



Oblix NetPoint 4.0 AuthMark Performance Details

By **Bruce Weiner**
([PDF version](#), 410 KB)

October 18, 2000

Contents

- ▶ [Executive Summary](#)
- ▶ [Test Methodology](#)
 - [iLOAD MVP](#)
 - [AuthMark](#)
- ▶ [Result Analysis](#)
- ▶ [Server Hardware](#)
- ▶ [Server Software](#)
- ▶ [Client Test Systems](#)

Test Methodology

Mindcraft[®] tested the performance of Oblix NetPoint 4.0 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 NetPoint 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 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 used to test NetPoint). 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 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.

NetPoint 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 will analyze the performance characteristics of Obliv NetPoint 4.0 including its performance scalability with different server configurations.

1,000,000 User Login Performance

The NetPoint Access Server is the control point for all authentication and authorization. Our tests were structured to push the Access Server systems as close as possible to 100% CPU utilization. [Table 2](#) summarizes the Login Scenario performance as a function of the NetPoint Access 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.

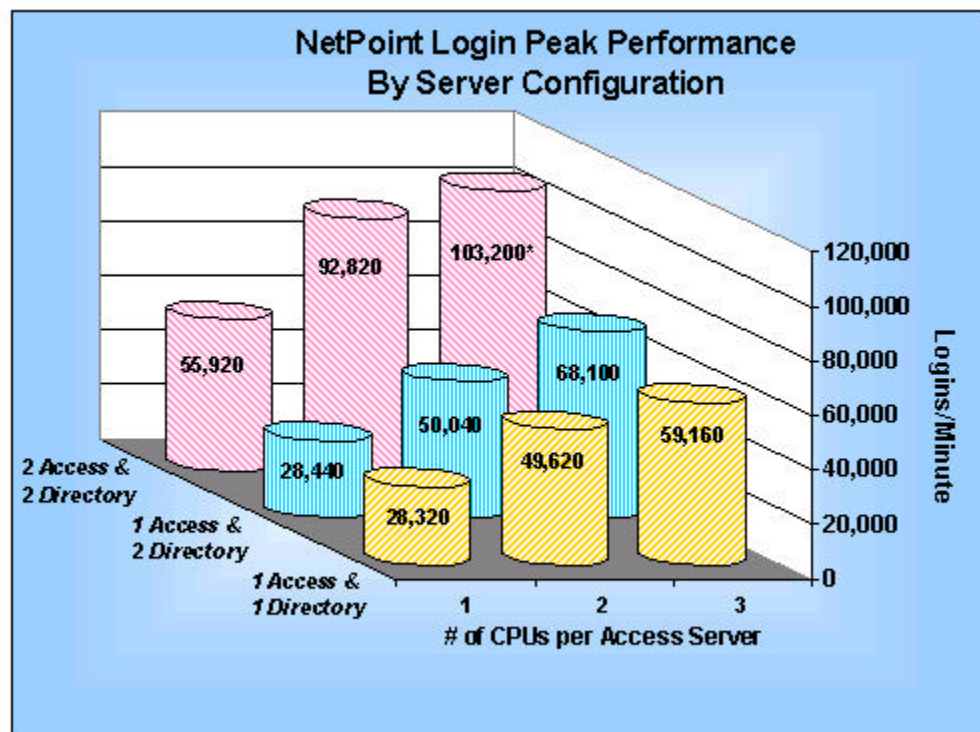
Table 2: NetPoint Login Performance Scalability - 1,000,000 User Database

NetPoint Access Server Configuration	#Directory Servers	Logins per Second	Logins per Minute	Scaling Factor
1 system, 1 CPU	1	472	28,320	Baseline
1 system, 2 CPUs	1	827	49,620	1.8
1 system, 3 CPUs	1	986	59,160	2.1
1 system, 1 CPU	2	474	28,440	1.0
1 system, 2 CPUs	2	834	50,040	1.8
1 system, 3 CPUs	2	1,135	68,100	2.4
2 systems, 1 CPU	2	932	55,920	2.0
2 systems, 2 CPUs	2	1,547	92,820	3.3
2 systems, 3 CPUs	2	1,720*	103,200*	3.6*

* - There were not enough Web servers available in the lab to fully utilize the CPUs in the NetPoint Access Servers.

