Scalable E-Commerce Solutions for Identity Management

Microsoft Corporation
Published: May 2003

Abstract

This white paper describes a series of tests that were performed for a financial client that is deploying Active Directory® to support nearly 18 million Internet-based customers. The testing was designed to prove the scalability and performance of Active Directory to support this number of user objects and the customer's specific performance requirements – both of which were successfully met by Active Directory.

Contents

Introduction

This paper documents a collaborative laboratory-based test effort conducted by Oblix™, Hewlett-Packard, and Microsoft that demonstrates the viability of our combined products to meet the real-world requirements of a large financial institution. The test architecture and methodology were modeled after the financial institution's consumer site – a sophisticated, large-scale extranet operation – and were designed to evaluate the products' ability to scale and handle five-year projected operational loads. Because the test architecture is modeled after a real-world extranet operation, as opposed to a generic benchmark, it is a highly realistic demonstration of the combined NetPoint™/Active Directory architecture's ability to scale to a large enterprise level. The test is also significant because it included identity profile modifications as part of transaction throughput testing, making this the first ever measurement of identity management system performance.

Testing was conducted at Microsoft's Performance Analysis Research Center (PARC). Oblix NetPoint provided the Identity Management and Single Sign-on (SSO) service for the architecture. Microsoft® Active Directory provided the directory service that NetPoint uses to authenticate users and store identity profile data.

The expected user base for the online banking project consists of 17.6 million users. Mercury Interactive's LoadRunner product, along with a transaction mix comprised of 10 separate ASP and HTML pages, were used to simulate the authentication load generated by this number of users.

The test results confirm that the Hewlett-Packard hardware platform, Oblix NetPoint configuration, and Microsoft Active Directory, easily scaled to meet the financial institution's online banking project requirements. With 17.6 million users, and even under maximum load, the Microsoft Active Directory was not stressed. The system also demonstrated excellent failover characteristics: Load balancing successfully kicked in when servers were removed from the mix, and the system recovered within minutes in response to a simulated outage. The throughput testing not only demonstrated the ability of the NetPoint Access System™ to handle 17.6 million user authentication and authorization loads, but also demonstrated the ability of the NetPoint COREid System™ to handle a high volume of identity profile changes. The financial institution's requirements were met using one server of each type.

This paper summarizes the test project and test results. It also documents the salient conclusions and recommendations learned from the test effort, such as the minimum hardware required to meet the financial institution's extranet operation requirements.

Project Description

Test Objectives

The primary goal of the test effort was to verify that the performance of Oblix NetPoint and Microsoft Active Directory, operating together, meet the projected throughput, scalability, and failover requirements defined by the financial institution.

Throughput testing determines the number of transactions that can be successfully completed within a given timeframe, including the following:

- Successful and failed authentications
- Successful authorizations
- Successful identity profile changes

Unlike other benchmarks designed to test for web access management system transaction throughput, this test effort tested for both successful and failed authentications. This mix is more realistic than testing for successful authentications alone. Testing for authentications and authorizations stresses the NetPoint Access System and Microsoft Active Directory

In addition to this, the inclusion of identity profile changes in transaction testing makes this the first ever measurement of identity management system performance. Testing for successful identity profile changes stresses the NetPoint COREid System and the Microsoft Active Directory.

Scalability testing focuses on how well the overall system scales horizontally and provides a formula for determining when more servers are required. This test stresses the NetPoint Access servers and Active Directory.

Failover testing highlights the ability of the overall system to continue functioning in a reduced capacity, while still meeting acceptable performance metrics.

Test Methodology

Test Scenarios

The test requirements were defined by profiling the financial institution's real-life usage of Oblix NetPoint and Microsoft Active Directory, which included customer access of both secured and non-secured resources. The usage profile is split into two categories: "normal" usage, the usage observed on a typical business day, and "peak" usage, the usage observed on the heaviest business days near the middle and end of the month. The usage profile is based on a 5-year projected growth and has the following characteristics:

- 17.6 million users in the system.
- 7.3 million active users (that is, those who have logged on within the last 30 days).
- 2.7 million sessions per typical day.
- 14,600 concurrent users sessions on a normal day.
- 5.4 million sessions per peak day.
- 29,200 concurrent users sessions on a peak day.
- 8-minute average user session length.
- Typical session composed of 10 page views:
    - 4 unprotected pages
    - 4 protected pages, via a global authorization rule
    - 2 protected pages, via a role-based authorization rule
- A 20% unsuccessful login rate: For every five successful login attempts, one unsuccessful attempt is made (that is, invalid credentials are submitted).
- One percent of users at any given time are actively making a change to their identity profile (for example, changing their billing address).

