

Parameter	Value
Number of users in the security database	1,000,000
Number of Organizational Units or security groups	10
Total number of user sessions per test	100,000

The number of user sessions active during a given test run is determined by the length of the test and the number of logins. Sessions are not logged out once created. Instead, each session remains quiescent after login.

Running the Login Scenario

The basic steps for running the Login Scenario are:

1. Generate the data to fill the security database. iLOAD MVP provides a tool to generate realistic data for the LDAP V3 organizationalPerson object class and Netscape's inetOrgPerson object class. It also includes tools to load the same data into an LDAP directory, which was used for this test.
2. Load the security database with the user data.
3. Generate the test scripts for the Login Scenario. iLOAD MVP provides a tool to do this. These scripts drive iLOAD MVP to simulate user interaction with the Web server(s).
4. Load Web pages on the Web server(s). There are 100 Web pages each of which is 14 KB in size for the Login Scenario.
5. Load and configure the user management system or

authentication/authorization system.
6. Run the benchmark.

The Login Scenario test script selects users randomly from the user database (see Table 1 for the numbers we used for this test). The tester is free to select the number of client test systems and the number of iLOAD MVP client threads to use. These are called the *load generators*.

The tester selects the number of load generators to get the highest performance possible from the authentication/authorization system being tested. In order to obtain the peak performance from an authentication/authorization system, the tester may need to use multiple Web servers and database servers.

The tester is permitted, but not required, to do a warm-up run of the test scenario in order to get the servers to a state that would more likely represent the state they would be in during normal operation. For this benchmark, we warmed-up the servers by running the test script in its entirety.

Extranet Scenario

The Extranet Scenario is intended to simulate an environment where users must login to a Web site and where all access requests require authorization. This scenario depicts a more complete and more realistic usage pattern than the Login Scenario.

The Extranet Scenario test execution starts with the same operation sequence as the Login Scenario (steps 1 - 6 above) and continues with the following operations:

7. The test client requests a resource.
8. The authorization services check the validity of the user and and that the user is authorized to have access to the resource.
9. If the user is authorized, the resource is returned.
10. The test client then requests additional resources.

SiteMinder checks the continuing validity of the authenticated user each time a resource access request is made to ensure that the user session has not been revoked. However, the user is not re-authenticated. As a result, the user does not see a new login request as long as the resources being accessed are in the Internet domain in which the user has been authenticated.

The Extranet Scenario operation sequence consists of one login followed by 10 authorizations yielding a total of 11 operations per user session. We call these 11 operations an Extranet Sequence. For the Extranet Scenario, we warmed-up the servers by running the test script in its entirety.

Result Analysis

This section analyzes the Login and Extranet Scenario performance characteristics of Netegrity's SiteMinder 4.51 including its performance scalability with different server configurations.

1,000,000 User Login Performance

The SiteMinder Policy Server is the control point for all authentication and authorization. Our tests were structured to push the Policy Server systems as close as possible to 100% CPU utilization. Table 2 summarizes the Login Scenario performance as a function of the SiteMinder Policy Server system(s) configuration. The Scaling Factor in Table 2 shows how much faster a configuration is compared to a single system having one CPU.

