Secure LDAP Server

Scott McGee
August 24, 2003

GIAC Certified UNIX Security Administrator (GCUX)
Practical Assignment
Version 1.9 – Option 1

Table of Contents

Abstract

The purpose of this paper is to guide a systems administrator or security engineer through the setup of a secure LDAP server running Sun ONE Directory Server 5.1 on Solaris 8. Securing an LDAP server consists of locking down the server, setting up proper access controls, encryption and many software bug workarounds. This paper focuses on a transition from a NIS or files based directory service to secure LDAP.

Conventions

The following text conventions are used in this paper:

- **Section headings are Arial 14 pt bold.**
- Normal text is Arial 12 pt
- Hyperlinks are Arial 12 pt

```
- UNIX input/output is Courier 10 pt
- "#" or "root@cypher:/ :" are commands that must be run as root.
- "$" or "[smcgee@client smcgee]$" are commands that can be run as a user.
- Responses are in bold.
```

1 Introduction

Directory services form the core of a network infrastructure. A directory is a database that is optimized for read access. A directory service provides a simple way to look up complex information. The type of data that is typically stored for use with the Solaris 8 Operating Environment (OE) includes users, groups, aliases, hosts, netmasks, protocols, rpc, services, netgroups, ethers, bootparams and automounts. This set of data is common across the three main directory services available to Solaris: NIS, NIS+ and LDAP.

1.1 LDAP

From the OpenLDAP Faq-O-Matic[1]:

> Lightweight Directory Access Protocol (LDAP) is an open-standard protocol for accessing X.500 directory services. The protocol runs over Internet transport protocols, such as TCP.
>
> LDAP is a lightweight alternative to the X.500 Directory Access Protocol (DAP) for use on the Internet. It uses TCP/IP stack verses the overly complex OSI stack. It also has other simplifications, such as the representing most attribute values and many protocol items as textual strings, that are designed to make clients easier to implement. LDAP version 3 (LDAPv3) is an Internet "Proposed Standard" and is documented by the various RFCs, including:
>
> RFC 2251: Lightweight Directory Access Protocol (v3)
> RFC 2252: LDAPv3: Attribute Syntax Definitions
> RFC 2253: LDAPv3: UTF-8 String Representation of Distinguished Names
> RFC 2254: The String Representation of LDAP Search Filters
> RFC 2255: The LDAP URL Format
> RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3
> RFC 2829: Authentication Methods for LDAP
> RFC 2830: LDAPv3: Extension for Transport Layer Security
> RFC 3377: Lightweight Directory Access Protocol (v3): Technical Specification
>
> Copies of these documents can be obtained from the RFC-Editor (http://www.rfc-editor.org/).[2]

The OpenLDAP Faq-O-Matic has many other explanations of how LDAP is used and the LDAPv3 protocol.

1.2 Design Goals

The specific implementation that this document outlines is the Sun Solaris 8 OE and Sun ONE Directory Server 5.1 Service Pack 2. The goal is to convert from a NIS centric directory service to an LDAP based directory service without removing functionality. The domain name and structure of the directory are designed for the easiest transition from NIS to LDAP.

1.3 Security

Security was a driving force in the implementation of this architecture. The key security benefits realized from moving from NIS to LDAP are:

[1] http://www.openldap.org/faq/data/cache/1.html
[2] http://www.openldap.org/faq/data/cache/29.html

- User passwords are not world readable (even in crypt format)
- All traffic between the client and server is encrypted with 128 bit Secure Sockets Layer (SSL) encryption
- The server can lockout an account after repeated failed authentication attempts.
- Users are forced to change their password after a preset time period.
- A password history is stored requiring users to pick new unique passwords.
- Clients must authenticate before access is granted to the directory.

1.4 An Example

This document is to be used as a step-by-step example installation. For this example, shomo.com is the domain name. For LDAP, this corresponds to a base suffix of dc=shomo,dc=com. The hostname of the server is “cypher” and its Internet Protocol (IP) address is 192.168.1.20. A secondary LDAP server is “neo” at 192.168.1.25. Replace these values with the appropriate names and values for your environment.

1.5 Server Configuration

The servers that are setup in this example are two SunFire V120 [3] servers. Each server has a 550 or 650 MHz Ultrasparc IIi processor and 1.5 gigabytes of RAM. The configuration also has one 36-gigabyte hard drive per server. A second 36-gigabyte hard drive may be used for mirroring. Neither server is internally redundant, but both servers are cheap enough that a pair can be used for high availability requirements. The servers are running Solaris 8 OE. With a few changes to the specific commands, this document can also be used to setup Solaris 9 LDAP servers.

In their final state, the multi-master servers will be providing LDAP directory services to an internal network. User authentication data, hostname resolution and automount tables will be stored in the directory. They will be running Sun ONE Directory Server 5.1 Service Pack 2 and allow access through OpenSSH (current version is 3.6.1p2). Sun ONE Directory Server was previously named iPlanet Directory Server and was owned by Netscape. There are references to both Sun ONE and iPlanet throughout this document. They are the same product. For security hardening, YASSP is used. The LDAP servers will not be accessible to the public or to the Internet.

1.6 Requirements

The following tools, software and patches are required for this installation of LDAP. See the Tools section (Section 9.3) for the location where each can be obtained.

[3] http://www.sun.com/servers/entry/v120/index.html

- Sun ONE Directory Server 5.1 Service Pack 2
- Certutil (in the Sun ONE DS Resource Kit 5.1 or from Netscape/Mozilla)
- OpenSSL[4]
- YASSP[5]
- Sun Solaris 8 Patches:
    - 108993-23 or higher (The following are prerequisites for this patch)
        - 111023-02
        - 108528-13
        - 108989-01
        - 110386-01

For a Solaris 9 server, the following packages are required (installed in SUNWCXall installation):

IPLTadcon
IPLTadman
IPLTadmin
IPLTcons
IPLTdscon
IPLTdsman
IPLTdsr
IPLTdsu
IPLTjss
IPLTnls
IPLTnspr
IPLTnss
IPLTpldap

This installation also assumes the use of a self-generated and signed Certificate Authority (CA) keypair and certificate. The private key and self-signed certificate for the CA are required. This is how to create a Certificate Authority (CA) certificate. You will use the CA private key and certificate to trust any certificates signed by the CA.

Create the CA's keypair in a temp directory:

```
root@cypher:/ : mkdir /opt/DS51
root@cypher:/ : cd /opt/DS51
root@cypher:/DS51 : /usr/local/ssl/bin/openssl req -new -out cert.csr
Using configuration from /usr/local/ssl/openssl.cnf
Generating a 1024 bit RSA private key
...............++++++
.............++++++
writing new private key to 'privkey.pem'
Enter PEM pass phrase:
Verifying password - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
```

[4] http://www.openssl.org
[5] http://www.yassp.org/

```
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:Encinitas
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Shomo Technical
Systems
Organizational Unit Name (eg, section) []:Certificate Authority
Common Name (eg, YOUR name) []:Shomo
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:<password>
An optional company name []:
```

Self-sign CA's certificate:

```
root@cypher:/ : /usr/local/ssl/bin/openssl x509 -req -in cert.csr \
    -signkey privkey.pem -out cacert.pem -days 9999
Signature ok
subject=/C=US/ST=California/L=Encinitas/O=Shomo Technical
Systems/OU=Certificate Authority/CN=Shomo
Getting Private key
Enter PEM pass phrase: <password>
```

Where:

-req signifies an X.509 certificate signing request
-in denotes the certificate request file
-signkey denotes the CA private key file
-out denotes the output file name of the signed certificate
-days denotes the duration in days of the certificate
(9999 days is about 27 years)

A public certificate authority can also be used. Instead of signing the certificate request, send it to the CA of your choice and install the signed certificate that is sent back.

1.7 Risk Analysis

There are a number of risks or exploitation scenarios inherent in a directory service. The most likely vector for attacks is from inside the network from authenticated users, unless providing a public LDAP service. Most risks involve unauthorized access to the contents of the directory. Some are from authorized users accessing data or fields in the directory they do not have permission to access. See the next section for steps on how to mitigate these risks.

The first threat to the directory server is from unauthorized queries. By enumerating the contents of the directory, it is possible to determine such sensitive information as account names, lists of hostnames and corresponding IP addresses, and the names of NFS file servers. An attacker could use this information in formulating a plan of attack against a network.

Another threat to a directory server is unauthorized access to the userPassword field. This problem has plagued NIS and Microsoft Windows password stores. If a user can retrieve the encrypted password for each user, they can crack them at their leisure. If using the crypt function to encrypt user passwords, programs such as “crack” or “John the Ripper” facilitate offline password cracking. A user only needs to have read/write access to their own userPassword field in order to authenticate and change their passwords. They should not be able to retrieve the userPassword field from other user’s accounts.

Intercepting authentication data can compromise a user’s password. If authentication data is sent unencrypted over the network, it can be intercepted using a network sniffer such as “snoop” in Solaris or “tcpdump”. Gaining access to a valid user account is an entry point into the network. Specifically when using a centralized authentication source such as LDAP, an account may provide remote access, access to fileservers, and email.

The attack that is hardest to detect involves unauthorized modification of data in the directory. The risk is that the data in the directory can no longer be trusted and even backups of the data might be corrupted or have backdoor accounts added. If the Directory Manager’s account is compromised, the entire directory could be modified, including timestamps and access rights. A compromise of the Replication Manager’s account also gives access to the majority of the data in the directory.

1.8 Risk Mitigation

Steps can be taken to minimize the threats outlined above to the Sun ONE Directory server and the data it contains. In order to prevent unauthorized queries to the directory server, a host-based firewall can be used. If configured properly, a host-based firewall will limit access to ports 389 and 636 on the directory server to just those hosts that are LDAP clients. The proxyagent user is created to allow clients to authenticate users. Each client must authenticate as the proxyagent user in order to verify user accounts. The proxyagent account is kept secret.

Access to the userPassword field is blocked by Access Control Instructions [6] (ACIs). The ACIs that are setup on the server by default deny access to a user’s userPassword field except to that user. With the changes made to the ACIs for the proxyagent user, even the proxyagent cannot access the userPassword field. Users only need to be able to write and modify their passwords. They do not require read access either.

To prevent interception of authentication data, TLS/SSL encryption is used for all connections to the directory server. Passwords can also be hashed before being sent to the directory using MD5 or SASL. When using TLS/SSL encryption, the passwords are not hashed, but the entire communication is encrypted using 128-bit encryption. For ldapsearch commands that require binding as the Directory Manager, administrators should first ssh to the

[6] iPlanet Directory Server 5.1 Administrator’s Guide

directory server and then run the command locally. For all administrative access to the directory server, ssh is used to encrypt all communication. In addition, replication between servers is done through TLS/SSL encryption.

Preventing unauthorized changes to the directory rely upon protecting the two main administrative accounts. They are the Directory Manager (cn=Directory Manager) and the Replication Manager (uid=RManager,cn=config). Both accounts can read and write to the entire contents of the directory. Both accounts should use passwords with at least eight characters and a special character, number and capital letter. Any access using these accounts should be through TLS/SSL or protected by an ssh session. If either of these accounts is compromised, the data in the directory should not be trusted.

1.9 Open Ports and Access Control

By default, the server listens on port 389 for unencrypted LDAP connections and port 636 for TLS/SSL connections. When all clients utilize TLS/SSL, or encrypted connections, port 389 should be blocked using a host based packet filter. In order for Solaris 8 clients to connect using encryption, they must have a copy of the Certificate Authority's self-signed encryption certificate in /var/ldap. Turning off port 389 will stop manual searches using the /usr/bin/ldapsearch command because it does not utilize encryption. The ldaplist and ldapaddent commands will still work.

The Sun ONE Administrative server, which is required to use the GUI, listens on a high port specified during the installation. In this example, it is set to port 15000. The Administrative Server should be left off and only turned on when the GUI is required. The Server is effectively a web server that requires authentication.

Limiting client connections can be accomplished by limiting connections to ports 389 and 636 by using a host-based packet-filtering firewall. Ipfilter[7] can be configured on Solaris to control access to those ports.

