Baltimore Technologies SelectAccess 3.1 AuthMark Performance Details

By Bruce Weiner
(PDF version, 295 KB)

August 6, 2001

Contents

Test Methodology

Mindcraft® tested the performance of Baltimore Technologies SelectAccess 3.1 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 SelectAccess 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.

SelectAccess 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 Baltimore Technologies SelectAccess 3.1 including its performance scalability with different server configurations.

Login Performance

Table 2 summarizes the Login Scenario performance as a function of the SelectAccess policy server system(s) configuration. The Scaling Factor in Table 2 shows how much faster a configuration is compared to a single system with one CPU using one directory server, the smallest configuration.

We compute the logins/minute/total CPUs by dividing the logins/minute by the total number of CPU used as shown in the column *# of CPUs by Server Type* in Table 2. See the hardware configurations for more details on the test environment.

Because the SelectAccess 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. The *CPU Utilization* column in Table 2 shows the average CPU utilizations by type of server. These show that the LDAP directory server was barely used, so it was not a performance bottleneck.

The networks between the load generators and Web servers also were not saturated—the highest performance test had 3,423 logins per second, which generated total network traffic of 777.6 Mbits/second across four switches. The most bandwidth used in any switch was 222.2 Mbits/second, well below the switch maximum of 614.4 Mbits/second. In addition, the most bandwidth in any switch port was 37 Mbits/second, which is significantly below the bandwidth limit for a 100Base-TX network segment. The network link between a policy server and the Web servers was used about 30% at the highest login rate.

Looking at the policy server and the Web server CPU utilizations together, we see that policy server CPU utilization dropped as policy server CPUs were increased from three to four while the number of Web servers and Web server CPUs stayed constant. The resulting Web server CPU utilizations increased to 78% but we could not raise it above that level. This indicates that if we had used more Web server CPUs then we could have been able to increase the policy server CPU utilization and might have achieved

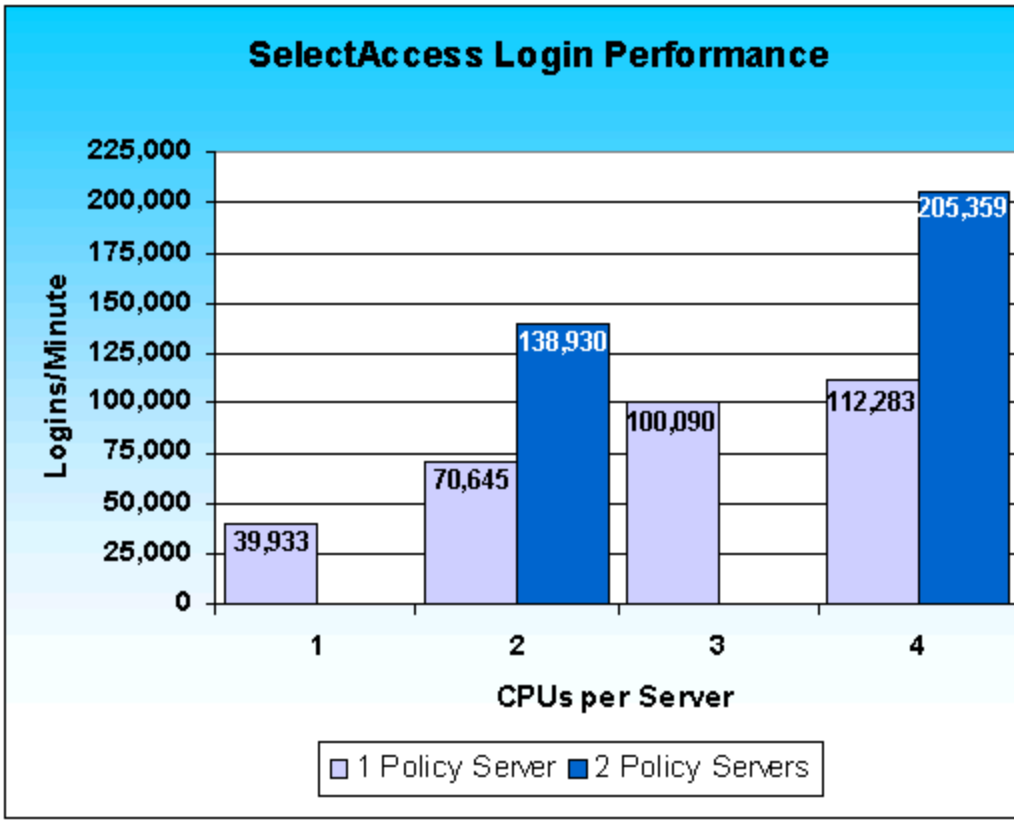
a higher login rate.

