



# IBM Tivoli Access Manager for e-business v3.8 AuthMark Performance Details

By **Bruce Weiner**

([PDF version](#), 171 KB)

April 9, 2002

[Update](#) to the February 15, 2002 version

## Contents

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

## Disclosure

Tivoli sponsored the testing in this report. Mindcraft, Inc. conducted the performance tests described in this report at Tivoli's test lab in Santa Cruz, California.

IBM Tivoli Access Manager for e-business v3.8 sets new Extranet performance records. Mindcraft's tests show:

- For a 1,000,000-user directory, Tivoli Access Manager delivered up to 553,245 [Extranet](#) operations/minute, the highest [full-cache](#) performance we've measured by 52%.
- For a 1,000,000-user directory, Tivoli Access Manager delivered 19,732 Extranet operations/minute/CPU on a test bed with 25 CPUs, over 67% higher per-CPU performance on Sun servers than any other full-cache test we've done.

The [Test Methodology](#) section below describes how we tested the performance of Tivoli Access Manager and explains the [Extranet](#) performance metrics.

## Detailed Extranet Results

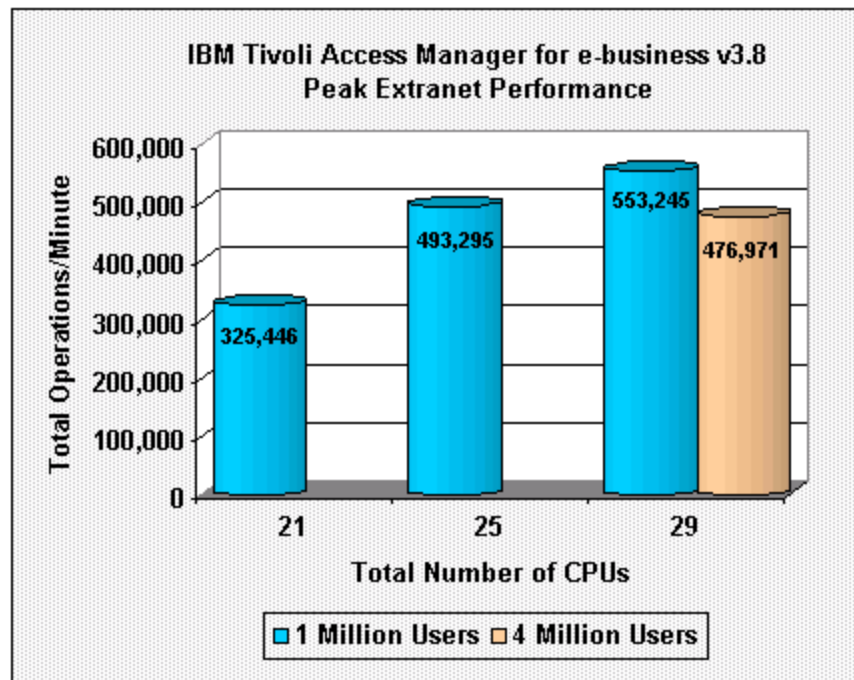
The Extranet Scenario simulates customers or suppliers logging into a private Web site and obtaining information they are authorized to get. It measures the combination of one user authentication and 10 authorizations for access to resources (these 11 operations constitute one *Extranet sequence*). We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

All of the Extranet tests were done with Tivoli Access Manager configured to cache user status information, group membership and passwords, 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. Note that Tivoli Access Manager actually does not cache access control information. Instead it stores a replicated copy of the access control database on each server. When the master access control database is updated, the changes are automatically pushed out to all Tivoli Access Manager servers. In addition, each Tivoli Access Manager instance was configured to act as a Web server.

[Figure 1](#) shows the Extranet Scenario performance of Tivoli Access Manager v3.8 for tests with 1,000,000-user and 4,000,000-user directories. The X-axis shows the total number of CPUs used in all of the servers, including the directory server. We only tested the 4,000,000-

user directory using 29 CPUs. See the [Server Hardware and Software Set Up](#) section below for the details on the configurations tested.