Performance Metrics

The following response times were considered as acceptable performance, given a fully functional environment:

- 2-second response time for successful authentication
- .2- second response time for successful authorization
- 4-second response time for successful identity change

Using these metrics, any given user interaction had to be completed in its specified time limit to be judged successful. Only through a combination of generating the simulated transaction mix load and ensuring that all transactions completed successfully within the acceptable timeframes was the throughput and scalability testing considered successful.

Readers should note that web access management system performance benchmarks may not necessarily define minimum acceptable performance levels, and are therefore less realistic than this test.

Rebooting and Caching

Several measures were taken to avoid contrived test results. First, before restarting new test cycles, all machines except the domain controllers were rebooted. Second, consideration of user data caching was taken into account. The default Active Directory domain controller cache was used, which allows approximately 20,000 users to be cached. The LoadRunner script used a random number generator to determine which accounts were accessed so that the same accounts were not used between runs. This reduced the likelihood that the cached users would skew the performance results.

Lab Environment

The test environment began in a "baseline" configuration, which consisted of a single Virtual Local Area Network (VLAN), and 100,000 users in a single Active Directory forest with no load balancing. The baseline configuration then went through major revisions during the course of testing until it reached the following full-scale configuration:

- 12 LoadRunner client machines
- 8 Web servers with NetPoint WebGate™
- 1 NetPoint COREid Server™
- 3 NetPoint Access Servers™
- 6 VLANs
- 2 F5 load balancers
- 1 Active Directory forest (admin.net)
- 2 Active Directory domain controllers (1 for admin.net, and 1 more for cst.net)

Oblix NetPoint (version 6.0.1.1) was configured to support both LDAP and ADSI, and both protocols were tested. Additional background details and definitions are provided in Appendix I: Background Details and Definitions, including details about the Load Generation tool, SAN configuration, user directory account creation, and the Oblix NetPoint components.

