Securant ClearTrust Version 4.2 AuthMark Login Performance Details

By Bruce Weiner
(PDF version, 73 KB)

June 8, 2000

Contents

Test Methodology

Mindcraft® tested the performance of Securant's ClearTrust Version 4.2 using our iLOAD MVP™ tool and the AuthMark ™ Benchmark Login Scenario. In this section, we describe both of 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 users is; it occurs typically 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 a Web server 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 ClearTrust tests we used the AuthMark Login Scenario.

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 and 5,000,000
Number of Organizational Units or security groups	10
Total number of user sessions per test	100,000 for 1,000,000 database 500,000 for 5,000,000 database

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 orgalizationalPerson schema and Netscape's inetOrgPerson schema. It also includes tools to load the same data into an Oracle database, 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 ClearTrust). 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 used a ten-minute warm-up period.

Result Analysis

This section will analyze the performance characteristics of ClearTrust including its performance scalability with different server configurations and with two sizes of user databases.

1,000,000 User Database Login Performance

The performance measurements in Table 2 show the result of the warmed-up Login Scenario tests for three different server configurations with a 1,000,000 user database. The Scaling Factor in Table 2 shows how much faster a configuration is compared to a single authorizer system having one CPU.

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

Authorizer Configuration	Logins per Second	Logins per Minute	Scaling Factor
1 system, 1 CPU (see Figure 1)	391	23,445	-
1 system, 2 CPUs (see Figure 2)	630	37,783	1.61
2 systems, 1 CPU (see Figure 3)	763	45,767	1.95

The server CPU utilization during the tests will give you insight into how to configure an environment to get the maximum performance from ClearTrust. Table 3 shows the CPU utilization on each of the servers for each Authorizer configuration. The database server's low CPU utilization demonstrates that ClearTrust's caching is very effective (for these tests, the Authorizers were configured to cache information for 110,000 users).

Table 3: ClearTrust CPU Utilization - 1,000,000 User Database

Authorizer Configuration	Authorizer Server(s) CPU Utilization	Web Servers CPU Utilization	Database Server CPU Utilization
1 system, 1 CPU	100%	2 servers: 98% & 50%	4%
1 system, 2 CPUs	96%	3 servers: 75% - 80%	10%
2 systems, 1 CPU	100%	3 servers: 85% each	15%

5,000,000 User Database Login Performance

Table 4 compares the login performance of ClearTrust with a 5,000,000 user database to that with a 1,000,000 user database. The test results show that ClearTrust's performance holds up extremely well when servicing a very large number of users. The Scaling Factor in Table 4 shows performance relative to the test with a 1,000,000 user database.

Table 4: ClearTrust Login Performance Scalability - 1,000,000 and 5,000,000 User Database

Authorizer Configuration	Logins per Second	Logins per Minute	Scaling Factor
1,000,000 users 1 system, 1 CPU	391	23,445	-
5,000,000 users 1 system, 1 CPU	370	22,216	0.95

Table 5 shows the CPU utilization of each of the servers for the 5,000,000 user database test. The 1,000,000 user database test for the same Authorizer configuration is included in Table 5 to facilitate comparison. ClearTrust's caching remains very effective for 5,000,000 users as the database server's low CPU utilization demonstrates (for the 5,000,000 user tests, the Authorizer was configured to cache information for 500,000 users).

Table 5: ClearTrust CPU Utilization - 1,000,000 and 5,000,000 User Databases

Authorizer Configuration	Authorizer Server CPU Utilization	Web Servers CPU Utilization	Database Server CPU Utilization
1,000,000 Users 1 system, 1 CPU	100%	2 servers: 98% & 50%	4%
5,000,000 Users 1 system, 1 CPU	100%	2 servers: 72% each	9%

Conclusions

These test results lead us to conclude that:

- ClearTrust's login performance scales extremely well, almost doubling, when you add a second Authorizer system. We saw nothing during our tests to indicate performance scaling would slow down as more Authorizer systems were added.
- Adding a second processor to an Authorizer system will improve ClearTrust's login performance significantly, as long as other resource constraints such as insufficient memory are not encountered.
- ClearTrust's caching is very effective and should be set to support the maximum number of concurrent

sessions expected.

- ClearTrust delivers high login performance that is nearly independent of the number of users in its database through at least 5,000,000 users.