Table 2: SiteMinder Login Performance Scalability - 1,000,000 Users

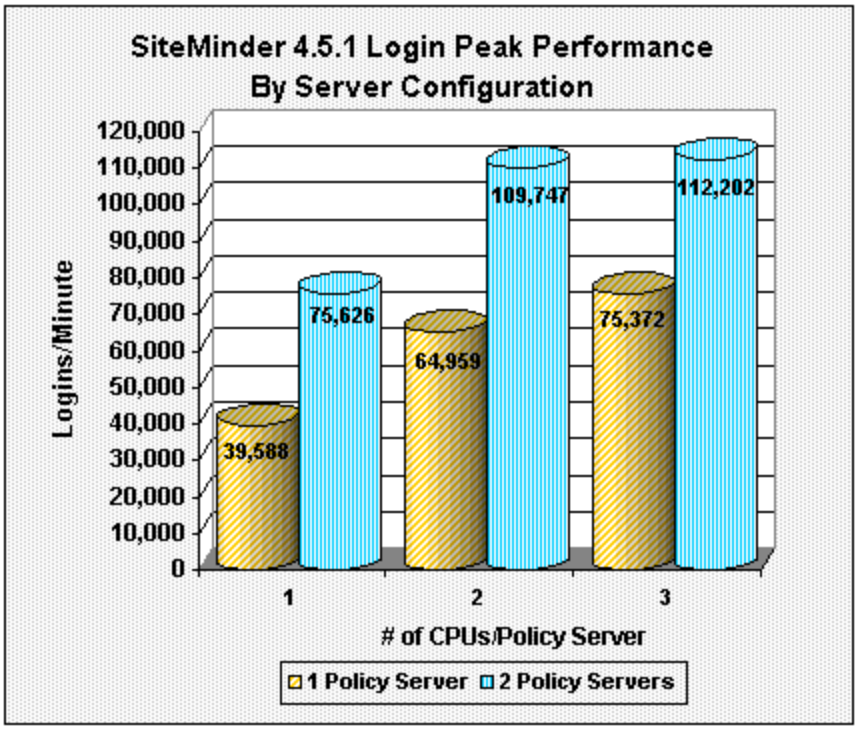
Logins per second	Logins per minute	Logins/ minute/ Policy Server CPU	Scaling factor	Policy Server (s) CPU Utilization	SiteMinder Policy Server configuration
660	**39,588**	**39,588**	-	100%	1 system, 1 CPU
1,083	**64,959**	**32,480**	1.6	97%	1 system, 2 CPUs
1,256	**75,372**	**25,124**	1.9	88%	1 system, 3 CPUs
1,260	**75,626**	**37,813**	1.9	98%	2 systems, 1 CPU
1,829	**109,747**	**27,437**	2.8	75% - 80%	2 systems, 2 CPUs
1,870	**112,202**	**18,700**	2.8	55%	2 systems, 3 CPUs

The CPU utilizations for the Policy Server configurations with one system, three CPUs and with two systems, two and three CPUs show that we did not have enough Web servers or fast enough ones to drive the Policy Servers to full CPU utilization. This lack of Web servers showed up for the test of the Policy Server configuration using two systems with two CPUs each even though we added a four-processor Enterprise 4500 Web server with 400 MHz CPUs to the ones we were using for the other tests. And when we used an additional Enterprise 450 with four 300 MHz CPUs for the test of two Policy Servers with three CPUs each, we still had insufficient Web server performance to drive the Policy Servers to full CPU utilization. If the lab had enough Web servers available, we fully expect that SiteMinder would have achieved more logins per minute than it did.

During each of the tests, the LDAP directory server showed only 10% to 15% CPU utilization on one CPU while its other CPUs were idle. This shows that SiteMinder made very efficient use of the LDAP directory server.

Figure 1 presents SiteMinder's performance from Table 2 by server configuration, with the gold columns showing the results for a single Policy Server and the blue column showing the result for dual Policy Servers.

Figure 1: SiteMinder Login Scalability for 1,000,000 Users



1,000,000 User Extranet Performance

Table 3 compares the SiteMinder Extranet Scenario performance to that of the Login Scenario for the same hardware configuration - one Policy Server with one CPU. The results in Table 3 demonstrate that the SiteMinder Policy Server performs authorizations several times faster than authentications. It is not possible to calculate the exact performance difference because the CPU utilization of the Policy Server CPU was 50% for the Extranet test and was 100% for the Login test. This also means that the Extranet performance would have been significantly higher if there were enough Web servers available in the lab to drive the Policy Server's CPU to full utilization.