Lab Architecture

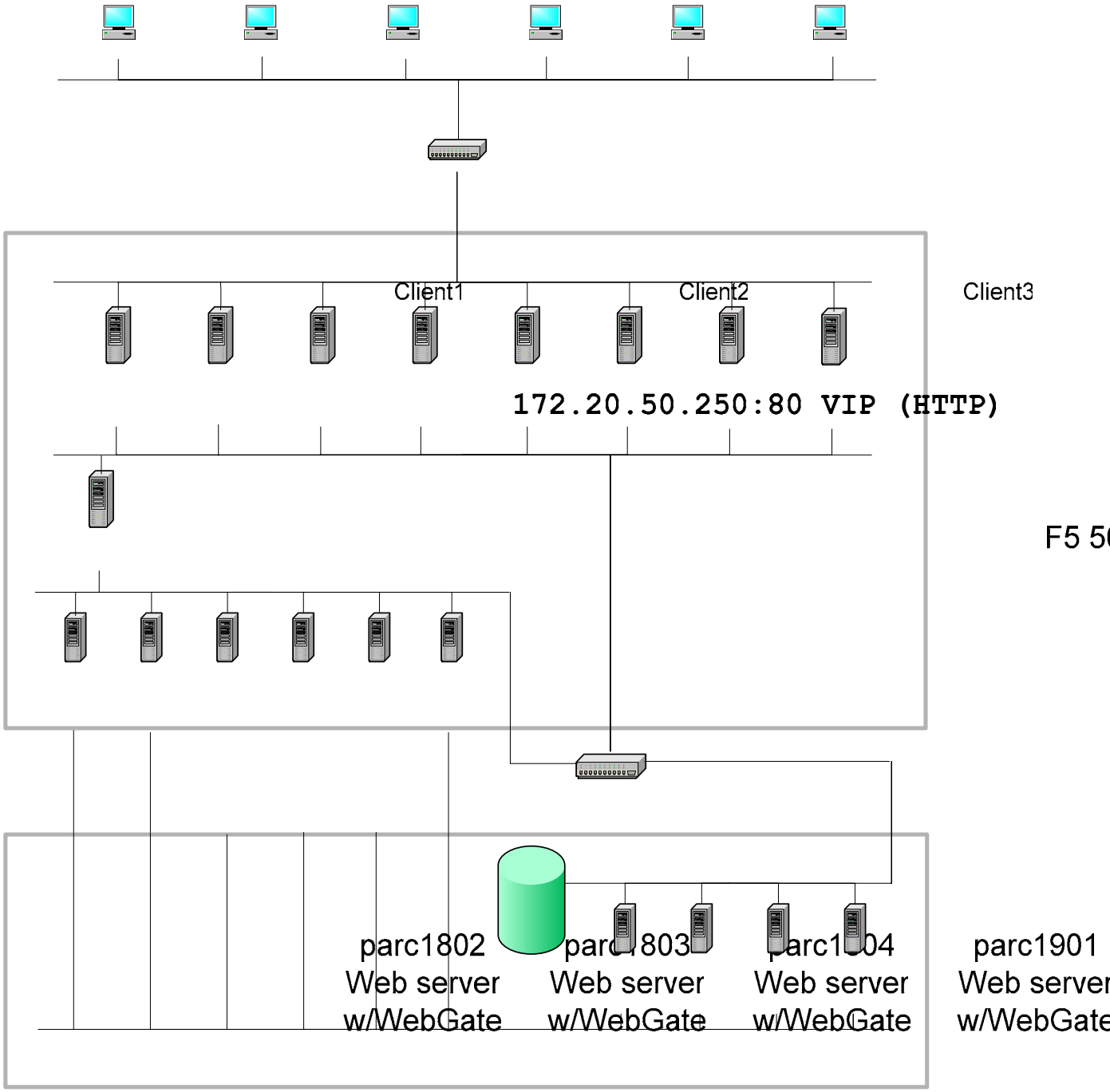

Figure 1 Lab Architecture

Test Summary

Throughput

As stated previously, the primary goal of lab testing was to confirm that Oblix NetPoint could support the load generated by the projected online banking user base using Microsoft Active Directory. Throughput test objectives were easily met using both ADSI and LDAP.

Non-zero domain controller CPU utilizations, summarized in Table 1, confirm that user data caching is not skewing performance test results. All results are displayed as averages.

Table 1 CPU Utilization

CPU Utilization	1.76m Users (LDAP Normal)	17.6m Users (LDAP Peak)	17.6m Users (LDAP Max)	17.6m Users (ADSI Normal)
Access Server (CPU utilization)	6.71%	13.27%	9.01% (3 Access Servers)	17.52% (3 Access servers)
COREid Server (CPU utilization)	2.33%	4.12%	7.88%	2.12%
Domain Controller (CPU utilization)	8.65%	16.34%	43.24%	22.46%
WebGate Server (CPU utilization)	NA	47.25%	77.14%	NA

Scalability

The financial institution's normal usage load was easily handled by a single NetPoint Access Server, a single NetPoint COREid Server, and a single Microsoft Active Directory domain controller, for both LDAP and ADSI. This same combination of servers also handled the peak load while using the LDAP protocol. However, the addition of two more NetPoint Access Servers was required to handle the peak load when operating with ADSI. Achieving peak performance for both ADSI and LDAP required six Web Servers with NetPoint WebGate. Based on these results, the financial institution should deploy a minimum of two Access Servers (using LDAP) to allow for failover and maintenance.

During testing with LDAP, the load, the number of NetPoint Access Servers, and the number of NetPoint WebGate Servers were increased until throughput was maximized (that is, until performance linearity was lost). Maximum performance (using LDAP) was achieved with three NetPoint Access Servers and nine NetPoint WebGate Servers (in addition to a single NetPoint COREid Server and a single Microsoft Active Directory domain controller). Ultimately, the WebGate Server CPU utilization pinned the upper limit on transaction throughput, not the NetPoint Access and COREid Servers or the Microsoft Active Directory. (See Table 1.)

Failover

The original goal was to have multiple servers of each type (Access, COREid, domain controller, and so on), but test results only required a single server for NetPoint COREid and Active Directory Services to

meet the throughput requirements. Therefore, the only components that were tested for failover were the NetPoint Access Servers.

The system's failover characteristics were observed under maximum performance conditions (that is, with three Access Servers running). Taking one of the servers out of the mix caused the NetPoint load balancing to kick in and distribute the load among the two remaining Access Servers with a corresponding increase in CPU and Network utilization (as long as three Access servers were not running near capacity). We also simulated a rolling upgrade by replacing one of the Access Servers, removing the failed server from the pool, restarting the AAA_service, and placing it back into the pool using the F5.

The entire system was also stress tested several times by disabling the F5 interfaces while under peak load for LDAP to simulate an outage, and then enabling it to create Max load conditions. In all three cases, the system returned to normal operation within approximately five minutes.

Windows Server 2003

We upgraded the existing Windows® 2000 domain controller (containing all the Oblix schema extensions) to Windows Server™ 2003. Testing time constraints prevented us from obtaining accurate comparison data for the domain controller. However, if the load before the test is subtracted from the migration load during the test, the numbers are almost identical. All the Oblix NetPoint components were unaffected by the upgrade and performance matched the Windows 2000 numbers.