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

Logins per Second	Logins per Minute	Logins/ Minute/ Total CPUs	Scaling Factor	SelectAccess Policy Server Configuration	# of CPUs by Server Type	CPU Utilization
666	39,933	4,992	-	1 system, 1 CPU	Policy: 1 Web: 6 LDAP: 1 **Total: 8**	Policy: 100% Web: 38% LDAP: 2%
1,177	70,645	7,065	1.8	1 system, 2 CPUs	Policy: 2 Web: 7 LDAP: 1 **Total: 10**	Policy: 93% Web: 50% LDAP: 2%
1,668	100,090	6,673	2.5	1 system, 3 CPUs	Policy: 3 Web: 11 LDAP: 1 **Total: 15**	Policy: 85% Web: 65% LDAP: 2%
1,871	112,283	7,018	2.8	1 system, 4 CPUs	Policy: 4 Web: 11 LDAP: 1 **Total: 16**	Policy: 67% Web: 78% LDAP: 2%
2,315	138,930	5,146	3.5	2 systems, 2 CPUs	Policy: 4 Web: 22 LDAP: 1 **Total: 27**	Policy: 93% Web: 50% LDAP: 2%
3,423	205,359	4,890	5.1	2 systems, 4 CPUs	Policy: 8 Web: 33 LDAP: 1 **Total: 42**	Policy: 74% Web: 60% LDAP: 2%

Figure 1 shows SelectAccess's Login performance from Table 1 by server configuration.

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



Extranet Performance

Table 3 shows the SelectAccess Extranet Scenario performance for three configurations. The CPU utilizations shown are the average for each type of server.

For the configuration with SelectAccess two policy servers each having four CPUs, the policy servers CPU utilizations show that the Extranet performance was not limited by available CPU cycles. The network bandwidth for the three most heavily used switches between the load generators and the Web servers used 61.6% of the available switching bandwidth and about 63% of the bandwidth of each 100Base-TX network segment. For the two policy server tests, one of the policy servers handled six Web servers and the other handled five. For the test using four CPUs per policy server, the that served the six Web servers used about 57% of the available bandwidth on the network segment between it and the Web servers.

Table 3: SelectAccess Extranet Performance - 1,000,000 User Directory

Measurement	1 Policy Server with 2 CPUs	2 Policy Servers with 2 CPUs each	2 Policy Servers with 4 CPUs each
Authentications/minute	10,711	21,774	32,192
Authorizations/minute	107,110	217,740	321,920

Total Operations/minute	**117,821**	**239,514**	**354,112**
CPUs used	Policy: 2 Web: 7 LDAP: 1 **Total: 10**	Policy: 4 Web: 22 LDAP: 1 **Total: 27**	Policy: 8 Web: 33 LDAP: 1 **Total: 42**
Total operations/minute/CPU	**11,782**	**8,871**	**8,431**
CPU Utilizations	Policy: 95% Web: 65% LDAP: 2%	Policy: 95% Web: 55% LDAP: 2%	Policy: 76% Web: 70% LDAP: 2%

Conclusions

These benchmark results lead us to conclude that:

- Baltimore Technologies SelectAccess 3.1 delivers the highest overall AuthMark Login and Extranet performance we've measured to date.
- SelectAccess 3.1 achieves the highest Login performance per policy/security server CPU and the best Login and Extranet performance per CPU, for all CPUs used, that we have measured to date.
- SelectAccess delivers outstanding performance scaling as CPUs and policy servers are added to a configuration.

