



Netegrity SiteMinder 4.61 with Microsoft Active Directory AuthMark Performance Details

By Bruce Weiner

([PDF version](#), 131 KB)

April 18, 2002

Contents

- [Executive Summary](#)
- [Login Results](#)
- [Extranet Results](#)
- [Conclusions](#)
- [Test Methodology](#)
 - [iLOAD MVP](#)
 - [AuthMark](#)
- [Server Set Up](#)
- [Load Generators](#)

This part of the white paper details the [Login](#) and [Extranet](#) Scenario performance characteristics of Netegrity SiteMinder 4.61 SP2 with Microsoft Active Directory.

Detailed Login Results

[Table 1](#) summarizes the Login Scenario performance as a function of the SiteMinder Policy Server configuration and the number of entries in the directory. All of the Login Scenario tests used one Policy Server; only the number of CPUs was varied as shown in Table 1.

Disclosure

Netegrity sponsored the testing in this report. Mindcraft, Inc. conducted the performance tests described in this report at Microsoft's test lab in Redmond, Washington.

The SiteMinder Policy Server is the control point for all authentication and authorization. Our tests were structured to push the Policy Server system as close as possible to 100% CPU utilization. The *CPU Utilization by Server Type* column in Table 1 shows that the SiteMinder Policy Server was performing at its maximum. Except for the Login 1 test, all user credentials for the entries tested were cached in the SiteMinder Policy Server, which accounts for the Active Directory (AD) server CPU having been idle during the tests. At the same time, the Web server CPUs had plenty of performance left in them, so they were not performance bottlenecks for the tests. The load generator (LG) systems were sufficient to create a workload on the servers that drove the Policy Server to its peak performance.

Each of the three networks (load generators to Web servers, Web servers to Policy Servers, and Policy Servers to directory servers) had enough bandwidth available that they were able to support the highest load without limiting overall performance.

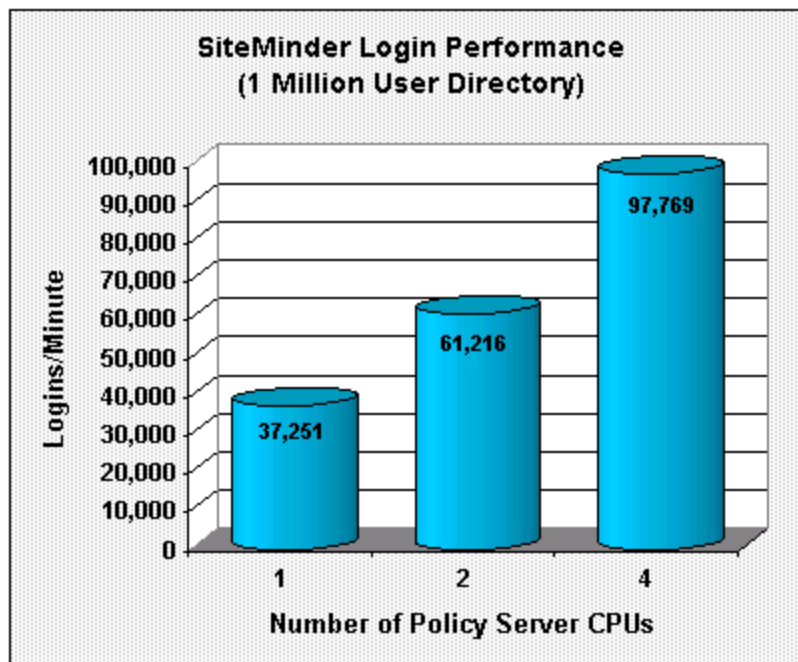
Table 1: SiteMinder 4.61 Login Performance