Table 3: SiteMinder Extranet and Login Performance - 1 Policy Server with 1 CPU

Measurement	Extranet Scenario	Login Scenario
Authentications/minute	20,179	39,588
Authorizations/minute	201,790	39,588
Total operations/minute	**221,969**	**79,176**

Conclusions

These test results lead us to conclude that:

- Netegrity SiteMinder 4.51 outperforms all other products we've tested so far for the AuthMark Login and Extranet Scenarios.
- SiteMinder 4.51 delivers the highest Login and Extranet performance per policy/security server CPU of any product we have tested to date.
- SiteMinder delivers outstanding performance scaling as CPUs and Policy Servers are added to a configuration.

Hardware Configurations Tested

Mindcraft used a mix of systems for the Web servers. Table 4 shows the Enterprise 450 Web server configuration we used. The Ultra 80 configurations we used for Web servers and the SiteMinder Policy server are shown in Table 5. Table 6 shows the Enterprise 4500 Web server configuration we used. Finally, Table 7 shows the Enterprise 4500 configuration we used for the LDAP directory server.

Table 4: Sun Enterprise 450 Web Server Configuration

Feature	Configuration
CPU	4 x 300 MHz UltraSPARC II Cache: L1: 16 KB I + 16 KB D; L2: 2 MB
RAM	4 GB ECC
Disk	5 x 4.2 GB SCSI; one for Solaris and one for the Web data
Networks	2 x 100Base-TX NICs

Table 5: Sun Ultra 80 Web and Policy Servers Configuration

Feature	Configuration
CPU	4 x 450 MHz UltraSPARC II (we used the psradm command to enable/disable processors in the Policy Server) Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	4 GB ECC
Disk	2 x 18 GB SCSI
Networks	2 x 100Base-TX NICs

Table 6: Sun Enterprise 4500 Web Server Configurations

Feature	Configuration
CPU	4 x 400 MHz UltraSPARC II (we used the psradm command to disable 10 of the 14 processors in the system)

	Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	14 GB ECC
Disk	4 x 18 GB SCSI
Networks	1 x Quad 100Base-TX NIC (4 ports, only 2 used)

Table 7: Sun Enterprise 4500 LDAP Directory Server Configuration

Feature	Configuration
CPU	14 x 400 MHz UltraSPARC II Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	14 GB ECC
Disk	4 x 18 GB SCSI, no RAID
Networks	1 x Quad 100Base-TX NIC (4 ports, only 1 used)

Figure 2 shows how the servers were configured for all of the Login Scenario tests using one Policy Server as well as the test using two Policy Servers with one CPU. Figure 3 gives the server configuration for the Login test using two Policy Servers with two CPUs. Figure 4 presents the server configuration for the Login Scenario test of two Policy Servers each with three CPU and for the one Policy Server with one CPU Extranet Scenario test. All of the systems were connected using Netgear 8 port 10/100 Base-TX hubs.

Figure 2: Server Configuration for all 1 Policy Server and 2 Policy Server with 1 CPU Login Tests