Since the domain controller was not the bottleneck and the Oblix NetPoint software was not optimized for Windows Server 2003, the results were as expected.

Server Performance

Table 2 and Table 3 show the load placed on each of the primary server types under normal load, for both LDAP and ADSI. Testing was conducted with one NetPoint Access Server, one NetPoint COREid Server, and one Microsoft Active Directory domain controller. For the server configurations for each server type, see Appendix II: Resources Required.

In general, ADSI is harder on Access Server CPUs and the domain controller CPUs. LDAP exhibits faster performance because of its connection pooling capability. Both protocols seemed to apply about the same amount of load on the disks containing the Active Directory database.

Server performance under peak load and maximum throughput loads (for LDAP) are documented in Appendix III: Additional Server Performance Data.

Table 2 17.6 million users, Normal Load (LDAP), 1 Access Server, 1 COREid Server, and 1 Domain Controller

PerfMon Counter	Access Server		COREid Server		Domain Controller	
	Avg	Max	Avg	Max	Avg	Max
%Processor Time (Processor_Total)	6.71	13.70	2.33	8.51	8.65	17.93
Processor Queue Length (System)	0.02	5.0	0.01	4.0	0.0	1.0
Page Faults/sec (Memory)	16.67	227.69	6.36	51.0	189.08	437.55
%Disk Time (PhysicalDisk 2E)	0.69	39.85	0.49	6.78	85.95	135.26
%Idle Time (PhysicalDisk 2E)	99.35	100	99.59	100	11.46	29.29
Bytes Total/sec (Server)	38.4 KB	181 KB	18.4 KB	37.6 KB	24.4 KB	53.5 KB
Private Bytes (Process_Total)	449 MB	551 MB	184 MB	294 MB	1.18 GB	1.18 GB

Table 3 17.6 million users, Normal Load (ADSI), 3 Access Servers, 1 COREid Server, and 1 Domain Controller

PerfMon Counter	Access Server		COREid Server		Domain Controller	
	Avg	Max	Avg	Max	Avg	Max
%Processor Time (Processor_Total)	17.52	28.65	2.12	7.55	22.46	35.81
Processor Queue Length (System)	.105	8.0	0	0	0.08	8.0
Page Faults/sec (Memory)	NA	NA	5.17	335.7	442.6	4121.6
%Disk Time (PhysicalDisk 2E)	0.48	40.36	0.49	4.17	81.73	127.26
%Idle Time (PhysicalDisk 2E)	NA	NA	NA	NA	NA	NA
Bytes Total/sec (Server)	25.3 KB	62.4 KB	18.6 KB	56.2 KB	23.7 KB	62.0 KB
Private Bytes (Process_Total)	249 MB	353 MB	110 MB	128 MB	1.18 GB	1.20 GB

LDAP vs. ADSI

For discussion purposes, LDAP is defined as a wire protocol, whereas ADSI is a Microsoft API that uses LDAP and is designed to abstract the process of interfacing with Active Directory easier, making the task of programming access to Active Directory easier. NetPoint authentication can be configured to use either LDAP or ADSI when accessing Active Directory. During the lab test, we started with ADSI because there was a known memory leak with the Netscape LDAP SDK used by Oblix NetPoint.

Switching all the Oblix NetPoint components between protocols was time-consuming. After confirming that ADSI could meet peak throughput requirements for 17.6 million users, we switched to LDAP for the duration of testing.

Test results show that both LDAP and ADSI hit normal and peak throughput goals defined by the financial institution for the 17.6 million user target. ADSI requires a connection setup and teardown for each bind request. The Netscape LDAP SDK can stuff multiple bind requests into a single network frame (we noticed an average of 10 bind requests per frame), which accounts for the bulk of the difference in performance characteristics between the two protocols.

Conclusions and Recommendations

Oblix NetPoint and Microsoft Active Directory easily met, and exceeded, test objectives for peak loads. With 17.6 million users in it, Active Directory was not being stressed, and maximum performance is actually limited by the number of WebGate Web servers instead of the NetPoint Access System, NetPoint COREid System, or Microsoft Active Directory.