Test ID	Directory Size (# entries tested)	Logins/Minute	Logins/Minute/Total CPUs	Logins/Minute/Policy Server CPU	Full Cache Enabled?	Number of CPUs by Server Type	CPU Utilization by System Type
Login 1	1 Million (100,000 tested)	19,074	2,725	19,074	No	Policy: 1 Web: 4 AD: 2 Total: 7	Policy: 95% Web: 40% AD: 76% LG: 29%
Login 2	1 Million (100,000 tested)	37,251	6,209	37,251	Yes	Policy: 1 Web: 4 AD: 1 Total: 6	Policy: 100% Web: 63% AD: 0% LG: 53%
Login 3	1 Million (100,000 tested)	61,216	5,565	30,608	Yes	Policy: 2 Web: 8 AD: 1 Total: 11	Policy: 98% Web: 58% AD: 0% LG: 76%
Login 4	1 Million (100,000 tested)	97,769	6,518	24,442	Yes	Policy: 4 Web: 10 AD: 1 Total: 15	Policy: 87% Web: 78% AD: 0% LG: 88%
Login 5	20 Million (1,000,000 tested)	81,586	4,079	20,397	Yes	Policy: 4 Web: 12 AD: 4 Total: 20	Policy: 95% Web: 53% AD: 0% LG: 78%

The Login 1 and 2 tests show the performance benefit that caching user credentials can bring. The two test configurations are identical except for the use of a second CPU in the Active Directory server for the Login 1 test; we needed to add this CPU in order to maximize the Policy Server performance. You can see that enabling caching in the Login 2 test increases performance 1.95 times that of the Login 1 test.

The Login 2, 3, and 4 tests (the gray shaded rows in Table 1) show how SiteMinder's performance scales as Policy Server CPUs are added. Going from one to two Policy Server CPUs in the Login 3 test improves performance 1.64 times over that in the Login 2 test. The Login 4 test uses four Policy Server CPUs and improves performance 2.62 times over the single CPU Login 2 test. As we added Policy Server CPUs, we also needed to add Web servers to create a load that maximized the performance of the Policy Server. [Figure 1](#) shows SiteMinder's performance for the Login 2, 3, and 4 tests by the number of Policy Server CPUs.

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



The Login 5 test used a directory with 20 million entries in it and tested 1 million active users. Comparing the performance for the Login 5 test with that of the Login 4 test, which used a 1 million-entry directory and tested only 10% of the number of active users used for the Login 5 test, you can see that SiteMinder continues to deliver high performance even as the number of active users increases by a factor of 10.

Detailed Extranet Results

The Extranet Scenario simulates customers or suppliers logging into a private Web site and obtaining information they are authorized to receive. It measures the combination of one user authentication and 10 authorizations for access to resources (these 11 operations constitute one *Extranet sequence*). We report the total operations per minute, which is 11 times the number of Extranet sequences. The Extranet Scenario, because it uses a more realistic mix of operations than the Login Scenario, provides a better basis for comparing access control and identity management solutions. You can find a more complete description of the [Extranet Scenario](#) below.

The Extranet test was done with SiteMinder configured to cache user credentials, as one would do if the servers were on the inside of a private network with firewalls to protect access to systems that store passwords and other sensitive information. We call this a *full-cache* configuration.

[Table 2](#) shows the Extranet Scenario performance metrics and CPU utilizations for each type of system. We used a single directory server with one CPU for this test. The Active Directory server CPU was essentially idle during the tests because we used a full-cache configuration.

Table 2: SiteMinder 4.61 Extranet Performance

Directory Size (# entries tested)	Extranet Operations/Minute	Extranet Operations/Minute/Total CPU	Extranet Operations/Minute/Policy Server CPU	Number of CPUs by Server Type	CPU Utilization by System Type
1 Million (100,000 tested)	161,192	11,514	161,192	Policy: 1 Web: 12 AD: 1 Total: 14	Policy: 46% Web: 72% AD: 0% LG: 87%

Conclusions

The benchmark results lead us to conclude that:

- SiteMinder 4.61 with Microsoft Active Directory sets the per CPU performance standard for 1,000,000-user directories against which other Windows 2000 Policy Server-based products will be measured.
- SiteMinder 4.61 on Microsoft Windows 2000 using Active Directory demonstrates the performance required to support 20,000,000 users.
- The SiteMinder 4.61 Policy Server on Windows 2000 delivers outstanding scalability across four processors.