1.10 The LDAP Protocol

The University of Oulu and VTT Electronics teamed up ("PROTOS[8] - Security Testing of Protocol Implementations") to test the most popular implementations of LDAP directory servers available for handling version 3 of the LDAP protocol. The PROTOS project developed a test suite in Java that tests LDAP v3 servers for handling exceptions. 12649 different test cases were tried against each server. Some of the tests against the iPlanet Directory Server 5.0 Beta showed evidence of buffer overflow and format string vulnerabilities[9]. According to Sun, versions 5.0 and newer are not vulnerable to these. The PROTOS project provides the source of the tests for download.

[7] http://coombs.anu.edu.au/~avalon/
[8] http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/ldapv3/
[9] See CERT Advisory CA-2001-18

A recent Bugtraq[10] posting[11] pointed out a directory traversal vulnerability in Sun iPlanet Administration Server 5.1. The Administration Server runs as root, so enumeration of the shadow file or other sensitive files is possible. This bug is fixed in Sun ONE Directory Server 5.2 or in iPlanet 5.1 Service Pack 2 Hotfix 2. Unfortunately, Hotfix 2 is only available for support customers. The mitigating factor with this vulnerability is that the Administration Server requires authentication as the Directory Manager. Frequently, the Directory Manager account and the root account are managed by the same administrator.

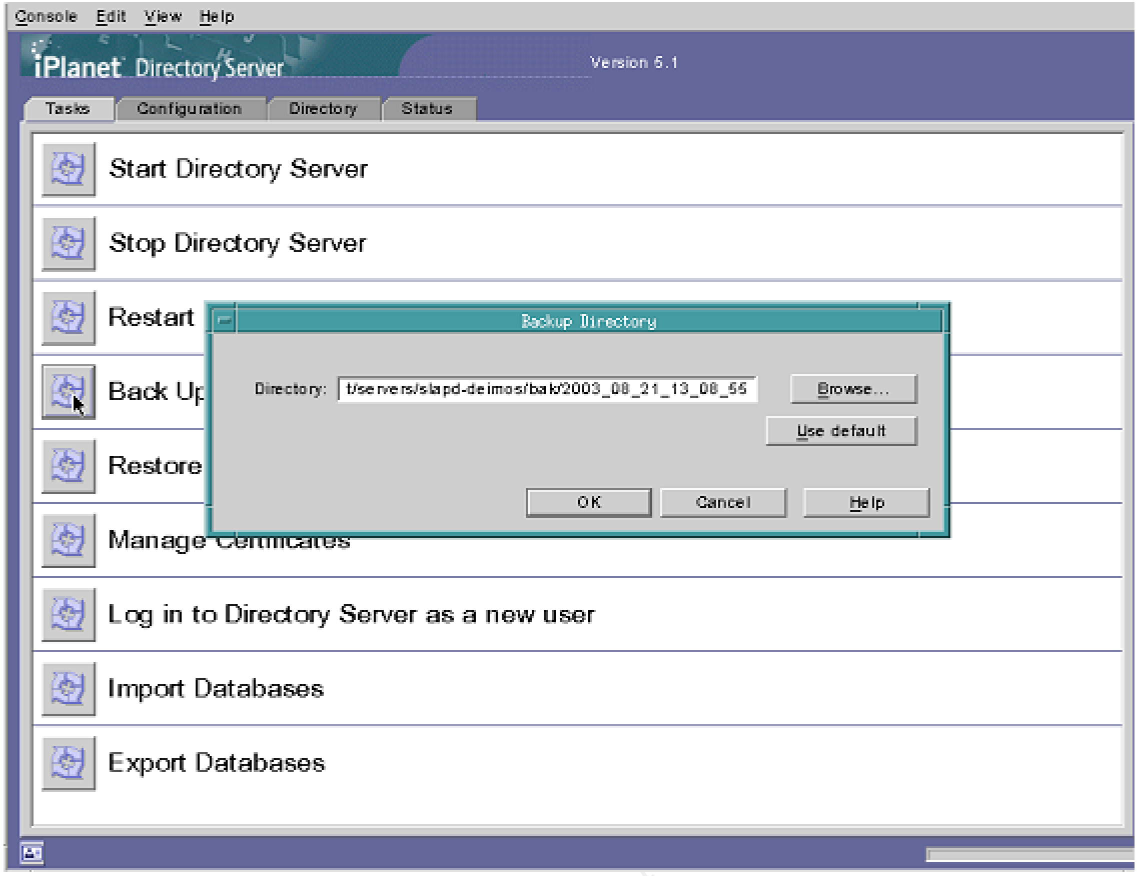
SPI Dynamics has written a whitepaper[12] on LDAP injection attacks. This form of attack only applies to sites that have created web based or form based interactive applications that work with the LDAP Directory. The attacks are very similar in nature to web-based SQL injection attacks where user input is not properly filtered. It is very important to filter from user input all characters except those that are specifically allowed characters.

1.11 Ongoing Maintenance

An LDAP server, like NIS, NIS+ or Active Directory requires routine maintenance to keep it running smoothly. Since it is a mission critical component of any network, frequent backups of user and host data is critical. When using multi-master replication, occasionally conflicts can occur between master servers, which must be resolved. Finally, frequent auditing of user account data will prevent unauthorized access and ensure that formers user's accounts are inactivated.

Backups of user and host data must be done frequently to guard against the catastrophic loss of both multi-master servers or from corruption of the directory server database. Sun ONE Directory Server provides for making a copy or backup of the database while the server is running through the Console GUI. Go to the Tasks tab -> Backup Directory. It will put a copy of the running database in a backup directory with the current date and time. To restore, select Restore Directory and choose the date and time that you wish to restore.

[10] http://www.securityfocus.com/archive/1
[11] http://www.securityfocus.com/archive/1/332399
[12] http://www.spidynamics.com/mktg/LDAP1/index.html



Directory: t/servers/slapd-deimos/bak/2003_08_21_13_08_55

Sun ONE Directory Server also allows backups and restores from the command line. To backup[13] the server while it is running, run:

```
# /usr/iplanet/servers/slapd-`hostname`/db2bak
```

This will create a backup directory under /usr/iplanet/servers/slapd-`hostname`/bak/<date> with the current date. The command can be automated using a cron job such as:

```
55 23 * * * /usr/iplanet/servers/slapd-`hostname`/db2bak > /dev/null 2>&1
```

Once per night at 23:55, the directory will be backed up. The /bak directory can then be backed up by network backup software. Ensure that there is enough space in the /usr/iplanet partition because there will be 365 backups per year. To restore from the command line, the directory server must be turned off. Use these commands with the backup directory to restore as the only argument:

```
# /usr/iplanet/servers/slapd-`hostname`/bak2db \
      /usr/iplanet/servers/slapd-`hostname`/bak/<date>
```

[13] iPlanet Directory Server 5.1 Administrator's Guide

When using multi-master replication, occasionally an object will be changed on both servers at the same time or a modification will be made that cannot replicate to the other server. Sun ONE Directory Server will flag the entry with an "`nsds5ReplConflict`" flag. It is possible to conduct an ldapsearch to check for the existence of these flags. Any items flagged as conflicting will need to be manually resolved between the servers:

```
$ ldapsearch -D "cn=Directory Manager" -b "dc=shomo,dc=com"
"nsds5ReplConflict=*"
```

See Sun's online documentation[14] for instructions on how to fix items that have a conflict:

Frequent auditing of user account data will help prevent unauthorized access. Verify that disabled accounts remain disabled and that no backdoor accounts have been created. A simple search of the user accounts using ldapsearch, getent or ldapaddent returns a list of accounts. Use the following commands on an LDAP client as any user to enumerate user accounts:

```
$ ldapaddent -d passwd
$ getent passwd
```

To retrieve more information on each account, use ldapsearch with a search filter of "uid=*". This search will return the uid number, description, password expiration time and if their account is locked:

```
$ ldapsearch -h cypher -b dc=shomo,dc=com "uid=*" \
uid uidnumber gecos passwordexpirationtime nsaccountlock

…
uid=test,ou=people,dc=shomo,dc=com
uid=test
uidnumber=602
gecos=Test User
passwordexpirationtime=20031018203741Z
nsaccountlock=true
```

[14] http://docs.sun.com/source/816-5606-10/replicat_new.htm

2 Solaris 8 Server Setup

2.1 Install a Minimized and Secure Solaris 8 OE

Install a minimized Solaris 8 Operating Environment. See the Jumpstart profile in the Appendix (Section 9). Next, install the latest recommended patch cluster from Sun. To secure the system, follow the recommendations in the *SANS Solaris Security Step by Step*.[15] Many of these hardening techniques are automated in the YASSP (Yet Another Solaris Security Program) toolkit[16]. A quick checklist of the steps to follow are below, which are a subset of YASSP and *SANS Solaris Security Step by Step*. All of them require root access.

Stop routing on the server (YASSP):

```
# touch /etc/notrouter
```

Turn off services that are not needed. This server will not have any NFS mounts nor be a client of any other directory service. In the bourne shell (sh or bash):

```
# cd /etc/rc2.d
for file in S30sysid.net S71sysid.sys S72autoinstall S73nfs.client S74autofs
*cache* S71rpc S76nscd S71ldap.client S88sendmail S80PRESERVE
do
      mv $file _$file
done
mv /etc/rc3.d/S15nfs.server /etc/rc3.d/_S15nfs.server
```

Edit /etc/init.d/syslog and add a “-t” to “/usr/sbin/syslogd –t > /dev/msglog 2>&1 &” to stop syslogd from listening for connections (YASSP).

Add to /etc/system (YASSP):

```
set noexec_user_stack=1
set noexec_user_stack_log=1
set sys:coredumpsize=0
set nfssrv:nfs_portmon=1
```

Remove NFS configuration files (YASSP):

```
# rm /etc/auto_master /etc/auto_home /etc/auto_direct /etc/dfs/dfstab
```

Add logging to all local file systems in /etc/vfstab. Example:

[15] Pomeranz, Pages 1-21

[16] http://www.yassp.org/

```
fd      -       /dev/fd fd      -       no      -
/proc   -       /proc   proc    -       no      -
/dev/dsk/c0t0d0s1  -       -       swap    -       no      -
/dev/dsk/c0t0d0s0 /dev/rdsk/c0t0d0s0      /       ufs     1       no
logging
/dev/dsk/c0t0d0s4 /dev/rdsk/c0t0d0s4      /usr    ufs     1       no
logging
/dev/dsk/c0t0d0s3 /dev/rdsk/c0t0d0s3      /var    ufs     1       no
logging
/dev/dsk/c0t0d0s5 /dev/rdsk/c0t0d0s5 /export/home    ufs     2       yes
logging
/dev/dsk/c0t0d0s7 /dev/rdsk/c0t0d0s7      /ODS    ufs     2       yes     -
/dev/dsk/c0t0d0s6 /dev/rdsk/c0t0d0s6      /opt    ufs     2       yes
logging
swap    -       /tmp    tmpfs   -       yes     -
```

Add extra syslog logging (YASSP):

```
# touch /var/log/authlog
# chown root /var/log/authlog
# chmod 600 /var/log/authlog
# touch /var/adm/loginlog
# chmod 600 /var/adm/loginlog
# chown root:sys /var/adm/loginlog
```

Add to /etc/syslog.conf:

```
auth.info         /var/log/authlog
```

Turn on BSM (Basic Security Module) audit logging as desired:

```
# echo y | /etc/security/bsmconv
```

Add to /etc/security/audit_control, as appropriate for your environment:

```
dir:/var/audit
flags:lo,ad,-all,^-fm
naflags:lo,ad
minfree:20
```

Remove the following users from /etc/passwd and /etc/shadow and change the shells for the rest, in a bourne shell (YASSP):

```
# for user in uucp nuucp lp smtp listen nobody4
do
      /usr/sbin/passmgmt –d $user
done

for user in adm daemon bin nobody noaccess
do
      /usr/sbin/passmgmt –m –s /usr/sbin/noshell $user
done
```

Remove .rhosts support from /etc/pam.conf (YASSP):

```
# grep –v rhosts_auth /etc/pam.conf > /etc/pam.new
# mv /etc/pam.new /etc/pam.conf
# chown root:sys /etc/pam.conf
# chmod 644 /etc/pam.conf
```

Prevent certain files that have security vulnerabilities from being written to:

```
# for file in /.rhosts /.shosts /.netrc /etc/hosts.equiv
do
      cp /dev/null $file
      chown root:root $file
      chmod 000 $file
done
```

Prevent any user but root from using cron or at jobs (YASSP):

```
# cd /etc/cron.d
# rm –f cron.deny at.deny
# echo root > cron.allow
# echo root > at.allow
# chown root:root cron.allow at.allow
# chmod 400 cron.allow at.allow
```

Create /etc/issue or /etc/motd with warnings appropriate for your environment:

```
# echo “Authorized uses only.  All access may be logged.” > /etc/motd
# eeprom oem-banner=“Authorized uses only.  All access may be logged.”
# eeprom oem-banner\?=true
```

Change in /etc/default/login (YASSP):

```
TIMEOUT=60
UMASK=077
SYSLOG=YES
```

In /etc/default/kbd, set:

```
KEYBOARD_ABORT=disable
```

In /etc/default/inetinit, set (YASSP):

```
TCP_STRONG_ISS=2
```

Edit /etc/inittab and remove the following line to disable serial line logins (YASSP):

```
#sc:234:respawn:/usr/lib/saf/sac –t 300
```

Add local user accounts for those who will administer the server. Install and configure “sudo”[17] for the local users who require root access.