Normal and peak requirements were easily met (using LDAP) with one NetPoint Access Server, one COREid Server, one Microsoft Active Directory domain controller, and six Web servers with NetPoint WebGate. Maximum system performance was achieved with two additional NetPoint Access Servers and three Web servers with NetPoint WebGate. However, the recommended approach for a production environment is to have at least one more of each server type of than required. With that in mind, the following lists the minimum recommended hardware to meet the financial institution's requirements, or to achieve maximum performance:

Table 4 Minimum Hardware Requirements

Server	Number required to meet "Peak" Throughput Requirements	Number required to achieve "Maximum" Throughput Performance
Access Server	2 (1 required, 1 for backup)	4 (3 required, 1 for backup)
COREid Server	2 (1 required, 1 for backup)	2 (1 required, 1 for backup)
Domain Controller /Global Catalogs	2 (1 required, 1 for backup)	2 (1 required, 1 for backup)
WebGate Server	7 (6 required, 1 for backup)	10 (9 required, 1 for backup)

Appendix II: Resources Required provides a list of the hardware and software resource requirements for this operation, as well as a concise "parts list".

The test effort also yielded a number of other recommendations:

- Both ADSI and LDAP can scale to meet the financial institution's requirements.
- When configured for ADSI disable referral chasing on the Oblix NetPoint Access Servers.
- Use NetPoint round-robin load balancing for WebGate server to Access/COREid server communication, not F5 load balancers.
- Use an F5 load balancer for monitoring traffic and taking Access/COREid servers out of service or adding them back in. Create separate VIPs for each Access/COREid server and configure the Oblix NetPoint software to load balance across them.
- Use F5 to load balance traffic between clients and WebGate servers.
- Use a large number of drives if putting NTDS.DIT on a SAN and optimize storage for read performance.

- The “max” LDAP test only drove the domain controller CPUs to an average of 43 percent utilization. Therefore, when optimizing the domain controllers, the focus should be on the disk sub-system and optimizing it for read access.
- Testing was conducted with dual-CPU WebGate Web servers. We did not have hardware available in the lab to determine whether it is more economical to use a quad-CPU Web server with WebGate, however, this should be tested before finalizing a design.
- Consider testing 64-bit Windows Server 2003 when it becomes available for the increased cache size available for the directory controller.
- Users planning to conduct similar tests in their own laboratory environment should refer to some additional information about user data security and authentication in Appendix IV: User Data Security and Authentication.

Appendix I: Background Details and Definitions

Load Generation Tool

Mercury Interactive's LoadRunner (version 7.51, SP1) was used to simulate the load generated by various numbers of concurrent users.

LoadRunner was configured to generate load using TPS and tests were run for 4.5 hours with "Automatic" ramp-up selected. A single LoadRunner controller machine was driving 12 LoadRunner client machines. Think time was adjusted to simulate the required number of concurrent connections (14,600 for normal and 29,200 for peak). The Test Summary results were generated after removing the ramp-up time (usually 20 minutes) and the shut down period (usually 10 minutes) from the test run.

SAN Configuration

The Active Directory database, containing 17.6 million user accounts, was created in the cst.net forest and hosted on a SAN to test the viability of using a SAN instead of locally attached storage. Hewlett-Packard provided a Compaq StorageWorks Modular Storage Array (MSA) SAN with 1.5TB (42 x 36 GB drives) of storage. The SAN was divided into three 500 GB partitions and configured for RAID 0+1 (striped and mirrored) providing 237 GB of usable space per partition. For 17.6 million users, the Active Directory database was approximately 145 GB on 14 x 36 GB disks.

The operating system and swap file were stored on locally attached storage (10 GB) using one disk controller. The Active Directory log files were stored on locally attached storage (10 GB) using a second disk controller.

Each of the three domain controllers was connected to a separate partition using Emulex 9000 Host Bus Adapters (HBAs). Two of the servers were Windows 2000 domain controllers for the cst.net domain. The third was a Windows Server 2003 domain controller that was initially intended to be used for testing NetPoint with Windows Server 2003.

Account Creation

User accounts were created in groups of 250,000 using LDAP Data Interchange Format (LDIF) files and numbered sequentially from 1 to 17,600,000. Passwords were assigned immediately after the account was created to avoid having to run two separate passes. Between five and eight LDIF files were imported concurrently.

Each user account had a total of 54 attributes, with all the default attributes set.

Oblix NetPoint Components

NetPoint consists of an identity management system called the NetPoint COREid System and an access control system known as the NetPoint Access System. The main features of the NetPoint COREid System include user self-service of profile information, delegated administration, password management, group management, and so on; whereas, the main features of the NetPoint Access System are Web single sign-on, authentication, authorization, auditing, personalization, and security administration.

The NetPoint COREid System enables you to manage identity information about individuals, groups, and organizations. In addition to managing identity information, using COREid, you can manage access

privileges for a user based on a specific user attribute, membership in a group, or association with an organization. You can link privileges together into a workflow so that, for example, when a user self-registers, the registration request is forwarded to the appropriate people for signoff.