Test Methodology

Mindcraft® tested the performance of SiteMinder with Active Directory using our [iLOAD MVP™](#) tool to run the [AuthMark™](#) Benchmark [Login](#) and [Extranet](#) Scenarios. We describe these tests in this section to further your understanding of the performance results discussed above.

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.
- Multithreaded 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.

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

Login Scenario Configuration

[Table 3](#) shows the AuthMark Login Scenario configuration parameters we used.

Table 3: AuthMark Login Scenario Configuration Parameters

Parameter	Values	
Number of users in the directory	1,000,000	20,000,000
Number of Organizational Units or security groups	10	200
Total number of user sessions per test	100,000	1,000,000

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:

- A. 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.
- B. Load the security database with the user data.
- C. 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).
- D. 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.
- E. Load and configure the user management system or authentication/authorization system.
- F. Run the benchmark.

The Login Scenario test script selects users randomly from the user database (see [Table 3](#) for the numbers we used for this test). The tester is free to select the number of load generator 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 peak performance, the tester may need to use multiple Web servers and directory 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 each test script in its entirety.

Extranet Scenario

The Extranet Scenario simulates an environment where users must login to a Web site and where all access requests require authorization. This scenario depicts a 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 - 8 above) and continues with the following operations:

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

The Extranet Scenario sequence consists of a total of 11 client operations per user session:

- The first resource request (which does two operations): the login request and the authorization for resource requested; and
- Nine more resource requests that require authorization.

SiteMinder checks the continuing validity of an 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.

For the Extranet Scenario, we warmed-up the servers by running the test script in its entirety.

Extranet Scenario Configuration

[Table 4](#) shows the AuthMark Extranet Scenario configuration parameters we used.

Table 4: AuthMark Extranet Scenario Configuration Parameters

Parameter	Values
Number of users in the directory	1,000,000
Number of OrganizationalUnits or security groups	10
Total number of user sessions per test	100,000

Sessions are not logged out once created. Instead, each session remains quiescent after all of its requests have been satisfied.

Running the Extranet Scenario

The basic steps for running the Extranet Scenario are:

1. Generate the data to fill the directory. iLOAD MVP provides a tool to generate realistic data for the LDAP V3 organizationalPerson object class and Netscape's inetOrgPerson object class. It generates the data in standard LDIF format so that it can be loaded directly into an LDAP directory
2. Load the directory with the user data.
3. Generate the test scripts for the Extranet Scenario. iLOAD MVP provides a tool to do this. These scripts drive the iLOAD clients to simulate user interactions with the Web servers.
4. Load Web pages on the Web servers. There are 100 Web pages each of which is 14 KB in size.
5. Load and configure the authentication/authorization system.
6. Run the benchmark.

The Extranet Scenario test scripts select users randomly from the user directory (see [Table 4](#) for the numbers we used for these tests). The tester is free to use any number of load generator systems each running any number of iLOAD MVP client threads (called *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, the tester may need to use multiple Web servers and directory servers.

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

Server Hardware and Software Set Up

Mindcraft used three types of servers for these tests: Web, Policy and Active Directory servers. [Table 5](#) shows the summary of the server configurations we used for each test. The detailed configurations of the SiteMinder Policy and Active Directory servers are shown in [Table 6](#) and [Table 7](#), respectively. [Tables 8](#) and [9](#) show the Web server configurations. [Figure 2](#) shows how the various servers were connected for the tests; however, you will need to refer to [Table 5](#) to see which systems were used for each test.

For half of the tests we used a Gigaset cLAN CL5300 30-port 1.25Gb/s switch and the associated CL1000 1.25Gb/s Host Bus Adapters for the network between the Web servers and the Policy Server. However, part way through our testing the CL5300 failed. So, we changed to an HP ProCurve 1600m 16-port 100Base-TX switch and used the 100Base-TX NICs in the servers for the Login 4, Login 5, and Extranet tests.