Build and install Zlib[18], OpenSSL[19], and OpenSSH[20]. Do not allow root logins (PermitRootLogin no) through OpenSSH. See the brief OpenSSH ssh_config file recommended in the Appendix, Section 9.2. Once OpenSSH is installed, turn off inetd:

```
# rm /etc/inet/inetd.conf /etc/inetd.conf
```

Configure /etc/inet/ntp.conf (NTP = Network Time Protocol) if there is a time source on the network. For log analysis and time correlation, NTP is highly recommended.

Reboot and verify the changes are persistent before proceeding. OpenSSH should be the only service running (port open) and there should be very few processes running on the server (not showing BSM auditing):

```
     UID   PID  PPID  C    STIME TTY      TIME CMD
    root     0     0  0   Aug 04 ?        0:12 sched
    root     1     0  0   Aug 04 ?        0:01 /etc/init -
    root     2     0  0   Aug 04 ?        0:00 pageout
    root     3     0  0   Aug 04 ?       90:34 fsflush
    root   199     1  0   Aug 04 console  0:00 /usr/lib/saf/ttymon -g -h -p
cypher console login:  -T sun -d /dev/console -l c
    root 10590     1  0 23:58:03 ?        0:00 /usr/sbin/syslogd -t
    root   186     1  0   Aug 04 ?        0:00 /usr/sbin/cron
  smcgee 10615 10613  0 20:51:10 ?        0:00 /opt/ssh/sbin/sshd
    root   202     1  0   Aug 04 ?        0:00 /usr/lib/inet/xntpd
    root 10613   329  0 20:51:07 ?        0:00 /opt/ssh/sbin/sshd
  smcgee 10617 10615  0 20:51:10 pts/1    0:00 -bash
    root 10638 10617  0 20:51:32 pts/1    0:00 ps -ef
    root   329     1  0   Aug 05 ?        0:00 /opt/ssh/sbin/sshd
```

2.2 Setup Sun ONE Directory Server 5.1

See the checklist in the Appendix, Section 9.8 for an outline of the steps required to setup the secure LDAP server. Conduct the installation as root. Create a temp directory for the install data:

```
# cd /opt
# mkdir DS51
```

[17] http://www.courtesan.com/sudo/ or ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/sudo-1.6.7p5-sol8-sparc-local.gz
[18] http://www.gzip.org/zlib/
[19] http://www.openssl.org/
[20] http://www.openssh.com/ ,
Also see *OpenSSH – A Survival Guide for Secure Shell Handling* https://store.sans.org//store_item.php?item=86

```
# mv directory-5.1sp2-us.sparc-sun-solaris2.8.tar.gz[21] DS51
# cd DS51
# gunzip -c directory-5.1sp2-us.sparc-sun-solaris2.8.tar.gz | tar xvf -
```

Create the “iplanet” user so the directory server runs as an unprivileged user:

```
# groupadd –g 636 iplanet
# useradd –u 636 -d /usr/iplanet -s /bin/false –g iplanet –c “iPlanet User” \
      iplanet
```

Idsktune will analyze the patch level and kernel settings of the system. It will make recommendations as to required patches and changes to the TCP/IP kernel settings. Some of the changes are not required and are only recommendations. It may also recommend patches that have already been obseleted by newer patches.

```
# ./idsktune -q
```

The server should be a standalone machine. It should not use NIS, NIS+ or LDAP for directory services. It should use local files for hostname lookups and authentication information so it is not reliant upon another machine. NFS mounts should also be avoided. The server will need to have its own fully qualified domain name (FQDN) in its /etc/hosts file. It is also required to have every client in its /etc/hosts file. They do not all have to be FQDNs. The `domainname` command should return the correct value for the installation. In this case, the `domainname` command should return “shomo.com”.

In a redundant server environment, another goal is to have each LDAP server be independent from other servers. Each server will have its own Administration Server that will house the configuration information. Sun ONE Directory Server allows configuring one master administration server, but this reduces the independence of each server.

The required patches include:

- Sun Solaris 8 Patches:
  - 108993-23 or higher (The following are prerequisites for this patch)[22]
    - 111023-02
    - 108528-13
    - 108989-01
    - 110386-01

Start the installation by running setup from the command line (responses in **bold**):

```
# cd /opt/DS51
# ./setup

      Select the items you would like to install [1]: 1
            1. iPlanet Servers
```

[21] Download from: http://wwws.sun.com/software/download/products/3e5beea5.html
[22] 108993-23 README

```
       Choose an installation type [2]: 2
             2. Typical installation
       Install location [/usr/iplanet/servers]: /usr/iplanet/servers
       iPlanet Server Products components [All]: All
       Server Core Components components [1, 2, 3]: 1, 2, 3
       iPlanet Directory Suite components [1, 2]: 1, 2
       Administration Services components [1, 2]: 1, 2
       Computer name [cypher.shomo.com]: cypher.shomo.com
       System User [nobody]: iplanet
       System Group [nobody]: iplanet
       Do you want to register this software with an existing
             iPlanet configuration directory server? [No]: No
       Do you want to use another directory to store your data? [No]: No
       Directory server network port [389]: 389
       Directory server identifier [cypher]: cypher
       administrator ID [admin]: admin
             password:
       Suffix [dc=shomo, dc=com]: dc=shomo, dc=com
       Directory Manager DN [cn=Directory Manager]: cn=Directory Manager
             Password:
       Administration Domain [shomo.com]: shomo.com
       Administration port [7079[23]]: 15000
       Run Administration Server as [root]: root


Extracting Netscape core components...
Extracting Server Core Components...
Extracting Core Java classes...
Extracting Java Runtime Environment...
Extracting iPlanet Directory Server...
Extracting iPlanet Directory Server Console...
Extracting iPlanet Administration Server...
Extracting Administration Server Console...
Extracting nsPerl 5.005_03...
Extracting PerLDAP 1.4.1...

[slapd-cypher]: starting up server ...
[slapd-cypher]: [14/Aug/2003:11:19:19 -0700] - iPlanet-Directory/5.1 Service
Pack 2 B2003.028.2338 starting up
[slapd-cypher]: [14/Aug/2003:11:19:25 -0700] - slapd started.  Listening on
all interfaces port 389 for LDAP requests
Your new directory server has been started.
Created new Directory Server
Start Slapd  Starting Slapd server configuration.


Success Slapd Added Directory Server information to Configuration Server.
Configuring Administration Server...
Your parameters are now entered into the Administration Server
database, and the Administration Server will be started.

Changing ownership to admin user root...
Setting up Administration Server Instance...
```

[23] This port is randomly chosen and will be different for every install. The chosen port is arbitrary but it is helpful to stay consistent across servers.

```
Configuring Administration Tasks in Directory Server...
Configuring Global Parameters in Directory Server...
iPlanet-WebServer-Enterprise/6.0SP2 B01/06/2003 22:24

warning: daemon is running as super-user

[LS ls1] http://cypher.shomo.com, port 15000 ready to accept requests

startup: server started successfully


Press Return to continue...

Go to /usr/iplanet/servers and type startconsole to begin
managing your servers.

cypher#
```

2.3 Directory Server Commands

To start the Sun ONE Directory Server:

```
# /usr/iplanet/servers/slapd-`hostname`/start-slapd
```

To stop the Sun ONE Directory Server:

```
# /usr/iplanet/servers/slapd-`hostname`/stop-slapd
```

To start the Administrative Server:

```
# /usr/iplanet/servers/start-admin
```

To stop the Administrative Server:

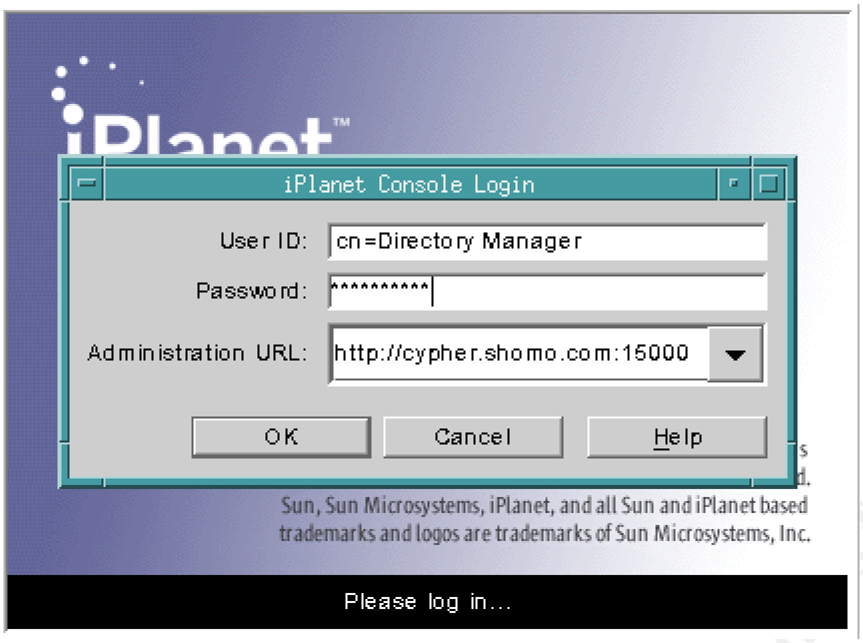
```
# /usr/iplanet/servers/stop-admin
```

To Start Administrative Console (GUI):

```
$ /usr/iplanet/servers/startconsole
```

To login to the Administrative Console, use (see the image below):

User ID: “cn=Directory Manager”
Password: <password>
Administration URL: http://cypher.shomo.com:15000