The NetPoint COREid System consists of these components:

- **COREid Server** The COREid Server is a stand-alone service or several instances of it that manage identity information about users, groups, organizations, and other objects. The COREid Server consists of several application modules such as User Manager™, Group Manager™, and Organization Manager™. Each module is used to manage specific "types" of objects in the directory server. The COREid Server stores user information on a directory server. The COREid Server keeps the directory data current so that the Access Server (described below) receives the correct information.
- **WebPass™** WebPass is a Web-server plug-in that passes information between the Web server and the COREid Server. When a user tries to access a resource on a Web server where a WebPass component is installed, WebPass maps the URL to a message format and forwards the request to a COREid server. Depending on the configuration, the COREid Server processes the request and outputs either an XML or HTML file. The request is returned to the WebPass, and then to the user's browser.

The NetPoint Access System consists of the following components:

- **Access Manager™** The Access Manager is installed on a Web server in the same directory as the COREid System component WebPass. The Access Manager provides a login interface to define resources to be protected and to group resources into policy domains. A policy domain consists of resource types to protect, rules for protection, policies for protection, and administrative rights.
- **Access System Console** The Access Manager has another application, the Access System Console, that permits administrators to add, change, and remove Access Clients and Access Servers, configure authentication and authorization schemes, configure master audit settings, and configure host identifiers.
- **Access Server** The Access Server is a stand-alone server, or several instances, that provide authentication, authorization, and auditing services. The Access Server validates credentials, authorizes users, and manages user sessions. The Access Server receives requests from an Access Client and queries authentication, authorization, and auditing rules in the directory server as follows:
    - Authentication involves determining what authentication method is required for a resource, gathering credentials over HTTP, and returning an HTTP response that is based on the results of credential validation.
    - Authorization involves granting access based on a policy and an identity established during authentication.
- **WebGate** The WebGate is an out-of-box Access Client for HTTP-based resources. A WebGate plug-in intercepts HTTP requests for Web resources and forwards them to an Access Server. WebGate is an Internet Server Application Procedural Interface (ISAPI) when installed on an IIS server. ISAPI is an Internet Web server extension that NetPoint uses to communicate with Microsoft Internet Information Server.

Oblix NetPoint Process Flow

1. When a user attempts to access content or an application, NetPoint WebGate checks to determine if the resource is protected. Servers that can be protected include Web servers and application servers, among others.
2. Oblix NetPoint authenticates the user with a customer-specified authentication method to determine the identity, leveraging information stored in the directory server. Oblix NetPoint authentication supports any third-party authentication method as well as different authentication levels. Resources of varying degrees of sensitivity can be protected by requiring higher levels of authentication, corresponding to more stringent ways of being authenticated.
3. Oblix NetPoint checks the directory server to validate credentials such as a user ID and password, sends the information back to WebGate, and generates an encrypted cookie to mark the user as being authenticated.
4. Once authenticated, WebGate prompts the Access Server to look up the appropriate security policies, compare them to the user's identity, and determine the user's level of authorization. The NetPoint Access System enables complete flexibility and control for setting access policies.
5. If the access is valid according to the policy, the user is allowed to access the desired content and applications, or both. If the policy is false, the user is denied access and redirected to another URL determined by the organization's administrator.