Table 5: Servers and CPUs

Test ID	Web Servers & CPUs	Policy Server & CPUs	Active Directory Server & CPUs	Load Generators
Login 1	2 x HP NetServer It 6000r. 2 CPUs each	1 x HP NetServer lxr 8500, 1 CPU	1 x HP NetServer lxr 8500, 2 CPUs	Dell Optiplex GX400, Dell Optiplex GX50, IBM NetVista 6578RAU, & HP Workstation x2000
Login 2	2 x IBM eServer xSeries 330. 2 CPUs each	1 x HP NetServer lxr 8500, 1 CPU	1 x HP NetServer lxr 8500, 1 CPU	Dell Optiplex GX400, Dell Optiplex GX50, IBM NetVista 6578RAU, & HP Workstation x2000
Login 3	2 x IBM eServer xSeries 330 & 2 x HP NetServer It 6000r. 2 CPUs each	1 x HP NetServer lxr 8500, 2 CPUs	1 x HP NetServer lxr 8500, 1 CPU	Dell Optiplex GX400, Dell Optiplex GX50, IBM NetVista 6578RAU, & HP Workstation x2000
Login 4	2 x IBM eServer xSeries 330 & 3 x HP NetServer It 6000r. 2 CPUs each	1 x HP NetServer lxr 8500, 4 CPUs	1 x HP NetServer lxr 8500, 1 CPU	Dell Optiplex GX400, Dell Optiplex GX50, IBM NetVista 6578RAU, HP Workstation x2000, & Dell PowerEdge 6350/550
Login 5	2 x IBM eServer xSeries 330 & 4 x HP NetServer It 6000r. 2 CPUs each	1 x HP NetServer lxr 8500, 4 CPUs	1 x HP NetServer lxr 8500, 4 CPUs	Dell Optiplex GX400, Dell Optiplex GX50, IBM NetVista 6578RAU, HP Workstation x2000, & Dell PowerEdge 6350/550
Extranet	2 x IBM eServer xSeries 330 & 4 x HP NetServer It 6000r. 2 CPUs each	1 x HP NetServer lxr 8500, 1 CPU	1 x HP NetServer lxr 8500, 1 CPU	Dell Optiplex GX400, Dell Optiplex GX50, IBM NetVista 6578RAU, HP Workstation x2000, & Dell PowerEdge 6350/550

Table 6: SiteMinder Policy Server Configuration - HP NetServer lxr 8500

Feature	Configuration
CPU	4 x Intel® Pentium® III Xeon 700MHz/2M CPUs (we used the "/numproc=" option in boot.ini to enable/disable processors as specified in Table 5) Cache: L1: 16 KB I + 16 KB D; L2: 2 MB (I+D)
RAM	3.4 GB ECC
Disk	HP NetRAID adapter <ul style="list-style-type: none"> ■ 2 x HP 9.1 GB C80-D94N ■ 2 x HP 18.2 GB C80-8C42
Networks	<ul style="list-style-type: none"> ■ 1 x HP Netserver 10/100 PCI NIC ■ 1 x Gigaset CL1000 Host Bus Adapter
Software	<ul style="list-style-type: none"> ■ Windows 2000 Advanced Server, SP 2 ■ SiteMinder 4.61 SP 2
Tunes	<p>Windows 2000 Advanced Server tunes:</p> <ul style="list-style-type: none"> ■ Registry: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535 ■ OS: boot with "/3GB" switch ■ OS: disabled services, left only these running: CLan Connection Manager