Hardware Configurations Tested

Table 4 shows the configuration of the Sun Enterprise 420R systems we used as Web, policy, and LDAP directory servers.

Table 4: Sun Enterprise 420R Server Configuration

Feature	Configuration
CPU	4 x 450 MHz UltraSPARC II Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	4 GB ECC
Disk	2 x 18 GB SCSI; one for Solaris and one for data
Networks	2 x 100Base-TX Sun NICs

Figure 2 shows how the systems were configured for the Login Scenario test using one Policy Server with one CPU. Figure 3 gives the server configuration for the Login and Extranet Scenario tests using one Policy Server with two CPUs. Figure 4 presents the server configuration for the Login Scenario tests of one Policy Servers each with three and four CPUs. Figure 5 shows the system configuration for all of the Login and Extranet Scenario tests that used two policy servers. All of the systems were connected using 8-port Hewlett-Packard ProCurve 408 10/100 Base-TX switches.

Figure 2: Server Configuration for 1 Policy Server with 1 CPU Login Test

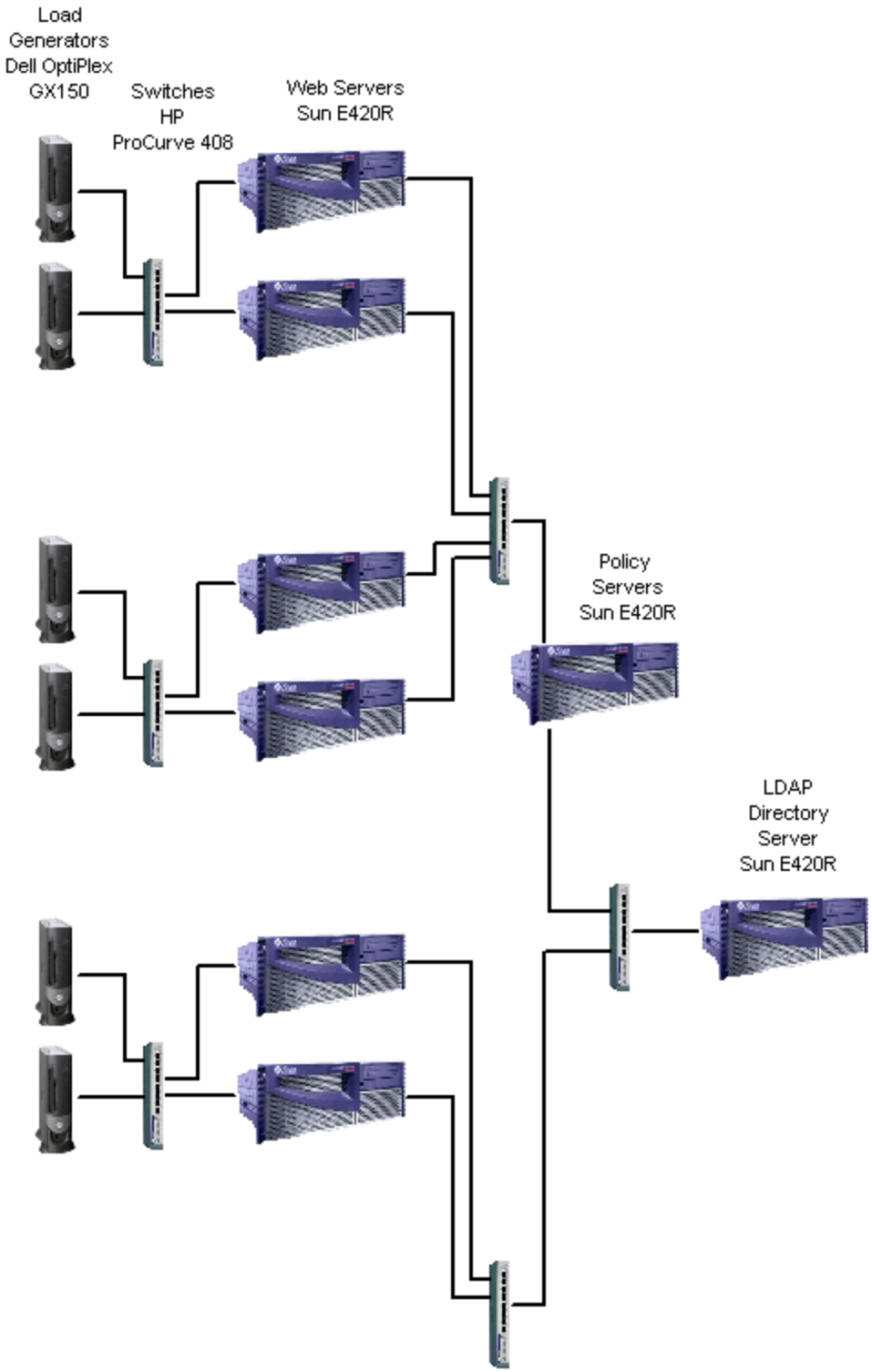


Figure 3: Server Configuration for 1 Policy Server with 2 CPUs Login and Extranet Tests