Figure 1 shows NetPoint's performance from Table 2 by server configuration, which are grouped by rows of the same color.

Figure 1: NetPoint Login Scalability for a 1,000,000 User Database



The server CPU utilization during the tests will give you insight into how to configure an environment to get the maximum performance from NetPoint. Table 3 shows the CPU utilization on each of the servers for each Access Server configuration. For the test of the configuration with two Access Servers with three CPUs, the last entry in Table 3, there were not enough Web servers available in the lab to fully utilize the CPUs in the NetPoint

Access Servers.

The LDAP directory servers showed no disk activity because they were able to cache user information in memory.

Table 3: NetPoint Login Scenario CPU Utilization - 1,000,000 Users

NetPoint Access Server Configuration	Access Server(s) CPU Utilization	Web Servers CPU Utilization	LDAP Server(S) CPU Utilization
1 system, 1 CPU	100%	15%	1 server: 50%
1 system, 2 CPUs	100%	35%	1 server: 75%
1 system, 3 CPUs	90%	40%	1 server: 85%
1 system, 1 CPU	100%	20%	2 servers: 25%
1 system, 2 CPUs	98%	40%	2 servers: 35%
1 system, 3 CPUs	98%	55%	2 servers: 55%
2 systems, 1 CPU	100%	65%	2 servers: 50%
2 systems, 2 CPUs	98%	75%	2 servers: 70%
2 systems, 3 CPUs	75%	90%	2 servers: 75%

1,000,000 User Extranet Performance

[Table 4](#) compares the NetPoint Extranet and Login Scenario performance for a configuration with two Access Servers each having one CPU. The results in Table 4 demonstrate that the NetPoint Access Server performs authorizations 60% faster than authentications. The Extranet Scenario, because it uses a more realistic mix of operations than the Login Scenario, provides a better basis for capacity planning purposes.

Table 4: NetPoint Login and Extranet Performance Comparison

Measurement	Extranet Scenario	Login Scenario
Authentications/minute	16,260	55,920
Authorizations/minute	162,600	55,920
Total operations/minute	178,860	111,840

[Table 5](#) compares the CPU utilization of each server for the Extranet Scenario to those for the Login Scenario. In the Extranet Scenario notice that the Web server CPU utilization is 80%, up from 65% for the Login Scenario. This is because the NetPoint WebGate, which runs on the Web servers, offloads some of the authorization function from the Access Servers and because of the higher operation rate. The lower LDAP server CPU utilization for the Extranet Scenario occurs because fewer authentications are done, which reduces the need to get information from the LDAP servers.

Table 5: NetPoint Extranet vs. Login Scenario CPU Utilization - 2 servers, 1 CPU each

AuthMark Scenario	Access Servers CPU Utilization	Web Servers CPU Utilization	LDAP Servers CPU Utilization
Extranet	90%	80%	2 servers: 15%
Login	100%	65%	2 servers: 50%

Conclusions

These test results lead us to conclude that:

- Obliv NetPoint delivers the best login and Extranet performance of any product we have tested to date.
- NetPoint's authentication performance scales almost linearly with the number of CPUs and Access Servers.
- NetPoint's authorization performance is outstanding, exceeding its authentication performance by 60%.
- NetPoint's performance can be maximized by using one or more fast directory servers and enough Web servers to support the authentication and authorization performance you want to achieve.

Hardware Configurations Tested

Mindcraft used Sun Enterprise 450 servers for the Web servers, NetPoint Access Servers and the LDAP directory server. [Table 6](#) shows the server configurations we used.

Table 6: Sun Enterprise 450 Configurations

Feature	Configuration
CPU	4 x 400 MHz UltraSPARC II (we used the psradm command to enable/disable processors) Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	4 GB ECC
Disk	Web servers : 2 x 9 GB SCSI; one for Solaris and one for the Web data NetPoint Access Servers : 2 x 9 GB SCSI; one for Solaris and one for NetPoint LDAP directory server : 1 x 9 GB SCSI for Solaris; 1 x 9 GB SCSI for LDAP log file; directory was on a Sun A5200 in split loop mode, each LDAP server had 2 Fibre Channel loops, each loop had 11 Fibre channel disks in a RAID 10 configuration with a 64KB stripe size (a total of 44 x 9GB 10,000 RPM disks)
Networks	2 x 100Base-TX NICs (Web and NetPoint servers) 1 x 100Base-TX integrated NIC (LDAP server)

[Figure 2](#) shows how the various servers were connected to each other for the tests using one Access Server and one LDAP directory server. [Figure 3](#) gives the server connections for the tests using one Access Server and two LDAP directory servers. [Figure 4](#) gives the server connections for the tests using two Access Servers and two LDAP directory servers. All of the systems were connected using Cisco Catalyst 2900 XL 100Base-TX switches.