User ID: cn=Directory Manager

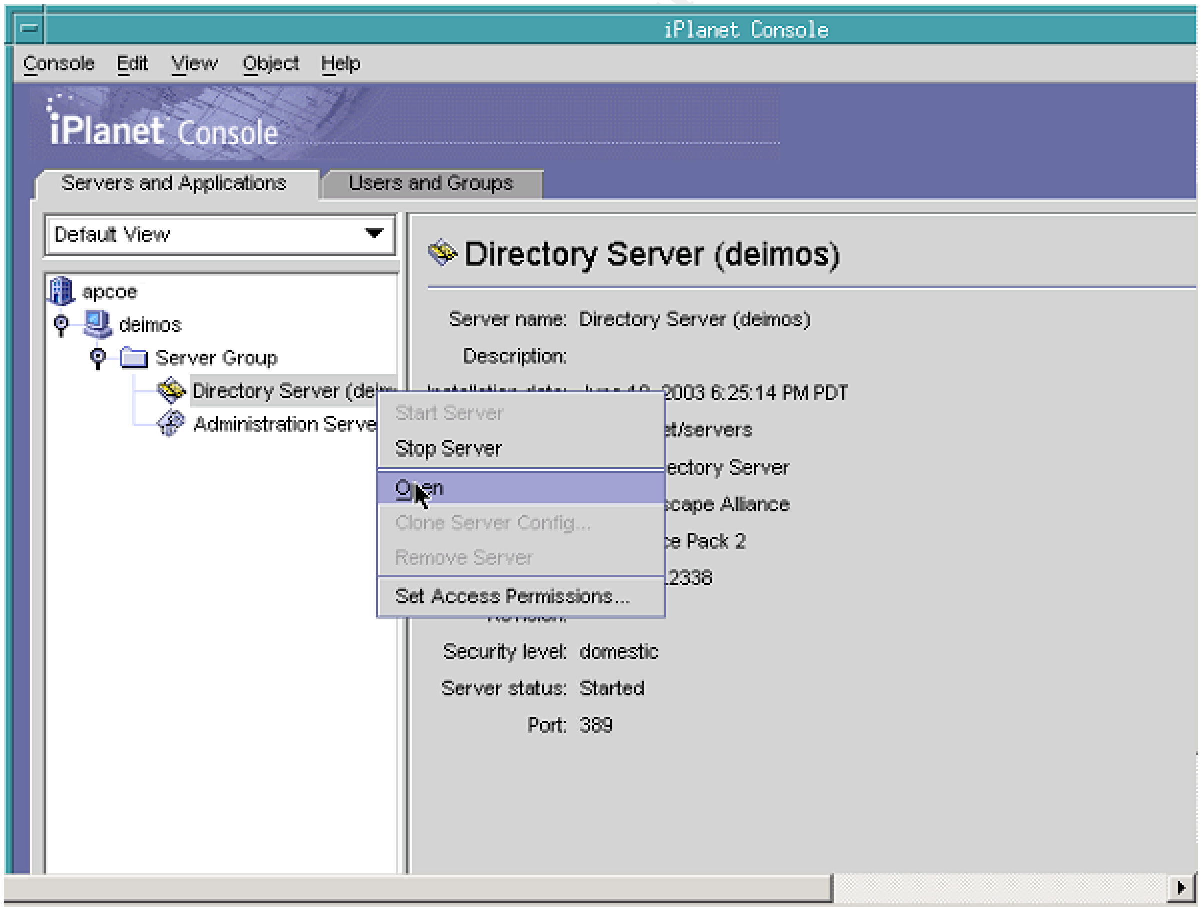
Password: **********

Administration URL: http://cypher.shomo.com:15000

Sun, Sun Microsystems, iPlanet, and all Sun and iPlanet based trademarks and logos are trademarks of Sun Microsystems, Inc.

Please log in...

This will launch the iPlanet Console. From the console (see image below), select and expand the server fully qualified domain name. Expand the Server Group and then the Directory Server. Double click or right click -> Open the Directory Server.



Directory Server (deimos)

Server name: Directory Server (deimos)

Description:

Installation date: June 10, 2003 6:25:14 PM PDT

et/servers

ectory Server

cape Alliance

e Pack 2

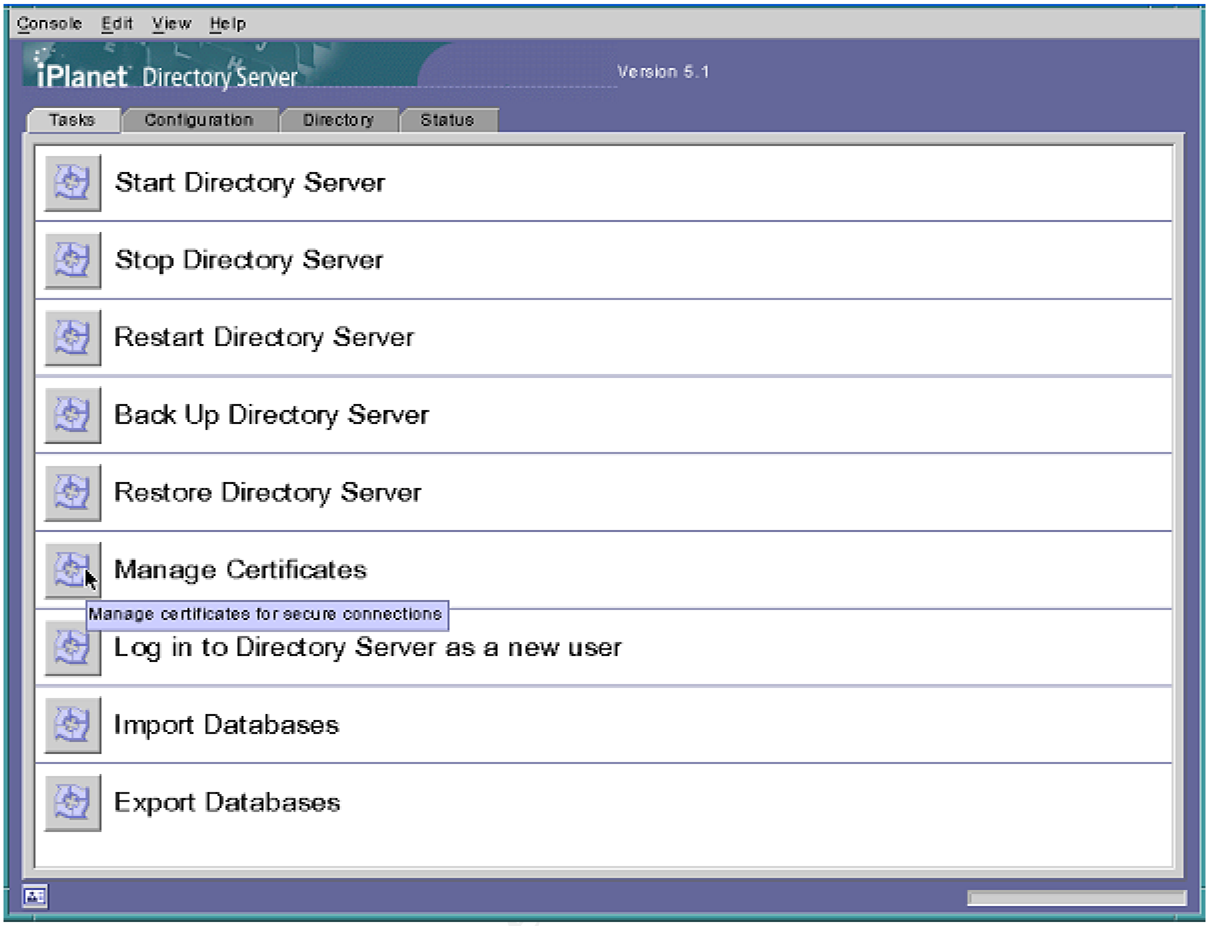
2338

Security level: domestic

Server status: Started

Port: 389

This will launch a second window with the actual directory.



The server will not start automatically upon reboot without an init script. Create one that calls /usr/iplanet/servers/slapd-`hostname`/start-slapd and /usr/iplanet/servers/start-admin. An example init script is in the Appendix (Section 8.4). It should be placed in /etc/init.d and named directory.

```
# chown root:sys /etc/init.d/directory
# chmod 755 /etc/init.d/directory
# ln -s /etc/init.d/directory /etc/rc3.d/S60directory
```

2.4 Configure Sun ONE Server for Solaris OE LDAP Client

In order to use Sun ONE Directory Server with native Solaris LDAP clients, the server needs special schema and database indexing. This also creates a client profile. The client profile defines the list of servers, the preferred server, the authentication method and level. Initially, we setup a profile with proxy level authentication and simple as the authentication method. Proxy level authentication requires each client to authenticate to the server using a proxyagent user account. Simple authentication uses username and password in cleartext.

Secure LDAP Server

After encryption is setup, we will use Transport Layer Security (TLS) encryption along with username and passwords.

First, the schema in Solaris 8 must be corrected. Make a backup of the 10rfc2307.ldif schema file:

```
# cd /usr/iplanet/servers/slapd-`hostname`/config/schema
# cp 10rfc2307.ldif 10rfc2307.ldif.orig
```

Edit the 10rfc2307.ldif schema file and remove two lines that contain automount entries with the following OIDs:

attributeTypes: (1.3.6.1.1.1.1.25 NAME ‘automountInformation’ …)
objectClasses: (1.3.6.1.1.1.2.9 NAME ‘automount’ …)

```
# cd /usr/iplanet/servers/slapd-`hostname`/config/schema
# cp 10rfc2307.ldif 10rfc2307.ldif.orig
# grep -v automount 10rfc2307.ldif > 10rfc2307.ldif.new
# mv 10rfc2307.ldif.new 10rfc2307.ldif
# /usr/iplanet/servers/slapd-`hostname`/restart-slapd
```

The schema for Solaris 8 will now match the schema for Solaris 9 and 10 and idsconfig will work properly. Restart the directory server so that the changes will take affect:

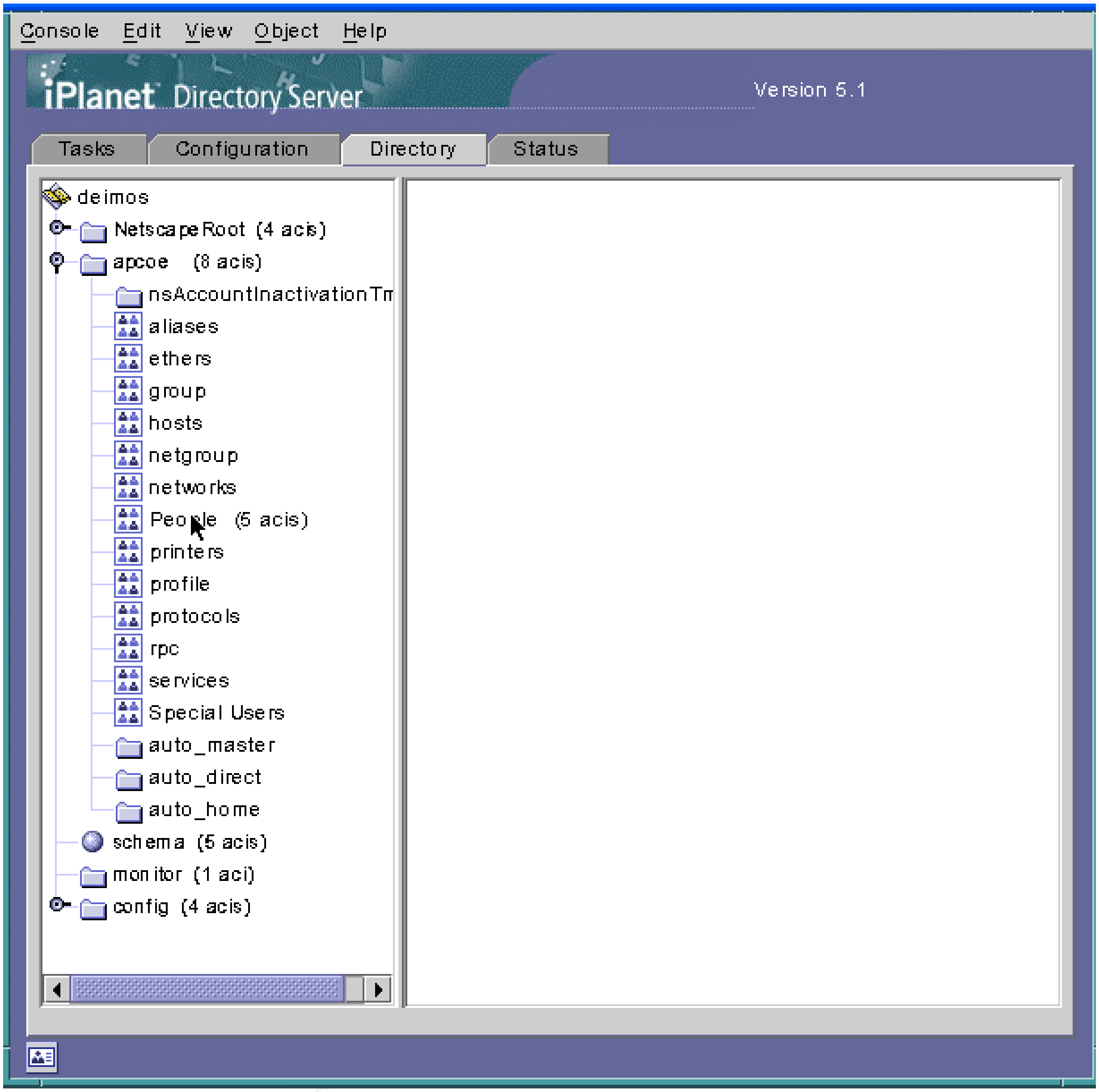
Idsconfig is the tool used to setup the server and create the profile (responses in **bold**):

```
# /usr/lib/ldap/Idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the iPlanet Directory Server's (iDS) hostname to setup: cypher
Enter the port number for iDS (h=help): [389] 389
Enter the directory manager DN: [cn=Directory Manager] cn=Directory Manager
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [shomo.com]  shomo.com
Enter LDAP Base DN (h=help): [dc=shomo,dc=com] dc=shomo,dc=com
Enter the profile name (h=help): [default] default
Default server list (h=help): [192.168.1.20] 192.168.1.20
Preferred server list (h=help):
Choose desired search scope (one, sub, h=help):  [one] one
The following are the supported credential levels:
  1  anonymous
  2  proxy
  3  proxy anonymous
Choose Credential level [h=help]: [1] 2
The following are the supported Authentication Methods:
  1  none
  2  simple
```

```
   3  sasl/DIGEST-MD5
   4  tls:simple
   5  tls:sasl/DIGEST-MD5
Choose Authentication Method (h=help): [1] 2

Current authenticationMethod: simple

Do you want to add another Authentication Method? n
Do you want the clients to follow referrals (y/n/h)? [n] n
Do you want to modify the server timelimit value (y/n/h)? [n] n
Do you want to modify the server sizelimit value (y/n/h)? [n] n
Do you want to store passwords in "crypt" format (y/n/h)? [n] y
Do you want to setup a Service Authentication Methods (y/n/h)? [n] n
Client search time limit in seconds (h=help): [30] 30
Profile Time To Live in seconds (h=help): [43200] 43200
Bind time limit in seconds (h=help): [10] 10
Do you wish to setup Service Search Descriptors (y/n/h)? [n] n



              Summary of Configuration

   1  Domain to serve               : shomo.com
   2  Base DN to setup              : dc=shomo,dc=com
   3  Profile name to create        : default
   4  Default Server List           : 192.168.1.20
   5  Preferred Server List         :
   6  Default Search Scope          : one
   7  Credential Level              : proxy
   8  Authentication Method         : simple
   9  Enable Follow Referrals       : FALSE
  10  iDS Time Limit                :
  11  iDS Size Limit                :
  12  Enable crypt password storage : TRUE
  13  Service Auth Method pam_ldap  :
  14  Service Auth Method keyserv   :
  15  Service Auth Method passwd-cmd :
  16  Search Time Limit             : 30
  17  Profile Time to Live          : 43200
  18  Bind Limit                    : 10
  19  Service Search Descriptors Menu

Enter config value to change: (1-19 0=commit changes) [0] 0
Enter DN for proxy agent: [cn=proxyagent,ou=profile,dc=shomo,dc=com]
Enter passwd for proxyagent:
Re-enter passwd:

WARNING: About to start committing changes. (y=continue, n=EXIT) y

   1. Changed passwordstoragescheme to "crypt" in cn=config.
   2. Schema attributes have been updated.
   3. Schema objectclass definitions have been added.
   4. NisDomainObject added to dc=shomo,dc=com.
   5. Top level "ou" containers complete.
   6. automount maps: auto_home auto_direct auto_master auto_shared processed.
   7. ACI for dc=shomo,dc=com modified to disable self modify.
   8. Add of VLV Access Control Information (ACI).
  9. Proxy Agent cn=proxyagent,ou=profile,dc=shomo,dc=com added.
  10. Give cn=proxyagent,ou=profile,dc=shomo,dc=com read permission for
password.
  11. Generated client profile and loaded on server.
  12. Processing eq,pres indexes:
      ipHostNumber (eq,pres)   Finished indexing.
      uidNumber (eq,pres)   Finished indexing.
      ipNetworkNumber (eq,pres)   Finished indexing.
      gidnumber (eq,pres)   Finished indexing.
      oncrpcnumber (eq,pres)   Finished indexing.
      automountKey (eq,pres)   Finished indexing.
  13. Processing eq,pres,sub indexes:
      membernisnetgroup (eq,pres,sub)   Finished indexing.
      nisnetgrouptriple (eq,pres,sub)   Finished indexing.
  14. Processing VLV indexes:
      shomo.com.getgrent vlv_index   Entry created
      shomo.com.gethostent vlv_index   Entry created
      shomo.com.getnetent vlv_index   Entry created
      shomo.com.getpwent vlv_index   Entry created
      shomo.com.getrpcent vlv_index   Entry created
      shomo.com.getspent vlv_index   Entry created

idsconfig: Setup of iDS server cypher is complete.


Note: idsconfig has created entries for VLV indexes.  Use the
      directoryserver(1m) script on cypher to stop
      the server and then enter the following vlvindex
      sub-commands to create the actual VLV indexes:

  directoryserver -s <server-instance> vlvindex -n userRoot -T
shomo.com.getgrent
  directoryserver -s <server-instance> vlvindex -n userRoot -T
shomo.com.gethostent
  directoryserver -s <server-instance> vlvindex -n userRoot -T
shomo.com.getnetent
  directoryserver -s <server-instance> vlvindex -n userRoot -T
shomo.com.getpwent
  directoryserver -s <server-instance> vlvindex -n userRoot -T
shomo.com.getrpcent
  directoryserver -s <server-instance> vlvindex -n userRoot -T
shomo.com.getspent
cypher#
```

The proxyagent account will be setup on each client to authenticate to the server. After idsconfig has run, there will be new containers in the directory. Looking at the Directory tab in the Sun ONE GUI should look similar[24] to the following:

[24] The auto_ tables will show up once they are populated in Section 2.6.



2.5 VLVIndexes for Improved Performance

After using idsconfig, the vlvindex commands will be printed out. However, these commands will only work on a Solaris 9 server (where DS 5.1 is installed using packages). Use the following commands instead. These commands will speed up database searches by creating indexes for each table.[25]

First, stop the Directory Server:

```
# /usr/iplanet/servers/slapd-`hostname`/stop-slapd
```

Then replace `hostname` with the name of the server instance if it doesn't match the hostname:

```
# /usr/iplanet/servers/slapd-`hostname`/vlvindex  -s `hostname` -n userRoot -
T `domainname`.getgrent

# /usr/iplanet/servers/slapd-`hostname`/vlvindex  -s `hostname` -n userRoot -
T `domainname`.gethostent

# /usr/iplanet/servers/slapd-`hostname`/vlvindex  -s `hostname` -n userRoot -
T `domainname`.getnetent

# /usr/iplanet/servers/slapd-`hostname`/vlvindex  -s `hostname` -n userRoot -
T `domainname`.getpwent

# /usr/iplanet/servers/slapd-`hostname`/vlvindex  -s `hostname` -n userRoot -
T `domainname`.getrpcent

# /usr/iplanet/servers/slapd-`hostname`/vlvindex  -s `hostname` -n userRoot -
T `domainname`.getspent
```

The server will print out error messages saying that it will have to brute force create the index. This is because the tables do not have any data in them. The indexes are still created correctly.

Finally, start the directory server up again:

```
# /usr/iplanet/servers/slapd-`hostname`/start-slapd
```

You can search for these indexes by using the following command line search:

```
$ ldapsearch –h `hostname` –b "cn=userRoot,cn=ldbm
database,cn=plugins,cn=config" "objectClass=vlv*"
```

There are two types of vlvindex entries, search (objectClass=vlvsearch) entries and index (objectClass=vlvindex) entries.

Example of a vlvsearch index:

```
cn=shomo.com_group_vlv_index,cn=userRoot,cn=ldbm
database,cn=plugins,cn=config
objectClass=top
objectClass=vlvSearch
cn=shomo.com_group_vlv_index
vlvBase=ou=group,dc=shomo,dc=com
vlvScope=1
vlvFilter=(objectClass=posixGroup)
```

[25] iPlanet Directory Server 5.1 Administrator's Guide

Example of a vlvindex index:

```
cn=shomo.com.getgrent,cn=shomo.com_group_vlv_index,cn=userRoot,cn=ldbm
database,cn=plugins,cn=config
cn=shomo.com.getgrent
vlvSort=cn uid
objectClass=top
objectClass=vlvIndex
vlvEnabled=1
vlvUses=0
```

2.6 Populate the Directory

Convert the Solaris 8 server to be a client of itself. This is not an officially supported function, but it is useful to populate the server with NIS or files data. The other option is to convert another machine to be a client. Ldapclient [26]is the tool used to convert a native Solaris 8 client to use LDAP instead of NIS, NIS+, or local files:

```
cypher# ldapclient -D cn=proxyagent,ou=profile,dc=shomo,dc=com \
-d shomo.com -P default cypher
credentialLevel requires proxyPassword
Proxy Bind Password:
System successfully configured
cypher#
```

Where:

-D is the proxyagent distinguished name (dn)
-d is the domain name
-P is the profile name
cypher is the server name

Collect NIS or files data in one location. Place them in /opt/DS51/maps. Certain maps need to be the originals, such as the auto_*, hosts, aliases and netgroups file and will come from a NIS master. The rest can be collected with ypcat. Ldapaddent is used to enter the data into the directory server in the correct format. The passwd file requires an additional -p switch to denote that the password field is included and not in a shadow file. If a shadow file is input, do not use the "-p" switch. Ldapaddent [27]must be run on an LDAP client. There is no option to specify a certain LDAP server, so it relies upon the client configuration.

[26] "Solaris 8 Enhanced LDAP Naming Services Feature Patch Documentation", Page 71.
[27] "Solaris 8 Enhanced LDAP Naming Services Feature Patch Documentation", Pages 64-65.

```
$ cd /opt/DS51/maps
$ ldapaddent -c -a simple -D "cn=Directory Manager" -p -f ./passwd passwd
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./group group
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./aliases aliases
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./auto_home auto_home
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./auto_master
auto_master
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./auto_direct
auto_direct
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./hosts hosts
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./netgroup netgroup
```

Where:

-c specifies to continue if it encounters an error or a duplicate record
-a specifies the authentication mechanism
-D is the authentication username
-f is the file to use
-p specifies the crypt password field is in the passwd file
The last entry is the type of map to load

- Verify the amount of data entered for each file with the number of entries in the LDAP database and compare to the item count under the hosts folder in the directory console:

```
$ wc -l /opt/DS51/maps/hosts
```

- Check automount entries for naming:
Ex: "auto_home" instead of "auto.home"

Copy the hosts file containing all of the clients into /etc/inet/hosts on the LDAP server. The server must have the ip address and hostname for all clients for SSL to work:

```
# cp /opt/DS51/maps/hosts /etc/inet/hosts
```

Uninitialize the Solaris 8 server so it is a standalone machine.

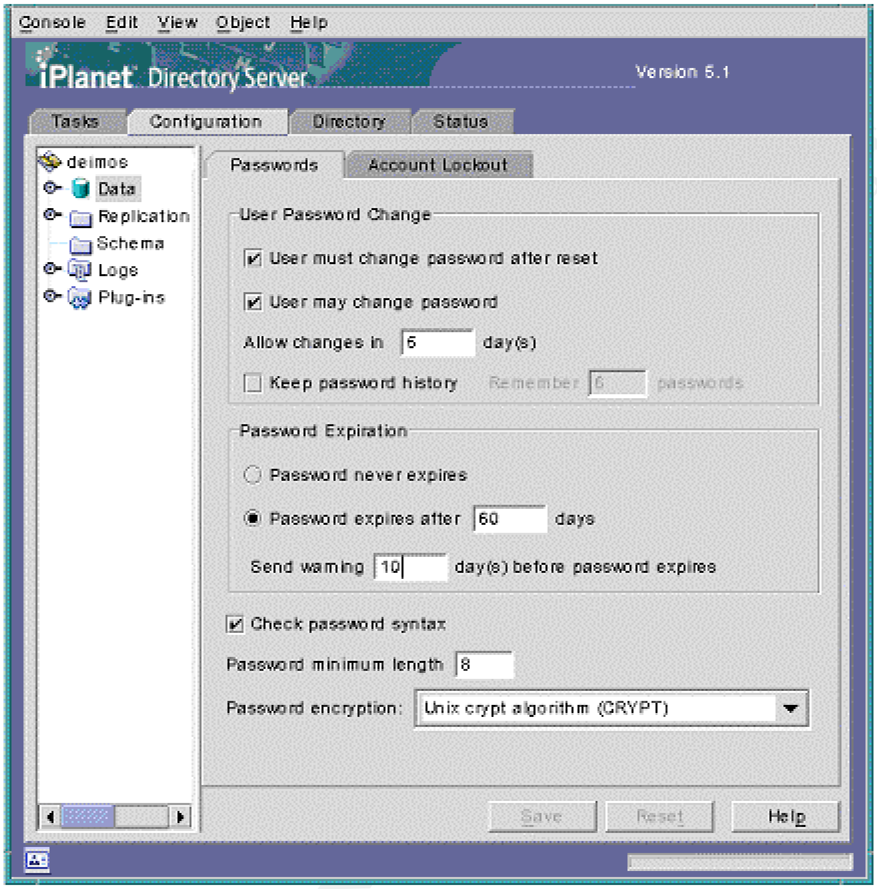
```
root@cypher:# ldapclient -u
System successfully unconfigured
root@cypher:#  ls /var/ldap
cachemgr.log
root@cypher:#  ps –ef | grep [l]dap_cachemgr
root@cypher:#
```

Verify it is no longer a client by checking the contents of /var/ldap. It should not contain ldap_client_file or ldap_client_cred file and the *ldap_cachemgr* process should not be running.