	<p>COM+ Event System Crystal Web Page Server Distributed Link Tracking Client Distributed Transaction Coordinator DNS Client Event Log IIS Admin Service IPSEC Policy Agent License Logging Service Logical Disk Manager Network Connections Plug and Play Protected Storage Remote Access Connection Manager Remote Procedure Call (RPC) Remote Registry Service Removable Storage RunAs Service Security Accounts Manager Server SiteMinder Authentication Service SiteMinder Authorization Service System Event Notification TCP/IP NetBIOS Helper Service Telephony Windows Management Instrumentation Windows Management Instrumentation Driver Workstation World Wide Web Publishing Service</p> <p>SiteMinder tunes:</p> <ul style="list-style-type: none"> ■ Connections from Policy Server to Directory Server: <ul style="list-style-type: none"> ■ For Login 1 test: 8 ■ For Login 2, 3, 4 and 5 as well as Extranet tests: 4 ■ Web agent - max sockets per port: <ul style="list-style-type: none"> ■ For Login 1 test: 7 ■ For Login 2, 3, and 4 as well as Extranet tests: 2 ■ For Login 5 test: 3 ■ User cache size <ul style="list-style-type: none"> ■ For Login 1, 2, 3, and 4 as well as Extranet tests: 110,000 entries ■ For Login 5 test: 1.1 million entries ■ Session cache size <ul style="list-style-type: none"> ■ For Login 1, 2, 3, 4 and 5: 0 ■ For Extranet tests: 40,000 per Web agent
--	---

Table 7: Active Directory Server Configuration - HP NetServer lxr 8500

Feature	Configuration
CPU	4 x Intel® Pentium® III Xeon 700MHz/2M CPUs (we used the "/numproc=" option in boot.ini to enable/disable processors as specified in Table 5) Cache: L1: 16 KB I + 16 KB D; L2: 2 MB (I+D)
RAM	4 GB ECC
Disk	1 x Symbios SYM 3c86c SCSI controller connected to 2 x HP 9.10GB internal SCSI disks (C80-D94N) 1 x Mylex Extreme RAID 2000 adapter with a 15 SCSI-disk drive array, RAID 0 with a 64KB stripe, made up as follows: <ul style="list-style-type: none"> ■ 12 x IBM DMVS09D, 9.1 GB, 10000 RPM ■ 3 x Seagate ST39103LC, 9.1 GB, 10000 RPM
Networks	1 x HP Netserver 10/100 PCI NIC

Software	<ul style="list-style-type: none"> ■ Windows 2000 Datacenter Server, SP 2
Tunes	<p>Windows 2000 Datacenter Server tunes:</p> <ul style="list-style-type: none"> ■ Registry: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535 ■ OS: boot with "/3GB" switch ■ Directory: Domain in 'native' mode ■ Directory: Changed default ACLs on the user object - Removed permissions for the following groups on the default user objects: Account Operators Cert Publishers RAS and IAS servers