Hardware Configurations Tested

Mindcraft used Sun Enterprise 450 servers for the Web servers, ClearTrust Authorizer servers and the database 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 **ClearTrust Authorizer servers** : 2 x 9 GB SCSI; one for Solaris and one for ClearTrust **Database server**: 2 x 9 GB SCSI; one for Solaris and one for the database data
Networks	1 x 100Base-TX integrated NIC

Figures 1, 2, and 3 show how the various servers were connected to each other for these tests. All of the systems were connected using a 100Base-TX switch.

Figure 1: Server Structure for Testing 1 Authorizer System with 1 CPU

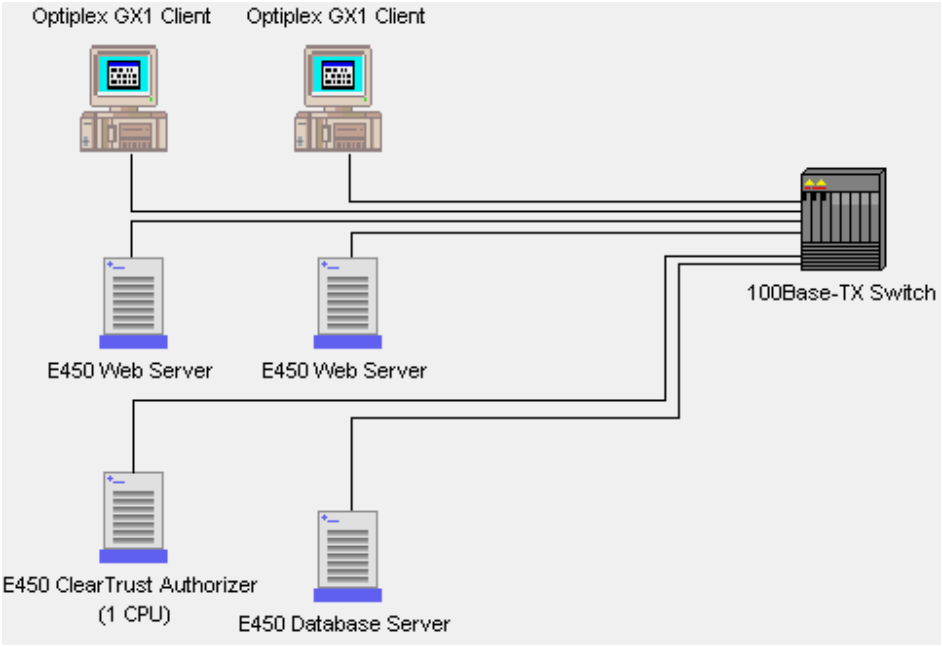


Figure 2: Server Structure for Testing 1 Authorizer System with 2 CPUs

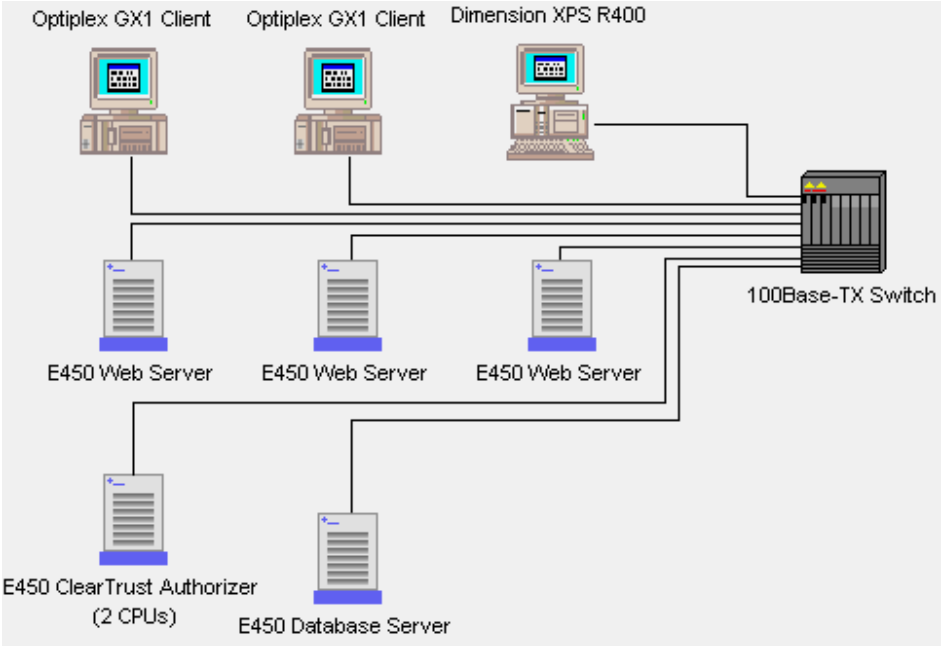
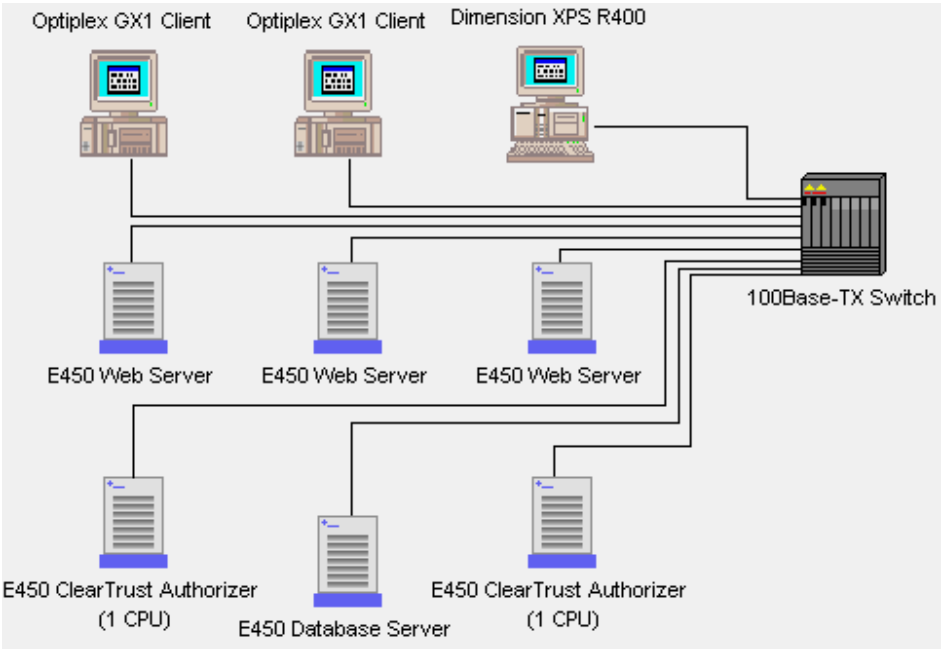


Figure 3: Server Structure for Testing 2 Authorizer Systems with 1 CPU



Server Software Configuration and Tuning

We used the following server software for these benchmark tests:

- Solaris 2.6 with the latest patch cluster as of May 1, 2000
- Oracle client 7.3 installed on the database server
- Netscape Enterprise Server 3.6.1 (Web servers)