Figure 2: Server Configuration for 1 Access Server, 1 LDAP Server Tests

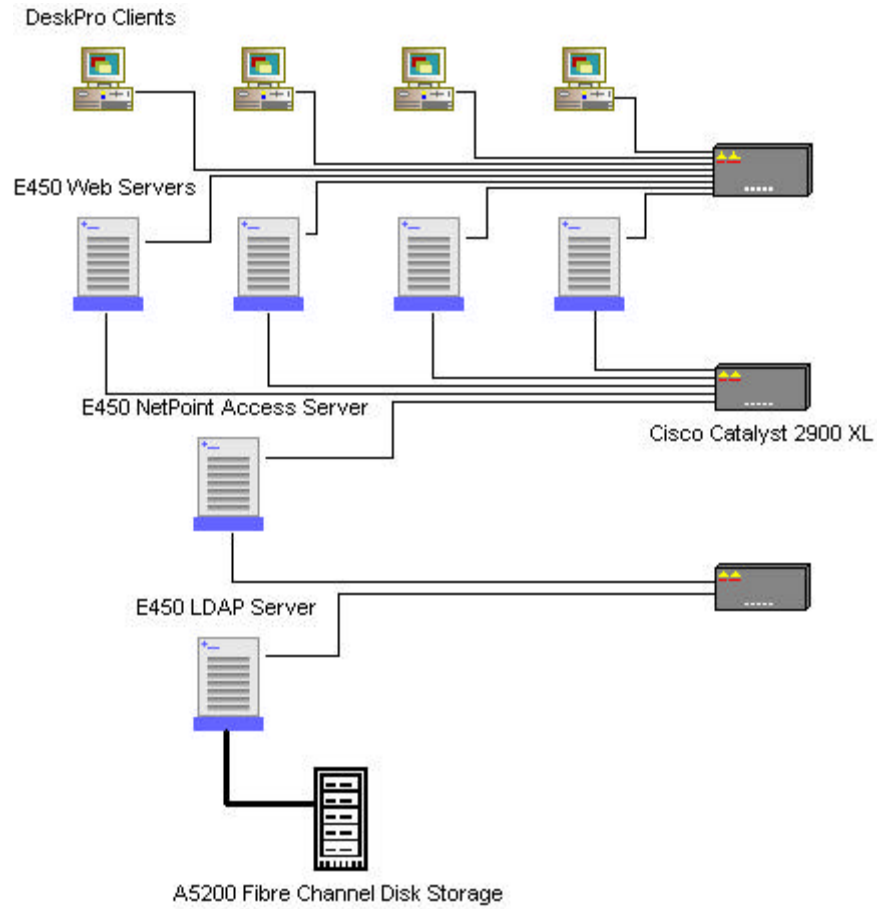


Figure 3: Server