Table 8: Web Server A Configuration - 4 x HP NetServer It 6000r

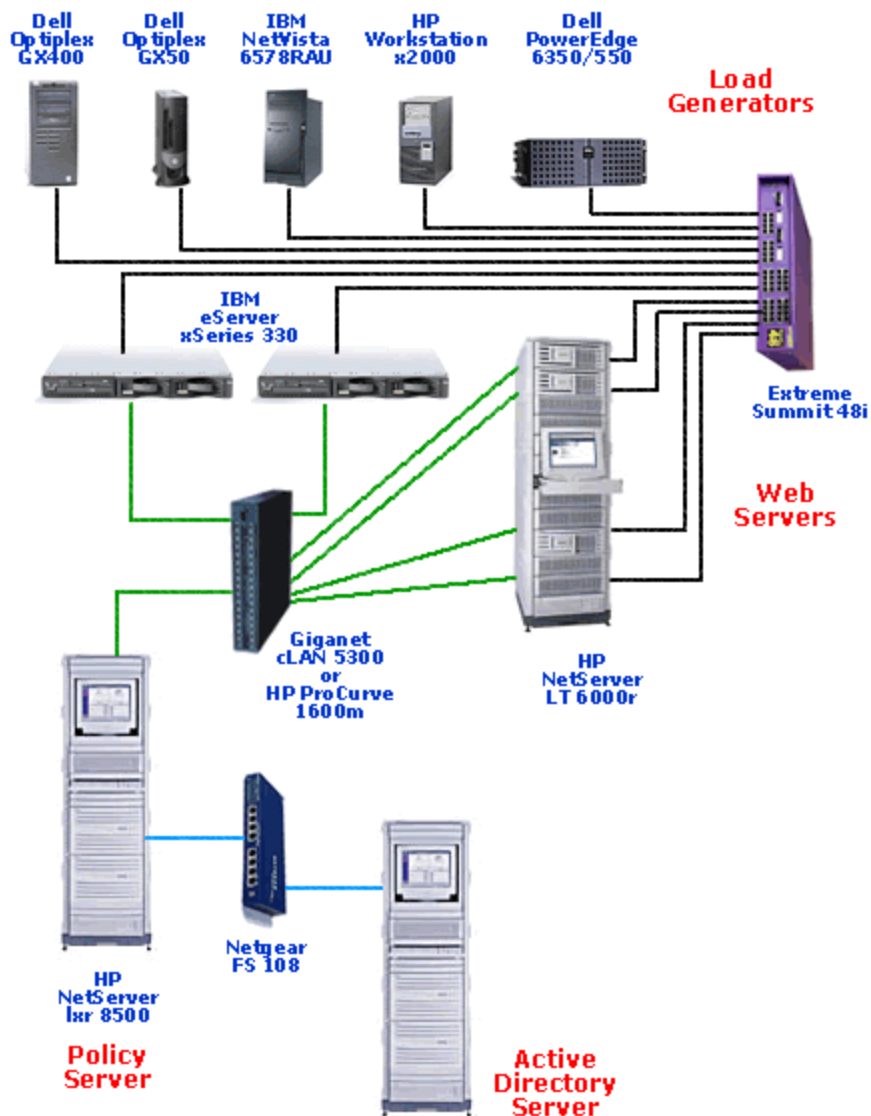
Feature	Configuration
CPU	4 x Intel® Pentium® III Xeon 700MHz/2M CPUs (we used the "/numproc=" option in boot.ini to disable 2 processors) Cache: L1: 16 KB I + 16 KB D; L2: 2 MB (I+D)
RAM	2 GB ECC; one server had 4 GB ECC
Disk	HP NetRAID adapter <ul style="list-style-type: none"> ■ 2 x HP 9.1 GB C80-D94N ■ 2 x HP 18.2 GB C80-8C42
Networks	<ul style="list-style-type: none"> ■ 1 x HP Netserver 10/100 PCI NIC ■ 1 x Gigaset cLAN CL1000 Host Bus Adapter
Software	<ul style="list-style-type: none"> ■ Windows 2000 Advanced Server, SP 2
Tunes	<p>Windows 2000 Advanced Server tunes:</p> <ul style="list-style-type: none"> ■ IIS – under "Performance" tab, set to "More than 100,000 hits per day" ■ Registry: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535 MaxFreeTWTcbs=1098000 MaxHashTableSize=65536 NumTcbTablePartitions=64 TcpTimedWaitDelay=60 ■ OS: boot with "/3GB" switch ■ For the NICs, set the following: Link speed=100mbps (default=auto) Duplex=full (default=auto) Coalesce buffers=32 (default=8) Receive buffers=768 (default=48) Transmit Control Blocks=64 (default=32)

Table 9: Web Server B Configuration - 2 x IBM eServer xSeries 330

Feature	Configuration
CPU	2 x Intel® Pentium® III 1128MHz CPUs Cache: L1: 16 KB I + 16 KB D; L2: 512 KB (I+D)
RAM	3.8 GB ECC

Disk	1 x Adaptec AIC 7892 Ultra 160/m PCI SCSI controller connected to 2 x 36.4 IBM ST336605LC SCSI disks
Networks	<ul style="list-style-type: none"> ■ 2 x IBM Netfinity Ethernet NICs ■ 1 x Giganet cLAN CL1000 Host Bus Adapter
Software	<ul style="list-style-type: none"> ■ Windows 2000 Advanced Server, SP 2
Tunes	<p>Windows 2000 Advanced Server tunes:</p> <ul style="list-style-type: none"> ■ IIS – under “Performance” tab, set to “More than 100,000 hits per day” ■ Registry: <ul style="list-style-type: none"> HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535 MaxFreeTWTcbs=1098000 MaxHashTableSize=65536 NumTcbTablePartitions=64 TcpTimedWaitDelay=60 ■ OS: boot with “/3GB” switch ■ For the NICs, set the following: <ul style="list-style-type: none"> Link speed=100mbps (default=auto) Duplex=full (default=auto) Coalesce buffers=32 (default=8) Receive buffers=768 (default=48) Transmit Control Blocks=64 (default=32)