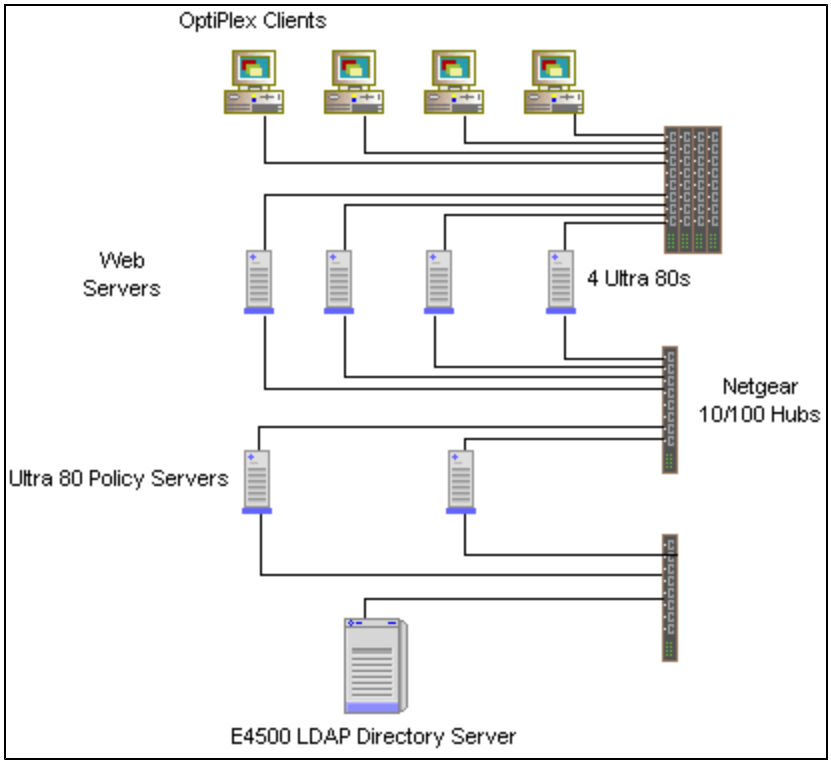


Figure 3: Server Configuration for 2 Policy Servers with 2 CPUs Login Test

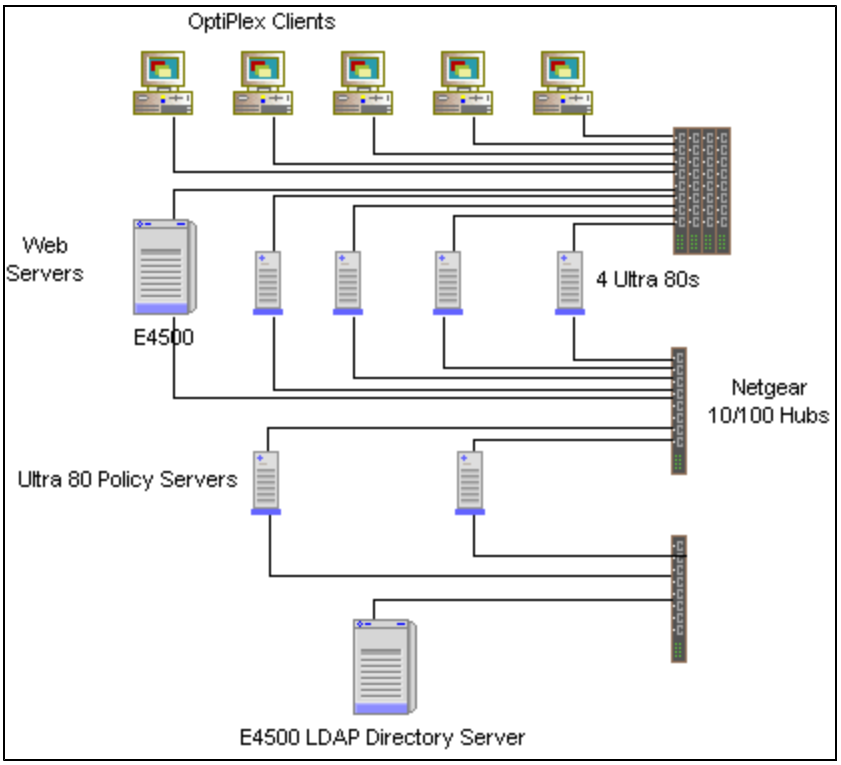
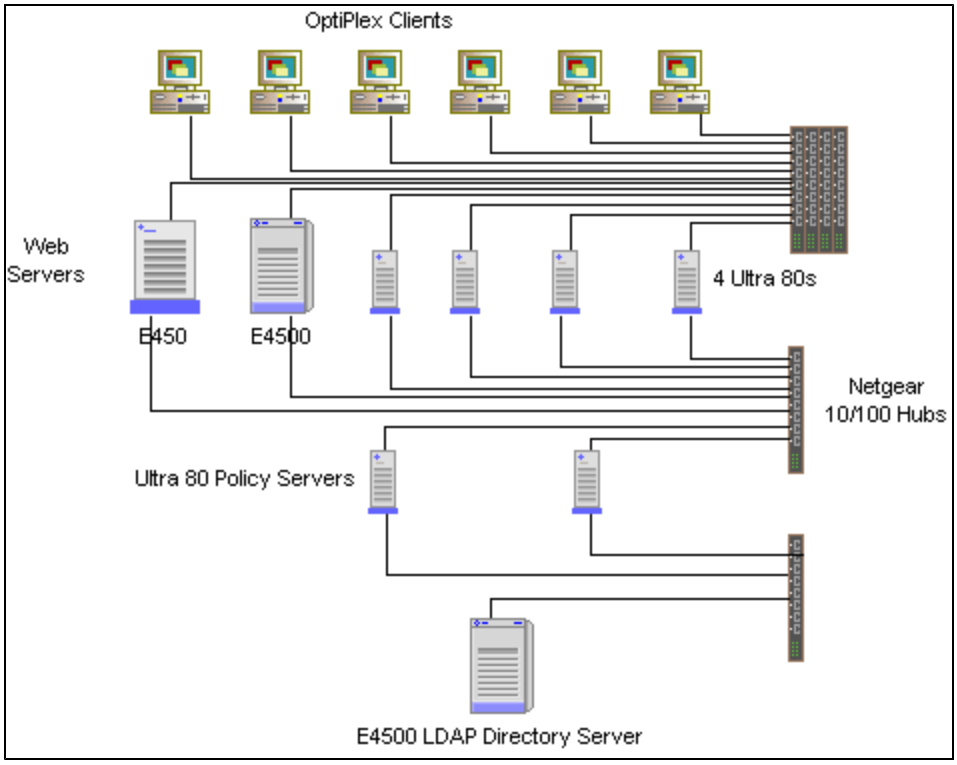