Figure 1: Tivoli Access Manager v3.8 Extranet Performance



[Table 1](#) shows the Extranet Scenario performance metrics and Tivoli Access Manager CPU utilization for the four tests we ran. We used a single directory server with one CPU for all of these tests. The directory server CPU was essentially idle during the tests because most user data was cached on the Tivoli Access Manager servers.

During Test #1, each load generator system's CPU was 74% utilized. For all of the other tests, the load generator systems were running at 100% CPU utilization. Because the Tivoli Access Manager CPUs were not fully utilized, the load generator systems limited the performance we were able to measure. If we had had faster load generator systems or more of them, it is likely that the Tivoli Access Manager servers would have performed at a higher rate.

Table 1: Tivoli Access Manager v3.8 Extranet Performance Metrics  
(Larger metrics are better)

Test #	# Users in Directory	# CPUs	Total Operations per Minute	Total Operations per Minute per CPU	Average Tivoli Access Manager CPU Utilization
1	1,000,000	21	325,446	15,497	97%
2	1,000,000	25	493,295	19,732	82%
3	1,000,000	29	553,245	19,077	87%
4	4,000,000	29	476,971	16,447	91%

For the test with 4,000,000-user directory, we configured the Extranet Scenario to use 1,500,000 users. This is 37.5% of the total users and substantially more than the typical configuration using 10% of the users in a directory. Because the LDAP directory server was idle during all of the Extranet tests, the number of users in the directory was not a factor in the performance measurements. So, the 4,000,000-user test performance is comparable to our typical Extranet test with 15,000,000 users in a directory.

## Conclusions

The benchmark results lead us to conclude that:

- IBM Tivoli Access Manager for e-business v3.8 outperforms all products we've tested to date by at least 52% in any full-cache Extranet environment.
- In a full-cache Extranet environment, IBM Tivoli Access Manager for e-business v3.8 delivers over 67% better per-CPU performance on Sun servers than any other product we've tested.
- IBM Tivoli Access Manager for e-business continues to deliver outstanding performance as the user directory grows to 4,000,000 or more entries.

## Test Methodology

Mindcraft<sup>®</sup> tested the performance of IBM Tivoli Access Manager for e-business v3.8 using our iLOAD MVP<sup>™</sup> tool to run the [AuthMark<sup>™</sup> Benchmark Extranet Scenario](#). In this section, we describe these tests so that you will be able to understand the performance results discussed in the [Detailed Extranet Results](#) section 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. For the Tivoli Access Manager tests we used the AuthMark Extranet Scenario.

### 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 complete and realistic usage pattern.

The following simplified sequence will walk you through the Extranet Scenario to show you how it works using Tivoli Access Manager, which uses the standard HTTP 1.1 authentication protocol to send the user name and password for every request:

1. The iLOAD test client (a script-driven program that emulates a web browser) sends a request to a Tivoli Access Manager server for a protected resource residing on a Web server or a Tivoli Access Manager server (Tivoli Access Manager can act as a Web server also).

2. Tivoli Access Manager determines that the iLoad test client has not been authenticated yet because there is no authentication header in the request. So Tivoli Access Manager sends back a "401" HTTP response to the iLOAD test client indicating that its identity has not been authenticated.
3. The iLOAD test client then resends a request for the same URL but this time includes an HTTP authorization header containing a user ID and password.
4. Tivoli Access Manager checks the user ID and password to see if they match the authentication information in its cache or stored in a directory. If they do, the iLOAD test client is authenticated.
5. Tivoli Access Manager then checks the iLOAD test client's authorization to access the requested resource. If the authorization fails, Tivoli Access Manager returns an error.
6. If the client is authorized, the resource, which in this case is one of the 14 KB Web pages used in the Extranet Scenario, is returned to the test client.
7. The test client requests another resource, resending the HTTP authorization header containing a user ID and password along with the request.
8. Tivoli Access Manager then performs both an authentication and authorization to check the validity of the user and that the user is authorized to have access to the resource.
9. If the user is authenticated and authorized, the resource is returned.
10. The test client then requests eight additional resources, for a total of 10 requested resources.