Figure 2: Test Lab Configuration
(Some servers are not used for all tests. See [Table 5](#) for details)



Load Generator Systems

We used a variety of load generator systems for these tests. Figures [2](#) and [3](#) show the specific load generator systems we used for each test. Tables 11 through 15 detail the configuration for each of the load generator systems.

Table 11: Dell Optiplex GX400 Configuration

Feature	Configuration
CPU	1 x Intel® Pentium® 4 1.8 GHz CPU Cache: L1: 12 KB I + 8 KB D; L2: 256 KB (I+D)
RAM	256 MB RDRAM
Disk	1 x Western Digital WDC WD200BB-75CLB0 19GB IDE disk
Networks	1 x 3Com Integrated Fast Ethernet (3C920)
Operating System	Microsoft Windows 2000 Professional, SP2
Tunes	Windows 2000 tunes: <ul style="list-style-type: none"> ■ Registry: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535

Table 12: Dell Optiplex GX50 Configuration

Feature	Configuration
CPU	1 x Intel® Pentium® III 900MHz CPUs Cache: L1: 16 KB I + 16 KB D; L2: 256 KB (I+D)
RAM	128 MB SDRAM
Disk	1 x 9.5 GB 1C35L010AVER07-0 IDE disk
Networks	1 x 3Com Integrated Fast Ethernet (3C920)
Operating System	Microsoft Windows 2000 Professional, SP2
Tunes	Windows 2000 tunes: <ul style="list-style-type: none"> ■ Registry: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535

Table 13: IBM NetVista 6578RAU Configuration

Feature	Configuration
CPU	1 x Intel® Pentium® III 930MHz CPUs Cache: L1: 16 KB I + 16 KB D; L2: 256 KB (I+D)
RAM	128 MB SDRAM
Disk	1 x 19 GB Quantum Fireball ICT15 20 IDE disk
Networks	1 x Intel PRO/100 VE Desktop NIC
Operating System	Microsoft Windows 2000 Professional, SP2
Tunes	Windows 2000 tunes: <ul style="list-style-type: none"> ■ Registry: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535

Table 14: HP Workstation x2000 Configuration

Feature	Configuration
CPU	1 x Intel® Pentium® 4 1.4 GHz CPU Cache: L1: 12 KB I + 8 KB D; L2: 256 KB (I+D)
RAM	128 MB SDRAM
Disk	1 x 19.5 GB IDE disk
Networks	1 x Intel PRO/100+ NIC
Operating System	Microsoft Windows 2000 Professional, SP2
Tunes	Windows 2000 tunes: <ul style="list-style-type: none"> ■ Registry: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535

Table 15: Dell PowerEdge 6350/550 Configuration

Feature	Configuration
CPU	4 x Intel® Pentium® III Xeon 550MHz CPUs Cache: L1: 16 KB I + 16 KB D; L2: 512 KB (I+D)
RAM	2 GB ECC
Disk	Dell PERC2 RAID Controller <ul style="list-style-type: none"> ■ 2 x Quantum Atlas 8.4 GB disks ■ 1 x IBM DDYS-T18350 16.9 GB disk
Networks	2 x Intel PRO/100+ Server Adapter (one was disabled)
Operating System	Microsoft Windows 2000 Advanced Server
Tunes	Windows 2000 tunes: <ul style="list-style-type: none"> ■ Registry: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters MaxUserPort=65534 TcpWindowSize=65535

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.

Mindcraft is a registered trademark of Mindcraft, Inc.

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



[Services](#) [Benchmarks](#) [Reports](#) [Price/Performance](#) [Company](#)

[Search](#) [Contact Us](#)

Copyright © 2002. 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