Figure 4: Server Configuration for 2 Policy Servers with 3 CPUs Login Test and 1 Policy Server with 1 CPU Extranet Test



Server Software Configuration and Tuning

We used the following server software for these benchmark tests:

- Solaris 8 with all current recommended patches on all of the Sun systems
- Netscape Directory Server 4.12 (B00.193.0237)
- iPlanet Web Server, Enterprise Edition 4.1 Service Pack 3
- Netegrity SiteMinder 4.51, Service Pack 1

All software ran with default settings except for the following:

- For Netscape Directory Server:

  Change in slapd.ldbm.conf:

  lookthroughlimit 10000
  allidsthreshold 5000
  cachesize 110000
  dbcachesize 1000000000
  db_home_directory /tmp/B2B

  index uid pres, eq, sub
  index ou eq, sub
  index o pres, eq

Changes in slapd.conf:

timelimit 600
sizelimit 10000

- For SiteMinder Policy Server:
  - user cache size = all users
  - 100% of all policies cached (there was one policy)
  - session timeout = 2 hours
- For the SiteMinder Web Agent:
  - User session cache disabled
  - resource cache size = 1000

Client Test Systems

For all of the tests, we used Dell OptiPlex GX 110 client test systems configured as shown in Table 8. The client test systems we used for each test are shown in Figures 2 , 3 and 4.

Table 8: Client Test Systems Configuration

Feature	Configuration
System	Dell OptiPlex GX 110, 1 x 667 MHz Pentium III CPU
RAM	384 MB SDRAM
Disk	1 x 14.5 GB ATA/66
Networks	1 x 100Base-TX (3Com 3C905C-TX)
Operating System	Microsoft Windows NT 4.0 Workstation, Service Pack 5

For more information, contact us at: info@mindcraft.com
Phone: +1 (408) 395-2404
Fax: +1 (408) 395-6324