Tivoli Access Manager did not use cookies, so every access to a requested resource did both an authentication and authorization. The extra transmissions in Steps 2 and 3 above only happen for the first request of each simulated user because subsequent requests (see Step 7 above) automatically include the standard HTTP authorization header. For the Extranet Scenario tests, we warmed-up the servers by running the test scripts in their entirety.

The Extranet Scenario operation sequence consists of a total of 11 client operations (transmissions) per user session:

- The first resource request (which results in two transmissions): the first resource request, without the user ID and password, and the second resource request, with the user ID and password header.
- Nine more resource requests (one transmission per request): each contains the HTTP authorization header with user ID and password.

## Extranet Scenario Configuration

[Table 2](#) shows the AuthMark Extranet Scenario configuration parameters we used. There were two different sets of configuration parameters based on the number of users in the directory. These configurations are designated 1M and 4M in Table 2.

Table 2: AuthMark Extranet Scenario Configuration Parameters

Parameter	1M Values	4M Values
Number of users in the directory	1,000,000	4,000,000
Number of Organizational Units or security groups	10	10
Total number of user sessions per test	100,000	1,500,000

The number of user sessions active during a given test run is determined by experimenting to obtain the highest performance. 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 security 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 security 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 2](#) for the numbers we used for these tests). The tester is free to use any number of client test systems (called *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 two types of servers for these tests: Tivoli Access Manager servers and an LDAP directory server. [Table 3](#) shows the summary of the server configurations we used for each test. The detailed configurations of the Tivoli Access Manager and directory servers are shown in [Table 4](#) and [Table 5](#), respectively. Figures [2](#), [3](#), and [4](#) show how the various servers were connected over the four networks

we used (each network is shown in a different color). We used HP ProCurve 2224 switches for each network.

Table 3: Servers and CPUs

Test #	Tivoli Access Manager Servers & CPUs/Server	LDAP Directory Servers & CPUs/Server	Lab Set Up
1	Servers: 5 CPUs: 4	Servers: 1 CPUs: 1	<a href="#">Figure 2</a>
2	Servers: 6 CPUs: 4	Servers: 1 CPUs: 1	<a href="#">Figure 3</a>
3	Servers: 7 CPUs: 4	Servers: 1 CPUs: 1	<a href="#">Figure 4</a>
4	Servers: 7 CPUs: 4	Servers: 1 CPUs: 1	<a href="#">Figure 4</a>

Table 4: Sun Enterprise 420R Tivoli Access Manager Server Configuration

Feature	Configuration
CPU	4 x 450 MHz UltraSPARC II Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	2 GB ECC
Disk	2 x 18 GB SCSI 10,000 RPM (Fujitsu MAG31826 SUN18G) using 1 x differential SCSI controller in PCI slot (Symbios 53C875)
Networks	<ul style="list-style-type: none"> <li>■ 1 x integrated 100Base-TX NIC</li> <li>■ 1 x Quad 100Base-TX NIC</li> </ul>
Software	<ul style="list-style-type: none"> <li>■ Solaris 8, version 01/01 with all recommended patches</li> <li>■ IBM Tivoli Access Manager for e-business v3.8 Base Fixpack 3</li> <li>■ IBM Tivoli Access Manager for e-business v3.8 WebSEAL Fixpack 1</li> </ul>
Tunes	<p><b>Tivoli Access Manager tunes:</b></p> <ul style="list-style-type: none"> <li>■ Configured four Tivoli Access Manager instances per Tivoli Access Manager machine</li> <li>■ In the /opt/pdweb/etc/Policy Directord.conf for each instance:</li> </ul> <pre>[ldap] default-policy-override-support = yes user-and-group-in-same-suffix = yes bind-dn = cn=root bind-pwd = &lt;cn=root password&gt;  [session] max-entries = 200000 #for 1M user tests max-entries = 300000 #for 4M user tests timeout = 1209600 inactive-timeout = 1209600 ssl-id-sessions = no  [ba] ba-auth = both</pre>