- ClearTrust 4.2

All software ran with default settings except for the following:

- For Solaris:

  tcp_conn_req_max_q=256

- For Netscape Enterprise Server:

  ListenQ 256
  MaxProcs=4

MaxAcceptThreadsPerSocket=4
MinAcceptThreadsPerSocket=4

Client Test Systems

For all of the tests, we used the two Dell client test systems configured as shown in Table 7.

Table 7: Base Client Test System Configurations

Feature	Configuration
System	Dell Optiplex GX1, 1 x 500 MHz Pentium III CPU
RAM	256 MB SDRAM
Disk	1 x 4 GB SCSI
Networks	1 x 100Base-TX 3Com 3C905B
Operating System	Microsoft Windows NT 4.0 Workstation, Service Pack 4

For the test using a ClearTrust Authorizer with two CPUs, we used an additional client test system configured as shown in Table 8.

Table 8: Additional Client Test System Configuration

Feature	Configuration
System	Dell Dimension XPS R400, 1 x 400 MHz Pentium II CPU
RAM	192 MB
Disk	1 x 4 GB SCSI
Networks	1 x 100Base-TX 3Com 3C905B
Operating System	Microsoft Windows NT 4.0 Workstation, Service Pack 3

For more information, contact us at: info@mindcraft.com
Phone: +1 (408) 364-2860
Fax: +1 (408) 364-2862