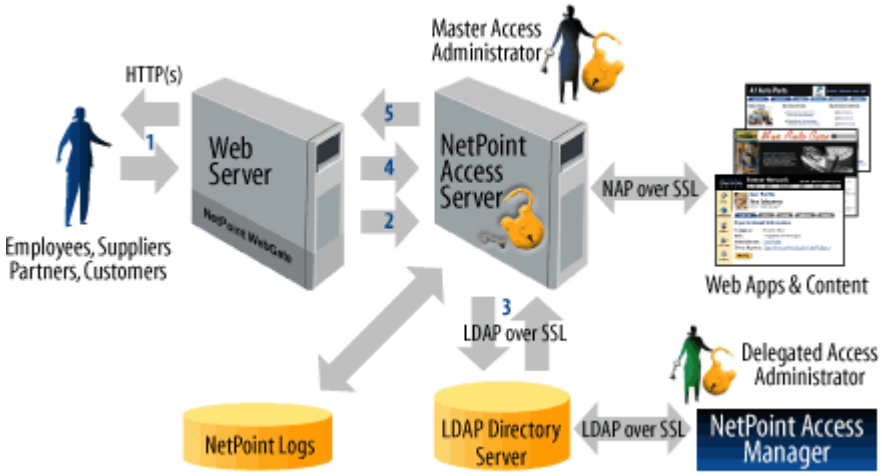

Figure 2 NetPoint Process Flow

Appendix II: Resources Required

Hardware and Software

Table 5 Oblix COREid/Access Server Configuration—Hewlett-Packard DL 580 G1

Feature	Configuration
CPU	4 x Intel® Pentium® III Xeon 700MHz/2M CPUs Cache: L1: 16 KB I + 16 KB D; L2: 2 MB (I+D)
RAM	4 GB ECC
Disk	Smart Array 5304/128 RAID 2 x HP 18.2 GB RAID 1 (OS and Swap) 2 x HP 36.4 GB RAID 0 + 1 (NetPoint software)
Networks	1 x NC3134 100 Mb (dual port) 1 x Giganet CL1000 Host Bus Adapter
Software	Windows 2000 Advanced Server, SP3 NetPoint 6.0 (maintenance release)

Table 6 Active Directory Server Configuration—Hewlett-Packard DL 8500

Feature	Configuration
CPU	4 x Intel® Pentium® III Xeon 700MHz/2M CPUs Cache: L1: 16 KB I + 16 KB D; L2: 2 MB (I+D)
RAM	4 GB ECC
Disk	Internal ORC Ultra-2 SCSI connected to 2 18 GB drives 1 Emulex HBA connected to HP Modular SAN Array 1000 (42 x 36 GB 10K RPM) SAN configured as 3 partitions (14 x 36 GB disks each) Total of 237 GB Raid 0+1 per partition. Each domain controller connected to a separate partition.
Networks	1 x NC3134 100Mb (dual port) 1 x Giganet CL1000 Host Bus Adapter
Software	Windows 2000 Advanced Server, SP3

Table 7 WebGate Server Configuration—Hewlett-Packard DL 360

Feature	Configuration
CPU	2 x Intel® Pentium® III 1.1GHz CPUs Cache: L1: 16 KB I + 16 KB D; L2: 512 KB (I+D)
RAM	4 GB ECC
Disk	Internal ROC Ultra-2 SCSI connected to 2 18 GB 10k drives
Networks	2 x built-in 100 Mb Ethernet PCI NICs
Software	Windows 2000 Advanced Server, SP3

Parts List

Table 8 Parts List for all Lab Components

Description	Type	Quantity
NetPoint COREid Server	HP DL 580 Intel P3 Xeon 700Mhz (4 CPU/4 GB RAM)	2
NetPoint Access Servers	HP DL 8500 Intel P3 Xeon 700Mhz (4 CPU/4 GB RAM)	3
Active Directory Domain Controllers	HP DL 580 Intel P3 Xeon 700Mhz (4 CPU/4 GB RAM)	2
Web Servers with WebGate	HP DL 360 Intel P3 1.1Ghz (2 CPU/4 GB RAM)	8
LoadRunner controller	Dell OptiPlex GX240 1.8GHz (1 CPU/512 MB RAM)	1
Client Workstations (for LoadRunner testing)	HP EVO Intel P4 1.8GHz (1 CPU/1 GB RAM)	12
F5 load balancers	5000 series	2
Xtreme fiber switches	Summit 48i	2
Compaq StorageWorks Modular SAN Array (MSA)	42 x 36.4 GB (1.5TB)	1

Appendix III: Additional Server Performance Data

Table 9 and Table 10 show the server performance under peak load and maximum throughput load, for operation under LDAP.

Table 9 17.6 million users, Peak Load (LDAP), 1 Access Server, 1 COREid Server, and 1 Domain Controller

PerfMon Counter	Access Server		COREid Server		Domain Controller		WebGate Server	
	Avg	Max	Avg	Max	Avg	Max	Avg	Max
%Processor Time (Processor_Total)	13.27	24.47	4.12	14.06	16.34	25.0	47.25	77.08
Processor Queue Length (System)	0.07	6.0	0.0	4.0	0.04	5.0	NA	NA
Page Faults/sec (Memory)	19.52	78.0	7.53	91.70	505.02	931.71	NA	NA
%Disk Time (PhysicalDisk 2E)	0.71	4.57	0.54	4.91	202.05	266.39	NA	NA
%Idle Time (PhysicalDisk 2E)	99.31	100	99.50	100	0.65	5.433	NA	NA
Bytes Total/sec (Server)	38.5 KB	82.6 KB	18.4 KB	63.2 KB	25.0 KB	110.7 KB	20.7 KB	82.6 KB
Private Bytes (Process_Total)	565 MB	725 MB	141 MB	183 MB	1.18 GB	1.18 GB	86.2 MB	92.7 MB