Configuration for 1 Access Server, 2 LDAP Servers Tests

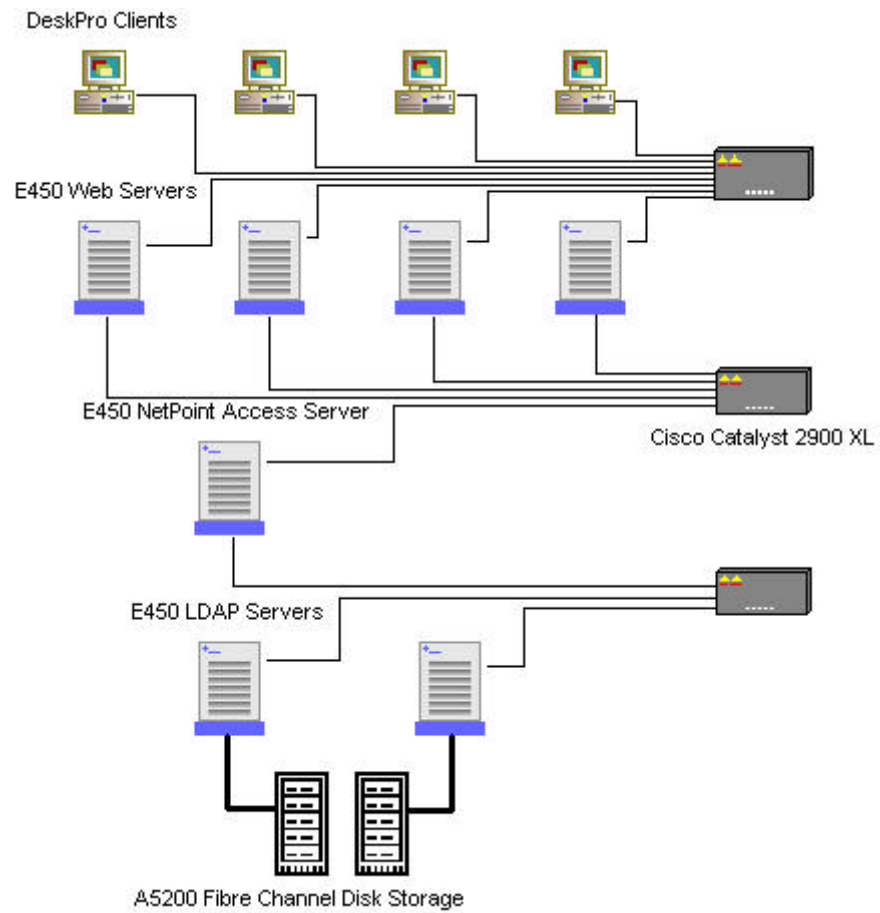
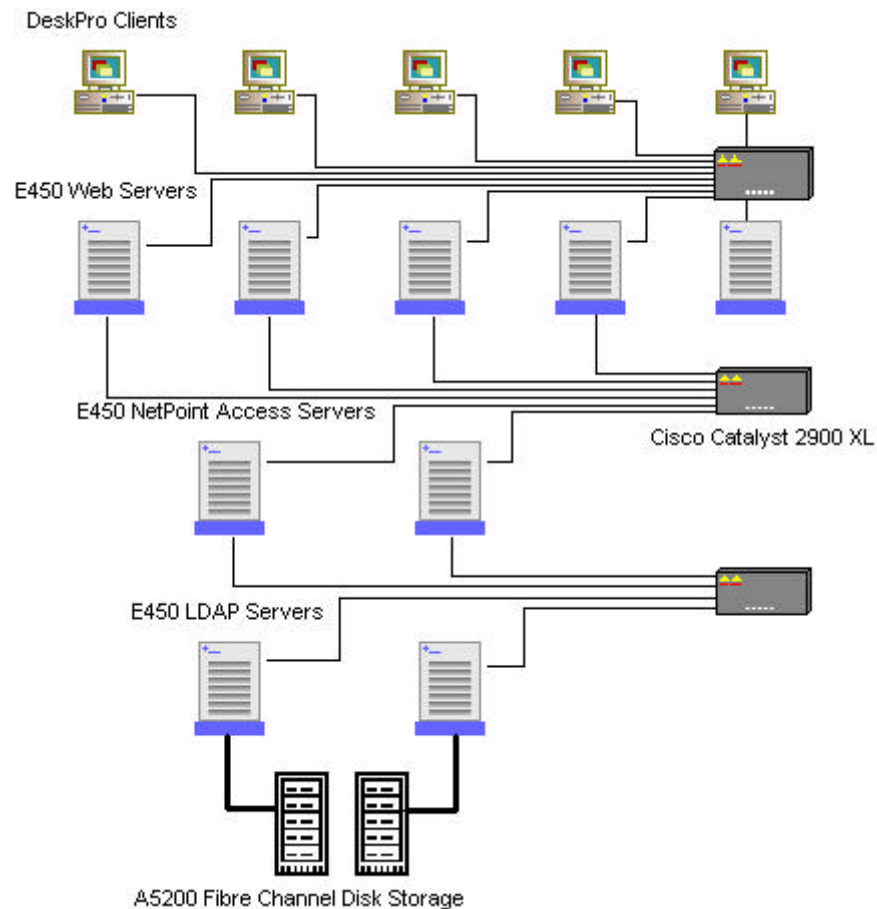