Table 5: Sun Enterprise 420R LDAP Directory Server Configuration

Feature	Configuration

CPU	4 x 440 MHz UltraSPARC II Cache: L1: 16 KB I + 16 KB D; L2: 4 MB
RAM	4 GB ECC
Disk	<ul style="list-style-type: none"> <li>■ 2 x 18 GB SCSI 10,000 RPM (Fujitsu MAG31826 SUN18G) using · 1 x differential SCSI controller in PCI slot (Symbios 53C875)</li> <li>■ 1 x StorEDGE D1000 drive array NOT configured as a RAID with a mix of 12 SCSI Sun disk drives: <ul style="list-style-type: none"> <li>■ Seagate ST318203L 18.2GB 10,000 RPM</li> <li>■ IBM DDYS-T18350 18.2GB 10,000 RPM</li> </ul> </li> </ul>
Networks	<ul style="list-style-type: none"> <li>■ 1 x integrated 100Base-TX NIC</li> <li>■ 1 x Quad 100Base-TX NIC</li> </ul>
Software	<ul style="list-style-type: none"> <li>■ Solaris 8, version 01/01 with all recommended patches</li> <li>■ IBM® DB2 7.1.0.28 Fixpack 1</li> <li>■ IBM® Directory 3.2.1 Fixpack 5</li> </ul>
Tunes	<p><b>Solaris tunes:</b></p> <ul style="list-style-type: none"> <li>■ ndd -set /dev/tcp tcp_time_wait_interval 60000 (default=240000)</li> </ul> <p><b>DB2 tunes:</b></p> <ul style="list-style-type: none"> <li>■ BUFFPAGE 512000</li> <li>■ DBHEAP 22000</li> <li>■ SORTHEAP 2500</li> <li>■ MAXLOCKS 100</li> <li>■ MINCOMMIT 25</li> <li>■ db2 "alter bufferpool ibmdefaultbp size -1"</li> </ul> <p><b>Directory tunes:</b></p> <ul style="list-style-type: none"> <li>■ In /etc/slapd32.conf: <ul style="list-style-type: none"> <li>■ ibm-slapdSetEnv: LDAP_CONCURRENTRW=ON</li> <li>■ ibm-slapdSetEnv: RDBM_CACHE_SIZE=500000</li> <li>■ ibm-slapdSetEnv: RDBM_FCACHE_SIZE=625000</li> </ul> </li> </ul>