Table 10 17.6 million users, Maximum Performance (LDAP), 3 Access Servers, 1 COREid Server, and 1 Domain Controller

PerfMon Counter	Access Server		COREid Server		Domain Controller		WebGate Server	
	Avg	Max	Avg	Max	Avg	Max	Avg	Max
%Processor Time (Processor_Total)	9.01	16.27	7.88	21.09	43.24	53.91	77.14	99.22
Processor Queue Length (System)	0.024	3.67	0.016	6.0	0.44	8.0	NA	NA
Page Faults/sec (Memory)	12.65	316.60	12.14	115.47	1488.33	2242.56	NA	NA
%Disk Time (PhysicalDisk 2E)	0.623	35.31	0.59	6.63	599.66	878.49	NA	NA
%Idle Time (PhysicalDisk 2E)	99.32	113.61	99.42	100.63	0	0.141	NA	NA
Bytes Total/sec (Server)	25.7 KB	52.3 KB	18.6 KB	32.8 KB	22.9 KB	57.0 KB	24.9 KB	25.8 KB
Private Bytes (Process_Total)	487 MB	580 MB	172 MB	237 MB	1.17 GB	1.17 GB	126 MB	132 MB

Appendix IV: User Data Security and Authentication

User Data Security

User data takes three primary paths during the process of authentication and authorization; passwords are in different states depending on where they are in the process and whether SSL is being used. The following is a brief summary of the various paths and how the user data appears on the wire while in transit:

- Conversations between the client and the WebGate server are either base64 encoded (no SSL) or encrypted (with SSL) depending on how the Web page (for example, the XYZZ login page) is configured. For example, if my password is "password" and SSL was not being used, a NetMon trace would display something like "**Authorization: Basic VW5nZXJfT3JnYW5pemF0aW9uOlVuZ2VyT3JnYW4=**" for the password field in the packet capture.
- Conversations between the WebGate server and Access Server are either encoded using simple basic encoding rules (SBER), which is the LDAP RFC standard, or the encoded packet is encrypted if the WebGate and Access servers are configured to support SSL. If SSL was not configured and you were able to take a network trace of the WebGate to Access Server conversation, you would not see "password" in the packet capture but it would be relatively easy to determine what the encoded password was.
- Conversations between the Access Server and the Active Directory domain controller are the same as the WebGate to Access Server scenario as are conversations between a COREid Server and an Active Directory domain controller.

Authentication

A user establishes a connection to a directory server by performing a *bind* operation. Part of the information used in performing this operation is the user's identity and password. The three basic bind mechanisms are anonymous, simple, or secure.

The simplest bind mechanism is an anonymous bind. Access is granted based on the user having no identity within the directory. While it is normal to provide read access to certain entries and attributes for anonymous users, most application data will be protected against retrieval by unknown users.

A simple bind operation is performed when the user provides a distinguished name (DN) for an entry within the directory and a password that goes with that entry. The entry must have a unicodePwd attribute, which is checked against the password provided. If the bind is successful, the user's identity will become that DN for the duration of the connection and access to entries will be based on that identity.

While the simple bind is adequate for most environments, it requires that you send the password over the network using lightweight basic encoding rules (LBER). Some directory servers implement secure authentication methods, such as Kerberos or certificate-based authentication like SSL. Any authentication method that is used must resolve to a directory entry to permit a comparison with the access control list (ACL). After authentication, the ACL specifies access controls that are based on the DN for the user.

Oblix NetPoint uses simple binds when authenticating users to Active Directory regardless of whether using LDAP or ADSI.

Table 11 outlines the authentication options available with the build of Oblix NetPoint used for lab testing (6.0.1.1):

Table 11 Oblix NetPoint Authentication Methods by Server Type for LDAP and ADSI

Traffic	Protocol	SSL	Payload	Port	PKI Required
Access Server to Active Directory	LDAP	No	Encoded using LBER	389	No
Access Server to Active Directory	LDAP	Yes	Encrypted	636	Yes
COREid Server to Active Directory	LDAP	(ADSI requires SSL)	Encrypted	636	Yes
Access Server to Active Directory	ADSI	No (option only available in build 6.0.1.1)	Encoded using LBER	389	No
Access Server to Active Directory	ADSI	Yes	Encrypted	636	Yes
COREid Server to Active Directory	ADSI	(ADSI requires SSL)	Encrypted	636	Yes

All LoadRunner tests were conducted without SSL for Access Server to Active Directory authentication.