2.7 Account Security Settings for the Server

In the Sun ONE GUI, change the security settings for passwords and account lockouts. The following values are recommended, but may be changed according to local security requirements.

Go to: Configuration tab -> Data icon



User Password Change

☑ User must change password after reset

☑ User may change password

Allow changes in 6 day(s)

□ Keep password history Remember 6 passwords

Password Expiration

○ Password never expires

● Password expires after 60 days

Send warning 10 day(s) before password expires

☑ Check password syntax

Password minimum length 8

Password encryption: Unix crypt algorithm (CRYPT)

Password Options:

- ✓ User must change password after a reset
- ✓ User may change password
  Allow changes in 6 days
- ✓ Keep password history: Remember 4 passwords
- • Password expires after 60 days
  Send warning 10 days before password expires
- ✓ Check password syntax
  Password minimum length: 8
  Password encryption: UNIX Crypt Algorithm (CRYPT)

A password history is stored forcing users to pick new unique passwords. Up to 24 passwords can be stored for each user.

Account Lockout Options:

- ✓ Accounts may be locked out
  Password Lockout:
  Lockout account after 3 login failures
  Reset failure count after 10 minutes
- Lockout forever

2.8 Create Replication User

Create a special user account that will allow replication between servers. This account has access rights to read and write to the entire directory and is used for replication between servers. Be sure to keep the account data private.

In the Sun ONE GUI, add Replication Manager Account[28]
- Directory -> Config -> right click -> New User

First Name: Replication
Last Name: Manager
uid=RManager,cn=config

Set a unique password that will only be used for replication. Select Advanced, then Add Attribute "passwordexpirationtime" so that password aging won't affect RManager:

passwordexpirationtime = 20380119031407Z[29]

2.9 Correct the Proxyagent Read Permission ACI

In order to secure the userPassword fields from public query (using “ldapaddent –d shadow”), the “read” permission must be removed from the proxyagent account’s access control. The proxyagent is only required to verify the user’s account exists. After this query, the LDAP client binds to the server as the user when using the pam_ldap module. This change is also required to enable the account security features included in the directory server including password expiration and account lockout. This change has to be made in conjunction with using the custom /etc/pam.conf in Section 8.2. ***Warning: Making this change may break authentication with rsh/rlogin using .rhosts unless the pam.conf***

[28] iPlanet Directory Server 5.1 Administrator's Guide
[29] iPlanet Directory Server 5.1 Administrator's Guide

configuration in the Appendix is used. OpenSSH using RSA/DSA public key authentication is broken by this in a similar manner. Sun is currently examining this issue to determine whether is it a problem in the PAM libraries or in OpenSSH. At this time, OpenSSH (3.6.1p2) does not support forcing password changes upon login without using a custom patch[30]. Check newer versions for this feature. Change the following ACI[31] on your directory server to remove "read" permission:

ACI Before:

```
(target="ldap:///dc=shomo,dc=com")(targetattr="userPassword")(version 3.0;
acl LDAP_Naming_Services_proxy_password_read; allow (compare,read,search)
userdn = "ldap:/// cn=proxyagent,ou=profile,dc=shomo,dc=com ";)
```

ACI After:

```
(target="ldap:/// dc=shomo,dc=com ")(targetattr="userPassword")(version 3.0;
acl LDAP_Naming_Services_proxy_password_read; allow (compare,search) userdn =
"ldap:/// cn=proxyagent,ou=profile,dc=shomo,dc=com";)
```

Right click on the base domain, for example - shomo (8 acis), and click “Select Access Permissions” or control-I, then select “LDAP_Naming_Services_proxy_password_read”. Click Edit and remove the word “read” from “allow (compare,*read*,search)”. Select “Check Syntax” and then “OK”.

The ACIs can be checked from the command line using ldapsearch:

```
$ ldapsearch -h cypher -b "dc=shomo,dc=com" "entrydn=dc=shomo,dc=com" aci
```

[30] http://www.zip.com.au/~dtucker/openssh
[31] Mark - iPlanet Support Engineer

3 Encryption

3.1 Generate a Server Certificate Request

Generate a Certificate Request [32]through the Sun ONE "Manage Certificates" Tool in the GUI. Go to the Directory Server window, select the Tasks tab, and click on the “Manage Certificates” button. You will be prompted to create a new password that will protect your encryption certificates. In the “Manage Certificates” window, select the “Server Certs” tab and click on the Request button at the bottom. Select “Request certificate manually” and then Next. Enter the fully qualified domain name for the “Server name” and the Organization as appropriate. Click Next. Enter the password you set above and click Next. Save the CSR to a text file named cypher_iplanet.csr under /opt/DS51/keys directory (create a new directory if necessary). Then select Done. If you have not created a self-signed Certificate Authority keypair and certificate, see the Requirements (Section 1.5).

3.2 Sign the Server Certificate

Sign the Sun ONE certificate request with the CA's private key:

```
root@cypher:keys : openssl x509 -req -in cypher_iplanet.csr \
-CA cacert.pem -CAkey privkey.pem -CAcreateserial  \
-out cypher_iplanet_cert.pem -days 9999[33]
```

Where:

-req signifies an X.509 certificate signing request
-in denotes the certificate request file
-CA denotes the CA certificate file
-CAkey denotes the CA private key file
-CAcreateserial -This is required the first time a key is signed by a CA.
-out denotes the output file name of the signed certificate
-days denotes the duration in days of the certificate
(9999 days is about 27 years)

It will prompt for the Certificate Authority’s private key pass phrase.

```
Signature ok
subject=/C=US/ST=California/L=Encinitas/O=Shomo Technical
Systems/OU=shomo.com/CN=cypher
Getting CA Private Key
Enter PEM pass phrase: <password>
```

You can print out the server certificate to verify the values and expiration date:

[32] iPlanet Directory Server 5.1 Administrator's Guide
[33] MAN page for openssl

```
root@cypher:keys : openssl x509 -text -in cypher_iplanet_cert.pem
```

Where:

-text means print the output in text format
-in denotes the certificate request file

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=US, ST=California, L=Encinitas, O=Shomo Technical Systems,
OU=Certificate Authority, CN=Shomo
        Validity
            Not Before: Dec 31 19:04:47 2002 GMT
            Not After : Jan 30 19:04:47 2030 GMT
        Subject: C=US, ST=California, L=Encinitas, O=Shomo Technical Systems,
OU=shomo.com, CN=cypher
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:ce:8b:6a:6e:38:35:7a:6d:fa:85:07:3f:84:bc:
                    4c:30:be:f2:ee:f0:8b:04:aa:bc:67:07:d0:1e:c3:
                    68:53:59:08:8a:b5:b8:08:e2:96:56:73:36:43:b5:
                    36:27:aa:55:ba:51:a3:ec:22:bd:55:c5:2c:0a:71:
                    59:a6:60:b2:94:2f:04:6a:55:1b:64:1f:5c:b1:ac:
                    c0:d8:f3:71:6d:10:6a:37:bd:f8:80:37:87:81:07:
                    fd:68:be:96:32:eb:48:d4:c1:b0:8e:aa:66:c6:c0:
                    9c:17:c6:19:fd:a5:c1:76:2b:89:8f:bd:67:75:c0:
                    8e:4f:bd:60:c3:2c:31:01:0b
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        68:57:76:eb:fc:67:71:0e:3b:15:d5:4c:55:1f:f9:ee:8d:31:
        b7:a7:d0:d7:9e:d7:64:73:bd:e3:9f:6c:da:ce:e3:87:cc:80:
        43:85:fe:18:74:8a:3c:8f:bc:35:33:f4:41:e6:41:75:96:f7:
        17:e7:7e:7a:bc:f2:9d:3e:c1:d2:95:9d:c1:6a:74:0f:cf:0e:
        c5:01:1e:4f:04:09:05:ed:48:e0:23:57:61:0c:3d:be:49:a3:
        c6:41:56:ef:86:b4:97:57:c4:ae:8e:e7:b3:d6:2d:ee:e3:4b:
        ca:05:c3:3d:93:97:96:85:81:db:30:c8:23:7c:d6:c1:60:40:
        90:2f
-----BEGIN CERTIFICATE-----
MIICcjCCAdsCAQEwDQYJKoZIhvcNAQEEBQAwgYgxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZ
m9ybmlhMRIwEAYDVQQHEwlFbmNpbml0YXMxIDAeBgNVBAoTF1Nob21vIFRlY2huaWNhbCBTeXN0ZW
1zMR4wHAYDVQQLExVDZXJ0aWZpY2F0ZSBBdXRob3JpdHkxDjAMBgNVBAMTBVNob21vMB4XDTAyMTI
zMTE5MDQ0N1oXDTAzMDEzMDE5MDQ0N1owejELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Ju
aWExEjAQBgNVBAcTCUVuY2luaXRhczEgMB4GA1UEChMXU2hvbW8gVGVjaG5pY2FsIFN5c3RlbXMxE
jAQBgNVBAsTCXNob21vLmNvbTEMMAoGA1UEAxMDbmDAQABMA0GCSqGSIb3DQEBBAUAA4GBAGhXduv
8Z3EOOxXVTFUf+e6NMben0Nee12RzveOfbNrO44fMgEOF/hh0ijyPvDUz9EHmQXWW9xfnfnq88p0+
wdKVncFqdA/PDsUBHk8ECQXtSOAjV2EMPb5Jo8ZBVu+GtJdXxK6O57PWLe7jS8oFwz2Tl5aFgdswy
CN81sFgQJAv
-----END CERTIFICATE-----
```

3.3 Install the Signed Server Certificate

The certificate can be installed from the “Manage Certificates” tool or using certutil (see below). Open the “Manage Certificates” window and select the Install button at the bottom. Select the “in this local file:” cypher_iplanet_cert.pem in /opt/DS51/keys/. Install as "server-cert". *It must be named "server-cert" in order for the Sun ONE server to startup correctly.*

The certificate should now be visible in the "Manage Certificates" window.

3.4 Add CA's Certificate to the Certificate Database

The CA’s certificate must be added to the server’s certificate database and given trust. The GUI “Manage Certificates” function does not correctly add a new Certificate Authority certificate. This has been fixed in Directory Server 5.2[34]. A tool named “certutil” can be used to manually add the CA certificate and assign trust to it. Certutil is available from mozilla.org[35] in the Netscape Security Services (NSS) toolkit. This has been tested with NSS version 3.1.4. Newer versions should also work.

Certutil requires Netscape libraries in the iPlanet directory to be in the library path. Use the following in a csh to set the library path:

```
# setenv LD_LIBRARY_PATH “/usr/lib:/usr/iplanet/servers/lib”
```

In a bourne shell (sh or bash), use:

```
# LD_LIBRARY_PATH=/usr/lib:/usr/iplanet/servers/lib
# export LD_LIBRARY_PATH
```

The output of ldd should show all the libraries found:

```
# ldd certutil
        libplc4.so =>    /usr/iplanet/servers/lib/libplc4.so
        libplds4.so =>   /usr/iplanet/servers/lib/libplds4.so
        libnspr4.so =>   /usr/iplanet/servers/lib/libnspr4.so
        libthread.so.1 =>        /usr/lib/libthread.so.1
        libnsl.so.1 =>   /usr/lib/libnsl.so.1
        libsocket.so.1 =>        /usr/lib/libsocket.so.1
        librt.so.1 =>    /usr/lib/librt.so.1
        libdl.so.1 =>    /usr/lib/libdl.so.1
        libc.so.1 =>     /usr/lib/libc.so.1
        libpthread.so.1 =>       /usr/lib/libpthread.so.1
        libmp.so.2 =>    /usr/lib/libmp.so.2
        libaio.so.1 =>   /usr/lib/libaio.so.1
        /usr/platform/SUNW,UltraAX-i2/lib/libc_psr.so.1
```

[34] “Sun ONE Directory Server 5.2 Release Notes”
[35] ftp://ftp.mozilla.org/pub/security/nss/releases/NSS_3_4_1_RTM/SunOS5.8_OPT.OBJ/nss-3.4.1.tar.gz

Make a backup of the current Sun ONE certificate databases:

```
# mkdir /usr/iplanet/servers/alias/bak
# cp -p  /usr/iplanet/servers/alias/slapd-cypher* \
      /usr/iplanet/servers/alias/bak/
```

Add the CA certificate to the database and give trust permissions to it:

```
root@cypher:keys : certutil -A -a -d /usr/iplanet/servers/alias/ \
 -P slapd-cypher- -i /opt/DS51/keys/cacert.pem \
 -t "TCu,TCu,TCu" -n shomo_CA[36]

Enter Pin for "NSS Certificate DB":
```

Where:

-A denotes "add"
-a denotes ASCII input format
-d denotes the path to the databases
-P denotes the database prefix (slapd-cypher-cert7.db)
-i is the CA certificate to add to the database
-t denotes the trust arguments to assign to the CA certificate
-n is the name to give the CA certificate

List the certificates in the Sun ONE cert database:

```
root@cypher:keys : certutil -L -d /usr/iplanet/servers/alias/ \
-P slapd-cypher-

shomo_CA                                                 CT,C,C
server-cert                                              u,u,u
```

Where:

-L denotes "list"
-d denotes the path to the databases
-P denotes the database prefix (slapd-cypher- in slapd-cypher-cert7.db)

Print the details of the server certificate from the Sun ONE cert database:

```
root@cypher:keys : certutil -L -d /usr/iplanet/servers/alias/ \
-P slapd-cypher- -n "server-cert"
```

Where:

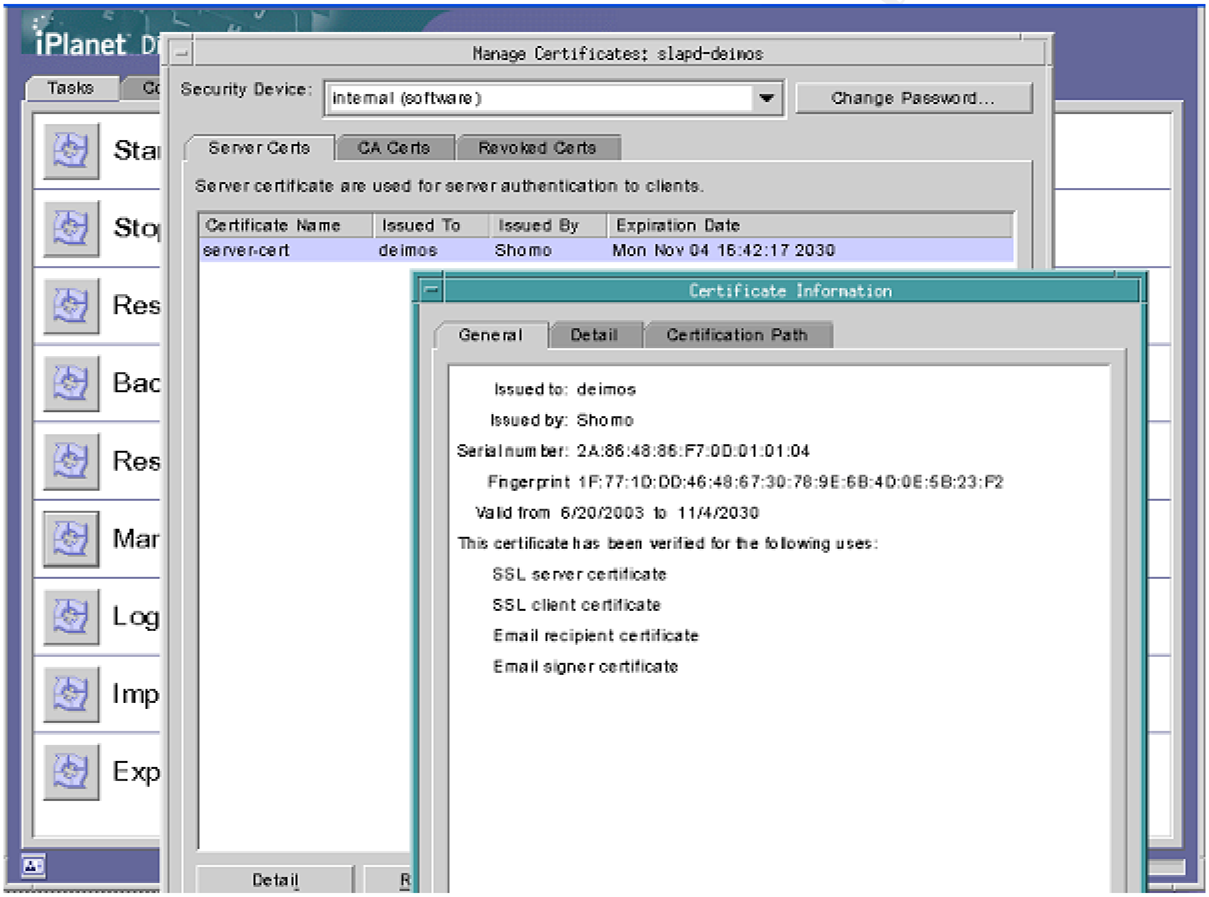
-L denotes "list"
-d denotes the path to the databases
-P denotes the database prefix (slapd-cypher- in slapd-cypher-cert7.db)
-n denotes the alias for the certificate to print

[36] http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html

Create a "pin" file for the Internal Encryption Database for Sun ONE DS 5.1 so the server will start without requesting a password. The file needs to be read-only to root for security:

```
# echo "Internal (Software) Token:<password>" > \
      /usr/iplanet/servers/alias/slapd-`hostname`-pin.txt
# chmod 400 /usr/iplanet/servers/alias/slapd-`hostname`-pin.txt
```

After the CA certificate has been added to the Encryption Database, the certificate details for "server-cert" in the Manage Certificates tool should look similar to the following image. Specifically, the part referring to: "This certificate has been verified for the following uses". Also, the Certification Path should not be a broken path. It should show the CA name above the hostname.



Security Device: internal (software)

Server certificate are used for server authentication to clients.

Certificate Name	Issued To	Issued By	Expiration Date
server-cert	deimos	Shomo	Mon Nov 04 16:42:17 2030

Issued to: deimos
Issued by: Shomo
Serial number: 2A:86:48:86:F7:0D:01:01:04
Fingerprint 1F:77:1D:DD:46:48:67:30:78:9E:6B:4D:0E:5B:23:F2
Valid from 6/20/2003 to 11/4/2030
This certificate has been verified for the following uses:
SSL server certificate
SSL client certificate
Email recipient certificate
Email signer certificate

3.5 Create CA Certificate Database for clients

The LDAP clients require a copy of the CA Certificate in order to use SSL connections to the server. Because the clients will trust the CA, they will implicitly trust any key signed by the CA.

Solaris 8 and 9 clients need a certificate database in the NSS Certificate DB format. To create a new certificate database[37] for use on the clients, use certutil:

```
root@cypher:/ : cd /opt/DS51/keys/
root@cypher:keys : certutil -N -d /opt/DS51/keys
In order to finish creating your database, you
must enter a password which will be used to
encrypt this key and any future keys.

The password must be at least 8 characters long,
and must contain at least one non-alphabetic character.

Enter new password:
Re-enter password:
```

Add the CA certificate to the new cert database:

```
root@cypher:keys : certutil -A -a -d /opt/DS51/keys -i cacert.pem \
-t "TCu,TCu,TCu" -n shomo
Enter Password or Pin for "NSS Certificate DB":
```

Verify the contents of the new cert database:

```
root@cypher:keys : certutil -L -d /export/home/smcgee/ldap_files/ssl
shomo                                                        CT,C,C
```

3.6 Convert Sun ONE Server to Use TLS/SSL Encryption

In the Sun ONE GUI, turn on SSL:
Configuration tab -> Encryption tab
Check:

- ✓ Enable SSL for this server
- ✓ Use this cipher family: RSA

Under Client Authentication:

- Allow client authentication

Then click [Save] at the bottom

Restart the Sun ONE server to turn on SSL:

```
/usr/iplanet/servers/slapd-cypher/restart-slapd
```

If it does not startup correctly, see Server Files (Section 7.2) for how to turn encryption off in the configuration file.

[37] http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html

3.7 Create New Client Profile for Encrypted Authentication

Run /usr/lib/ldap/idsconfig again to create a new client profile that uses encryption. This profile will also reference both multi-master servers, which will be setup later on. The full output of running the command is below (responses in **bold**):

```
[root@cypher /]# /usr/lib/ldap/idsconfig

It is strongly recommended that you BACKUP the directory server
before running idsconfig.

Hit Ctrl-C at any time before the final confirmation to exit.

Do you wish to continue with server setup (y/n/h)? [n] y
Enter the iPlanet Directory Server's (iDS) hostname to setup: cypher
Enter the port number for iDS (h=help): [389] 389
Enter the directory manager DN: [cn=Directory Manager] cn=Directory Manager
Enter passwd for cn=Directory Manager :
Enter the domainname to be served (h=help): [shomo.com] shomo.com
Enter LDAP Base DN (h=help): [dc=shomo,dc=com] dc=shomo,dc=com
Enter the profile name (h=help): [default] ssl
Default server list (h=help): [192.168.1.20]  192.168.1.20, 192.168.1.25
Preferred server list (h=help): 192.168.1.20
Choose desired search scope (one, sub, h=help):  [one] one
The following are the supported credential levels:
  1  anonymous
  2  proxy
  3  proxy anonymous
Choose Credential level [h=help]: [1] 2
The following are the supported Authentication Methods:
  1  none
  2  simple
  3  sasl/DIGEST-MD5
  4  tls:simple
  5  tls:sasl/DIGEST-MD5
Choose Authentication Method (h=help): [1] 4

Current authenticationMethod: tls:simple

Do you want to add another Authentication Method? no
Do you want the clients to follow referrals (y/n/h)? [n] n
Do you want to modify the server timelimit value (y/n/h)? [n] n
Do you want to modify the server sizelimit value (y/n/h)? [n] n
Do you want to store passwords in "crypt" format (y/n/h)? [n] y
Do you want to setup a Service Authentication Methods (y/n/h)? [n] y
Do you want to setup a Service Auth. Method for "pam_ldap" (y/n/h)? [n] y
The following are the supported Authentication Methods:
  1  simple
  2  sasl/DIGEST-MD5
  3  tls:simple
  4  tls:sasl/DIGEST-MD5
Choose Service Authentication Method: [1] 3

Current authenticationMethod: pam_ldap:tls:simple
```

```
Do you want to add another Authentication Method? no
Do you want to setup a Service Auth. Method for "keyserv" (y/n/h)? [n] y
The following are the supported Authentication Methods:
  1  simple
  2  sasl/DIGEST-MD5
  3  tls:simple
  4  tls:sasl/DIGEST-MD5
Choose Service Authentication Method: [1] 3

Current authenticationMethod: keyserv:tls:simple

Do you want to add another Authentication Method? no
Do you want to setup a Service Auth. Method for "passwd-cmd" (y/n/h)? [n] y
The following are the supported Authentication Methods:
  1  simple
  2  sasl/DIGEST-MD5
  3  tls:simple
  4  tls:sasl/DIGEST-MD5
Choose Service Authentication Method: [1] 3

Current authenticationMethod: passwd-cmd:tls:simple

Do you want to add another Authentication Method? no
Client search time limit in seconds (h=help): [30] 30
Profile Time To Live in seconds (h=help): [43200] 43200
Bind time limit in seconds (h=help): [10] 3
Do you wish to setup Service Search Descriptors (y/n/h)? [n] n