Figure 2: Test #1 - 5 Tivoli Access Manager Servers, 1 Million User Directory



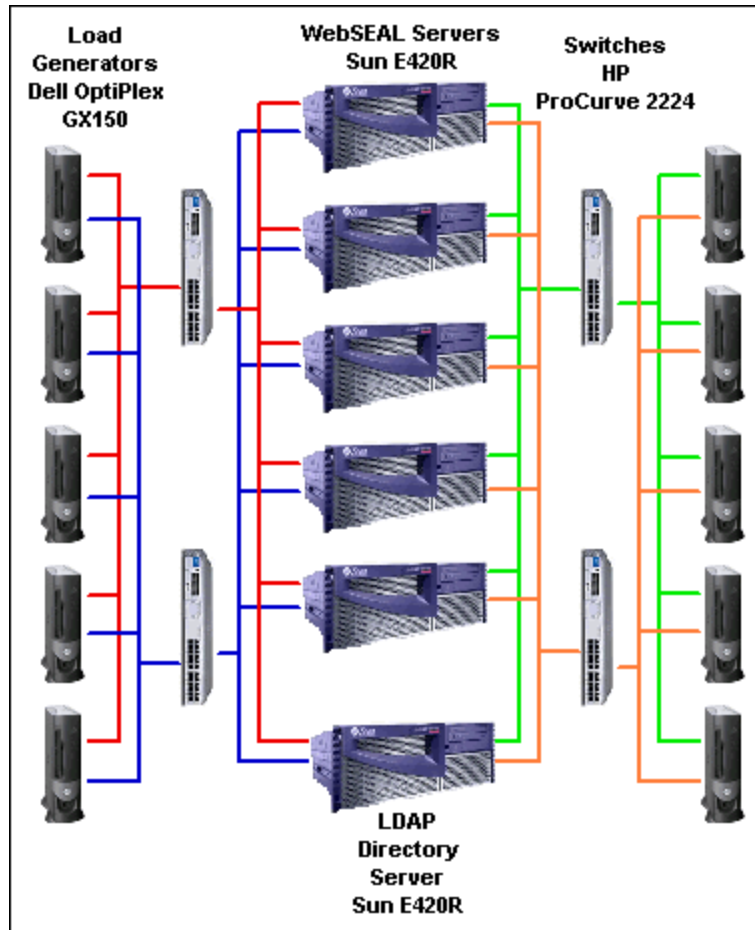


Figure 3: Test #2 - 6 Tivoli Access Manager Servers, 1 Million User Directory

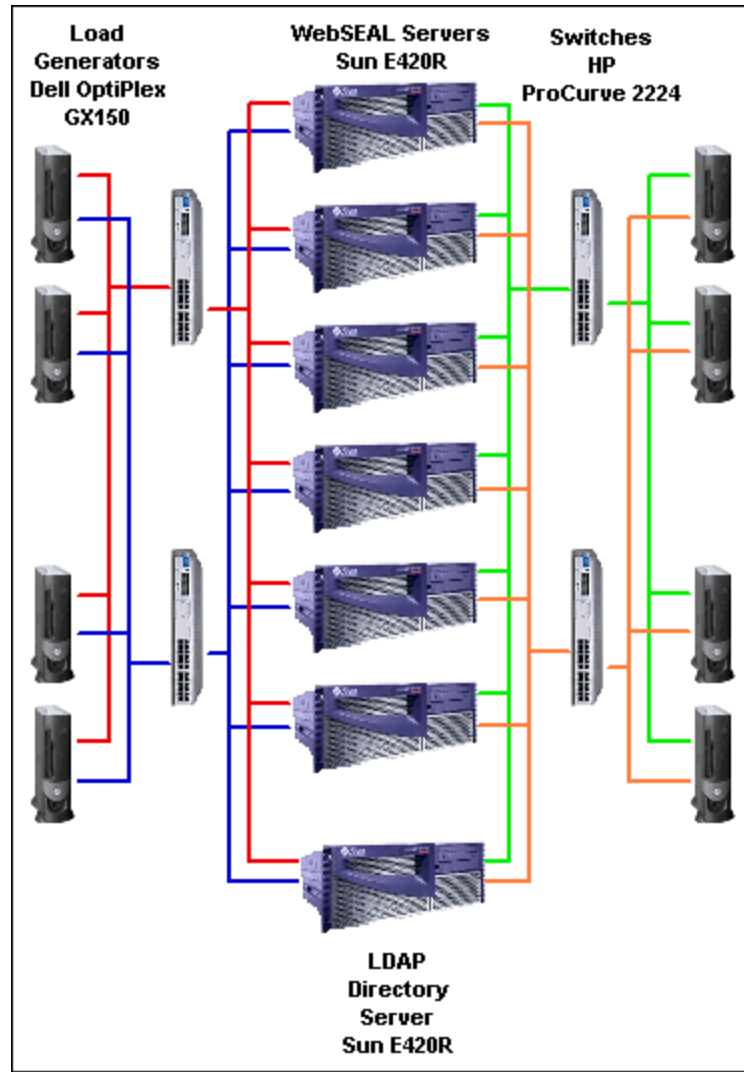
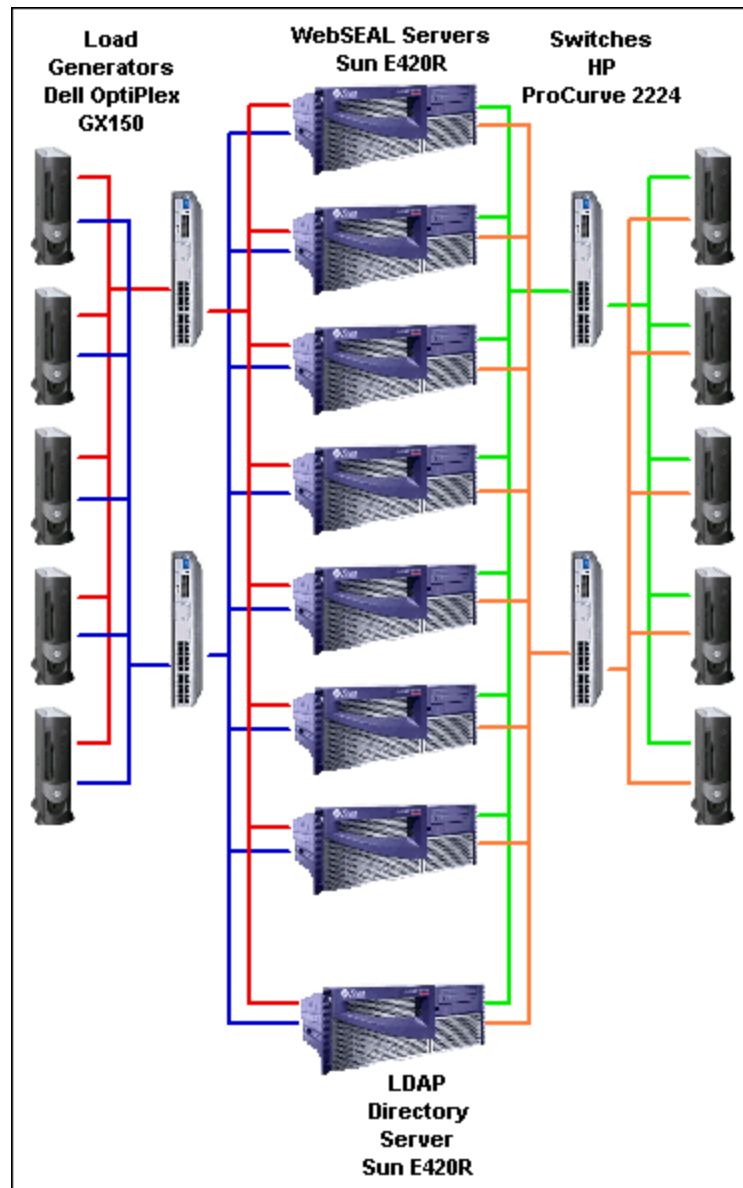