Figure 4: Server Configuration for 2 Access Servers, 2 LDAP Servers Tests



Server Software Configuration and Tuning

We used the following server software for these benchmark tests:

- Solaris 7 on the Sun E450 servers
- Netscape Directory Server 4.12
- iPlanet Web Server, Enterprise Edition 4.1 SP3
- Oblix NetPoint 4.0

All software ran with default settings except for the following:

- For Solaris 7:
 - Installed patches:
 - 106327-08, 106541-10, 106725-02, 106793-03, 106934-03,
 - 106944-02, 106952-01, 106960-01, 106978-09, 106980-11,
 - 107022-06, 107038-01, 107115-03, 107171-05, 107259-01,
 - 107337-01, 107359-02, 107451-02, 107454-04, 107456-01,
 - 107544-03, 107587-01, 107636-03, 107684-01, 107709-04,
 - 107792-02, 107885-06, 107887-08, 107893-05, 107972-01,
 - 108219-01, 108221-01, 108301-01, 108343-02, 108374-02,
 - 108482-01, 108484-01, 108662-01, 108721-01
- For Netscape Directory Server:
 - Change in slapd.ldbm.conf:

```
directory /ldap-db/B2B [on the Fibre Channel disks]
lookthroughlimit 10000
allidsthreshold 5000
cachesize 110000
dbcachesize 1000000000
db_home_directory /tmp/B2B
-- modify this index to:
index uid pres,eq,sub
-- add these indexes:
index obclass eq
index obname eq
index obuseraccountcontrol pres,eq
index ou eq,sub
index o pres,eq
index obapp eq
index obattr pres,eq
```

Changes in slapd.conf:

```
errorlog "/ldap-log/B2B/errors"
accesslog "/ldap-log/B2B/access"
auditfile "/ldap-log/B2B/audit"
timelimit 600
sizelimit 10000
```

Added these lines to the beginning of start-slapd:

```
dbhomedirectory="/tmp/B2B5M"
if (( test ! -w $dbhomedirectory || test ! -d $dbhomedirectory )) then
    mkdir $dbhomedirectory
    chown ldap:ldap $dbhomedirectory
fi
mkdir /ldap-log/B2B5M
chown ldap:ldap /ldap-log/B2B5M
```

- For NetPoint Access Server:

We used the default NetPoint Access Server cache configuration - a 100,000 user cache with a 30 minute timeout and a 10,000 entry policy cache with a two hour timeout. There is no cache in the NetPoint WebGate Web server plug-in.

Client Test Systems

For all of the tests, we used the Compaq DeskPro client test systems configured as shown in [Table 7](#).

Table 7: Client Test Systems Configuration

Feature	Configuration
System	Compaq DeskPro, 1 x 600 MHz Pentium III CPU
RAM	256 MB SDRAM
Disk	1 x 6 GB SCSI
Networks	1 x 100Base-TX (3 x 3Com 3C905D, 3Com 3C905, Intel Pro/100+ Management Adapter)
Operating System	Microsoft Windows NT 4.0 Workstation, Service Pack 5

NOTICE:

The information in this publication is subject to change without notice.

MINDCRAFT, INC. SHALL NOT BE LIABLE FOR ERRORS OR OMISSIONS CONTAINED HEREIN, NOR FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE FURNISHING, PERFORMANCE, OR USE OF THIS MATERIAL.

This publication does not constitute an endorsement of the product or products that were tested. This test is not a determination of product quality or correctness, nor does it ensure compliance with any federal, state or local requirements.



Services Benchmarks Reports Price/Performance Company

Search Contact Us

Copyright © 2000. Mindcraft, Inc. All rights reserved.

Mindcraft is a registered trademark of Mindcraft, Inc.

Product and corporate names mentioned herein are trademarks and/or registered trademarks of their respective owners.

For more information, [contact us](mailto:info@mindcraft.com) at: info@mindcraft.com

Phone: +1 (408) 395-2404

Fax: +1 (408) 395-6324