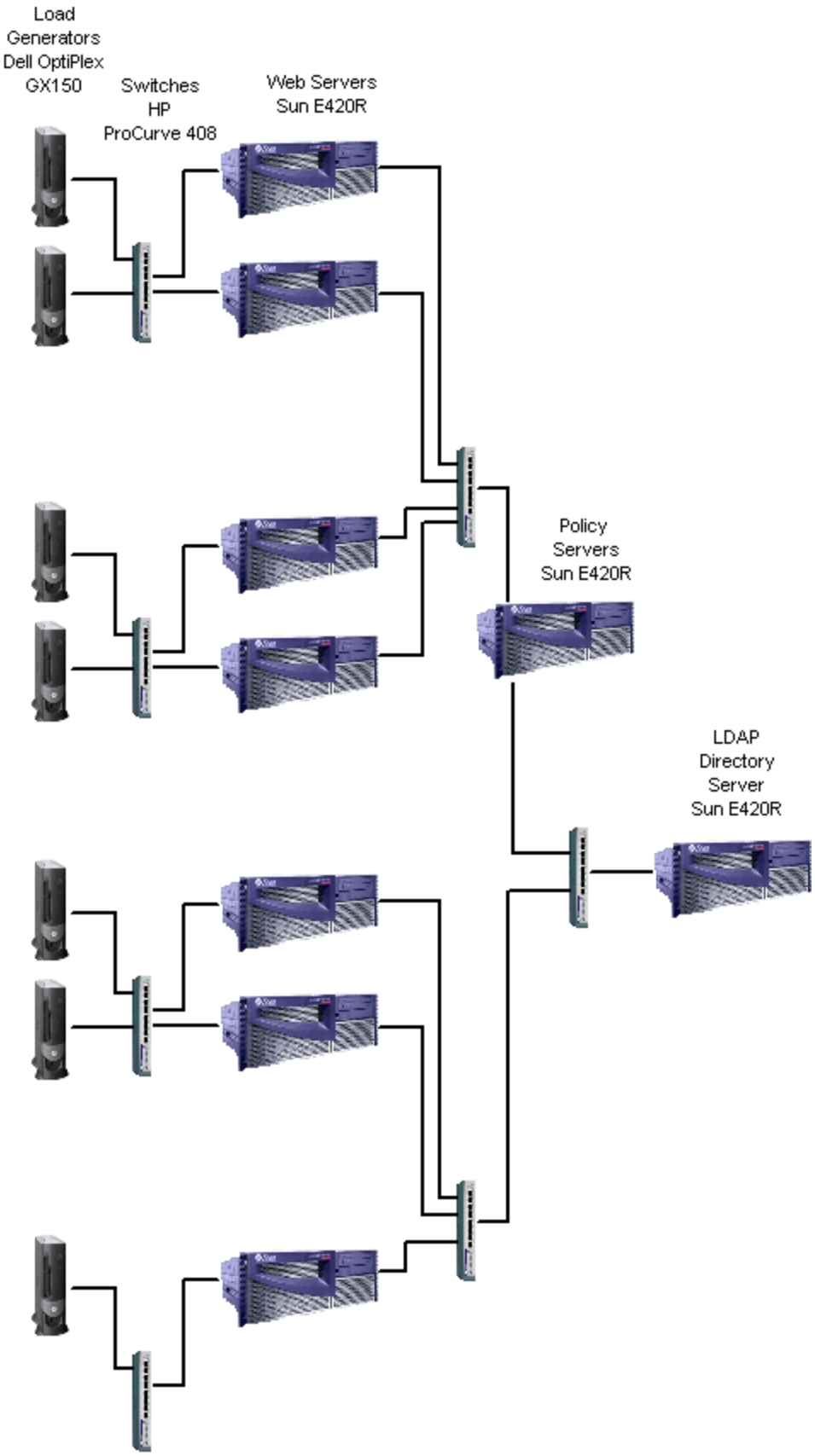

Load
Generators
Dell OptiPlex
GX150
Switches
HP
ProCurve 408
Web Servers
Sun E420R
Policy
Servers
Sun E420R
LDAP
Directory
Server
Sun E420R