Figure 4: Tests #3 and #4 - 7 Tivoli Access Manager Servers, 1 and 4 Million User Directory



## Load Generator Systems

For all of the tests, we used Dell OptiPlex GX150 computers configured as shown in [Table 6](#) as the load generator systems. The number of load generator systems we used for each test is shown in [Figures 2, 3, and 4](#).

Table 6: Dell OptiPlex GX150 Load Generator System Configuration

Feature	Configuration
System	1 x 1 GHz Pentium III CPU
RAM	512 MB SDRAM
Disk	1 x 38 GB Western Digital ATA/66
Networks	<ul style="list-style-type: none"> <li>■ 1 x 3Com Integrated Fast Ethernet (3C920)</li> <li>■ 1 3Com EtherLink XL 10/100 (3C905-TX)</li> </ul>

Operating System	Microsoft Windows 2000 Professional, SP1, FAT32 file system
Tunes	<b>Windows 2000 tunes:</b> <ul style="list-style-type: none"><li>■ In the registry, set MaxUserPort to 60,000</li></ul>

## Changes

- Only changed the product name to IBM Tivoli Access Manager for e-business from Tivoli Policy Director to correspond to the renaming.

### 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](mailto:info@mindcraft.com)*

*Phone: +1 (408) 395-2404*

*Fax: +1 (408) 395-6324*