Figure 4: Server Configuration for 1 Policy Server with 3 and 4 CPUs Login Test

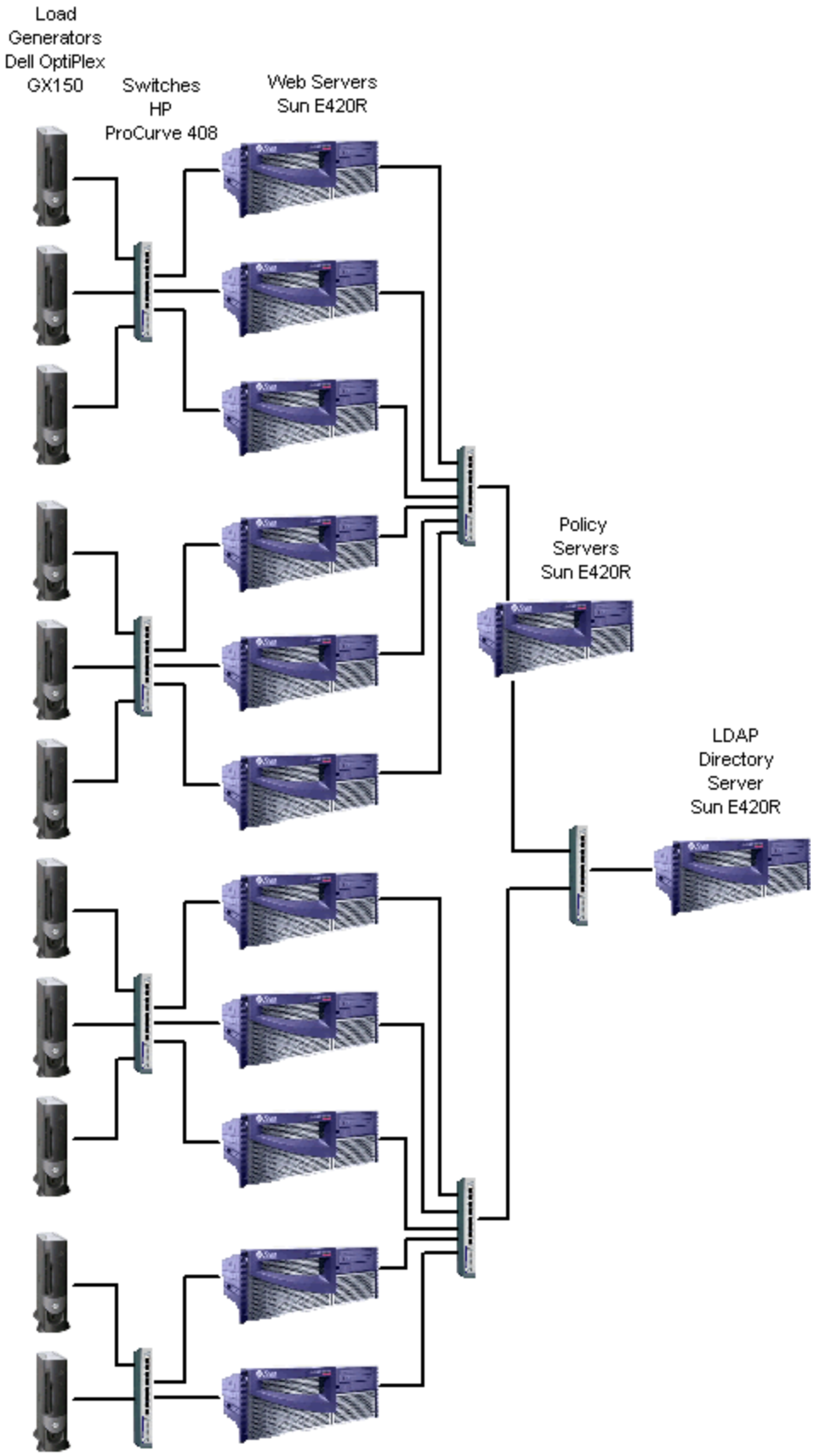
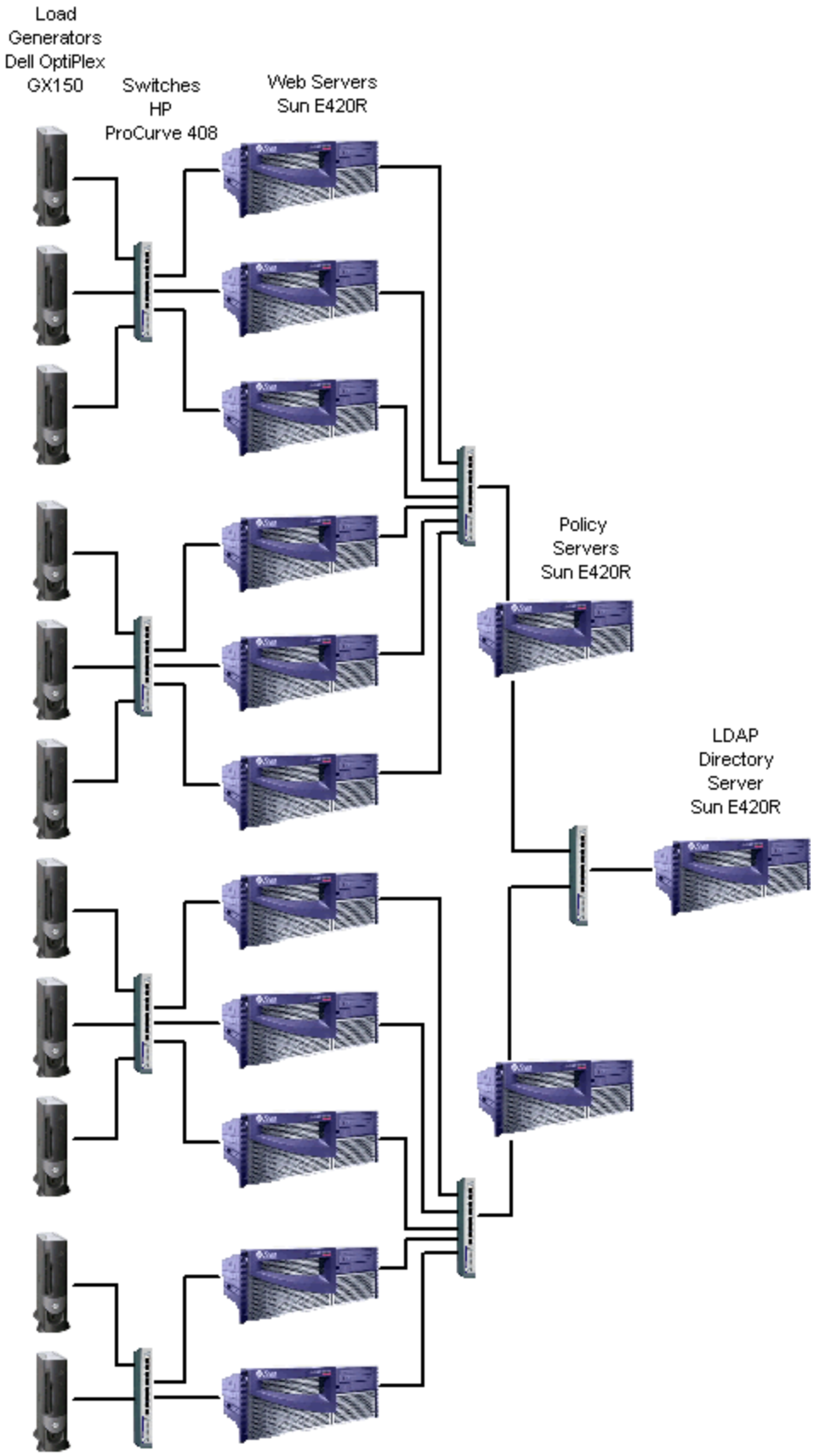

Load
Generators
Dell OptiPlex
GX150
Switches
HP
ProCurve 408
Web Servers
Sun E420R
Policy
Servers
Sun E420R
LDAP
Directory
Server
Sun E420R

Figure 5: Server Configuration for all 2-Policy Server Login and Extranet Test


Load
Generators
Dell OptiPlex
GX150
Switches
HP
ProCurve 408
Web Servers
Sun E420R
Policy
Servers
Sun E420R
LDAP
Directory
Server
Sun E420R

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
- iPlanet Directory Server 4.13
- iPlanet Web Server, Enterprise Edition 4.1 Service Pack 3
- Baltimore SelectAccess 3.1

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

- Solaris (set using ndd -set /dev/tcp on all servers):

  tcp_time_wait_interval 60000
  tcp_conn_req_max_q 1024
  tcp_conn_req_max_q0 4096
  tcp_ip_abort_interval 60000
  tcp_keepalive_interval 450000
  tcp_rexmit_interval_initial 500
  tcp_rexmit_interval_max 10000
  tcp_rexmit_interval_min 3000
  tcp_smallest_anon_port 1024
  tcp_slow_start_initial 2
  tcp_xmit_hiwat 32768
  tcp_recv_hiwat 32768
  tcp_deferred_ack_interval 5
  tcp_wscale_always 1

- Baltimore SelectAccess 3.1

Cached user names, passwords, and policies (only one policy was used). Cache grows dynamically as needed.

Client Load Generator Systems

For all of the tests, we used Dell OptiPlex GX 150 client load generator systems configured as shown in Table 5.

Table 5: Client Load Generator Systems Configuration

Feature	Configuration
System	Dell OptiPlex GX 150, 1 x 1 GHz Pentium III CPU
RAM	256 MB SDRAM
Disk	1 x 10 GB ATA/100
Networks	1 x 100Base-TX (integrated 3Com 3C920)
Operating System	Microsoft Windows 2000 Professional, Service Pack 1

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