              Summary of Configuration

  1  Domain to serve            : shomo.com
  2  Base DN to setup           : dc=shomo,dc=com
  3  Profile name to create     : ssl
  4  Default Server List        : 192.168.1.20, 192.168.1.25
  5  Preferred Server List      : 192.168.1.20
  6  Default Search Scope       : one
  7  Credential Level           : proxy
  8  Authentication Method      : tls:simple
  9  Enable Follow Referrals    : FALSE
 10  iDS Time Limit             :
 11  iDS Size Limit             :
 12  Enable crypt password storage : TRUE
 13  Service Auth Method pam_ldap  : pam_ldap:tls:simple
 14  Service Auth Method keyserv   : keyserv:tls:simple
 15  Service Auth Method passwd-cmd: passwd-cmd:tls:simple
 16  Search Time Limit          : 30
 17  Profile Time to Live       : 43200
 18  Bind Limit                 : 3
 19  Service Search Descriptors Menu

Enter config value to change: (1-19 0=commit changes) [0] 0
Enter DN for proxy agent: [cn=proxyagent,ou=profile,dc=shomo,dc=com]
Enter passwd for proxyagent:
Re-enter passwd:

WARNING: About to start committing changes. (y=continue, n=EXIT) y
```

```
  1. Changed passwordstoragescheme to "crypt" in cn=config.
  2. Schema attributes have been updated.
  3. Schema objectclass definitions have been added.
  4. NisDomainObject for dc=shomo,dc=com was already set.
  5. Top level "ou" containers complete.
  6. automount maps: auto_home auto_direct auto_master auto_shared processed.
  7. Top level ACI LDAP_Naming_Services_deny_write_access already exists for
dc=shomo,dc=com.
  8. Add of VLV Access Control Information (ACI).
  9. Proxy Agent cn=proxyagent,ou=profile,dc=shomo,dc=com already exists.
  10. Proxy ACI LDAP_Naming_Services_proxy_password_read already exists for
dc=shomo,dc=com.
  11. Generated client profile and loaded on server.
  12. Processing eq,pres indexes:
      ipHostNumber (eq,pres) skipped already exists
      uidNumber (eq,pres) skipped already exists
      ipNetworkNumber (eq,pres) skipped already exists
      gidnumber (eq,pres) skipped already exists
      oncrpcnumber (eq,pres) skipped already exists
      automountKey (eq,pres) skipped already exists
  13. Processing eq,pres,sub indexes:
      membernisnetgroup (eq,pres,sub) skipped already exists
      nisnetgrouptriple (eq,pres,sub) skipped already exists
  14. Processing VLV indexes:
      shomo.com.getgrent vlv_index skipped already exists
      shomo.com.gethostent vlv_index skipped already exists
      shomo.com.getnetent vlv_index skipped already exists
      shomo.com.getpwent vlv_index skipped already exists
      shomo.com.getrpcent vlv_index skipped already exists
      shomo.com.getspent vlv_index skipped already exists

idsconfig: Setup of iDS server cypher is complete.
```

4 Replication between Servers

4.1 Setup replication agreement on Primary Solaris 8 Server:

Launch Sun ONE GUI:

```
$ /usr/iplanet/servers/startconsole
```

and open the Directory Server GUI.

Configure Replication:

Configuration -> Replication
- Enable changelog
- Select "default" location
- Select Save

Turn on replication by setting up the type of replica node and by specifying the Supplier DN that will be used to authenticate to this directory. Multi-master replication makes both servers masters and both are able to read and write to the directory.[38]

Configuration -> Replication Node -> highlight Directory
- Check "Enable Replica"
- Select "Multiple Master" in Replica Role
- Common Settings -> specify Replica ID (must be unique among replicas)
- Add Supplier DN used to bind to this replica
    - Enter "uid=RManager,cn=config" and Add and click Save
    - This identifies which local account is the replication account

Configuration -> Replication Node -> Right click on userRoot -> New Replication Agreement
- Enter name "neo_to_cypher_ssl" and description
- Add Consumer "neo" and port 636
- Select "Use SSL for connection"
- Add Replication Manager account info from Secondary Solaris 8 server
    - -Bind As: "uid=RManager,cn=config" and enter password
- Select next -> Always keep directories in sync
- Initialize Consumer now
    - This will populate the Secondary Solaris 8 server with the entire database.

[38] "iPlanet Directory Server 5.1 Administrator's Guide"

4.2 Setup replication agreement on Secondary Solaris 8 Server:

Repeat the same steps as above, except at the Initialize Consumer option:

- Do not initialize Consumer now

5 Solaris 8 Client Setup

5.1 Install patch 111023-02

```
# patchadd 111023-02
```

Synopsis: SunOS 5.8: /kernel/fs/mntfs and /kernel/fs/sparcv9/mntfs patch

5.2 Install patch 108993-23

This patch will take a while:

```
# patchadd 108993-23
```

Synopsis: SunOS 5.8: LDAP2 Patch

5.3 Add the LDAP servers to /etc/inet/hosts on the client

The entries in the local /etc/inet/hosts file on each client must match the encryption certificate on the server. The SSL certificate was created with the fully qualified domain name of the server. The server’s entry in the /etc/inet/hosts file must have the fully qualified server name first and alias second. If not, errors will fill /var/adm/messages like:

```
Aug 20 09:54:52 client.shomo.com login: [ID 605618 auth.error] libldap:
CERT_VerifyCertName: cert server name ‘cypher.shomo.com’ does not match
‘cypher’: SSL connection denied

Aug 20 09:54:52 client.shomo.com login: [ID 293258 auth.error] libsldap:
Status: 85  Mesg: openConnection: simple bind failed[Timed
out][cn=proxyagent,ou=profile,dc=shomo,dc=com]
```

Add the servers to the local /etc/hosts file on each client:

```
# echo “192.168.1.20 cypher.shomo.com cypher” >> /etc/inet/hosts
# echo “192.168.1.25 neo.shomo.com neo” >> /etc/inet/hosts
```

5.4 Copy CA certificate and pam.conf

Copy the CA certificate databases created in Section 3.5 (secmod.db, cert7.db and key3.db) to /var/ldap:

```
# cd /opt/DS51/keys
# cp secmod.db cert7.db key3.db /var/ldap
```

Copy the custom pam.conf to /etc/ (See the Appendix, Section 8.2):

```
# cp /etc/pam.conf /etc/pam.conf.orig
# cp /opt/DS51/pam.conf /etc/pam.conf
```

5.5 Convert to SSL LDAP client using ldapclient

Turn off NIS Client:

```
# /usr/lib/netsvc/yp/ypstop

# ldapclient -D cn=proxyagent,ou=profile,dc=shomo,dc=com \
-d shomo.com -P ssl cypher
Enter Bind password:
```

Where:

-D is the proxyagent distinguished name (dn)
-d is the domain name
-P is the profile name
cypher is the server name

Make sure the proxyagent's password is entered correctly before rebooting. Run `ldaplist` to verify the client can connect to the server. If it is not entered correctly, you will not be able to log in except as root after rebooting. *It does not validate the password when you initialize the client.*

```
# reboot
```

After rebooting, verify that any automounted directories are present and that hostnames, groups and uids resolve correctly.

6 Solaris 9 Client Setup

6.1 Add the LDAP servers to /etc/hosts on the client:

The entries in the local /etc/hosts file on each client must match the encryption certificate on the server. The SSL certificate was created with the fully qualified domain name of the server. The server's entry in the /etc/hosts file must have the fully qualified server name first and alias second.

```
# echo “192.168.1.20 cypher.shomo.com cypher” >> /etc/inet/hosts
# echo “192.168.1.25 neo.shomo.com neo” >> /etc/inet/hosts
```

6.2 Copy CA Certificate and pam.conf

Copy the CA certificate databases created in Section 3.5 (secmod.db, cert7.db and key3.db) to /var/ldap:

```
# cd /opt/DS51/keys
# cp secmod.db cert7.db key3.db /var/ldap
```

Copy the custom pam.conf to /etc/ (See the Appendix, Section 8.2):

```
# cp /etc/pam.conf /etc/pam.conf.orig
# cp /opt/DS51/pam.conf /etc/pam.conf
```

6.3 Convert to SSL LDAP client using ldapclient

```
# ldapclient init -a proxyDn=cn=proxyagent,ou=profile,dc=shomo,dc=com \
-a domainname=shomo.com -a profilename=ssl cypher
```

Where:

-proxyDn is the proxyagent distinguished name (dn)
-domainname is the domain name
-profilename is the profile name
cypher is the server name

```
# reboot
```

After rebooting, verify that any automounted directories are present and that hostnames, groups and uids resolve correctly.

7 LDAP Tools

7.1 Client Tools

The Solaris 8 LDAP tools are located in /usr/bin/ldap*. "ldaplist" is the only binary that correctly uses SSL. The other tools do not use SSL encryption.

For queries to the LDAP database on LDAP clients, use getent. Calling getent without a specific entity will dump all the entries.

```
$ getent hosts neo
192.168.1.25 neo neo.shomo.com

$ getent passwd smcgee
smcgee::600:101:Scott McGee:/home/smcgee:/usr/bin/csh

$ getent group shomo
shomo::101:smcgee,test,test2
```

More complicated queries can be done with the ldapsearch command:

```
$ ldapsearch –h cypher –b dc=shomo,dc=com “cn=smcgee”
```

Where:
-h is the ldap server name
-D is the bind distinguished name (dn) (optional, defaults to bind as current user)
-b is the domain name
cypher is the server name

To add multiple entries to the LDAP database, use /usr/sbin/ldapaddent from an LDAP client:

```
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./group group
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./aliases aliases
$ ldapaddent -c -a simple -D "cn=Directory Manager" -f ./auto_home auto_home
```

For Role Based Access Control (RBAC), use:

```
# /usr/sadm/bin/smrole
```

Netgroups work for limiting login rights to a netgroup of users. In /etc/nsswitch.conf add:

```
passwd: compat files
passwd_compat: ldap

group: compat files
group_compat: ldap
```

Then list the groups in /etc/passwd and /etc/shadow:

```
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
nobody:x:60001:60001:Nobody:/:
+@sys_netgroup
+@shomo_netgroup
+:*:::::/bin/false
```

Netgroups can also be used for limiting which hosts can mount NFS shares. LDAP requires that the hostnames in the netgroups be FQDN (fully qualified domain names). Once the netgroups are created, they can be used in the same manner as NIS and NIS+ netgroups.

On the client, the profile can be refreshed by using the ldap_cachemgr command. It is also started and stopped by /etc/init.d/ldap.client. To show the current status of the LDAP profile, use:

```
$ /usr/lib/ldap/ldap_cachemgr -g[39]
```

and to refresh the profile information, use:

```
# pkill –HUP ldap_cachemgr
```

Note: LDAP returns the fully qualified domain name for hostnames. For example, the .rhosts file on a client requires “cypher.shomo.com” instead of just “cypher”.

7.2 Server Files

The Sun ONE Directory Server 5.1 logs are stored in /usr/iplanet/servers/slapd-`hostname`/logs/. The key logs files to look at are “access” and “errors”. Both logs are useful for troubleshooting connection problems and authentication problems.

The directory server configuration file is /usr/iplanet/servers/slapd-`hostname`/config/dse.ldif. In case the server will not start up, this file can be edited to restore operation. If the server will not start due to an error with the server certificate or other encryption errors, the entries used to turn encryption on and off are:

```
      nsslapd-security:  off/on
      nsSSL3:  off/on
```

[39] MAN ldap_cachemgr

8 Validating the Configuration

8.1 Verify SSL Communication between Directory and Clients

Run snoop on the directory server while authenticating as a user on an LDAP client. The traffic should look similar to the following:

```
# snoop host client and port 389 or host client and port 636
         client -> cypher        TCP D=636 S=58671 Syn Seq=760014120 Len=0
Win=24820 Options=<nop,nop,sackOK,mss 1460>
       cypher -> client          TCP D=58671 S=636 Syn Ack=760014121
Seq=1690915853 Len=0 Win=24820 Options=<nop,nop,sackOK,mss 1460>
         client -> cypher        TCP D=636 S=58671     Ack=1690915854
Seq=760014121 Len=0 Win=24820
         client -> cypher        TCP D=636 S=58671     Ack=1690915854
Seq=760014121 Len=98 Win=24820
       cypher -> client          TCP D=58671 S=636     Ack=760014219
Seq=1690915854 Len=0 Win=24820
       cypher -> client          TCP D=58671 S=636     Ack=760014219
Seq=1690915854 Len=122 Win=24820
         client -> cypher        TCP D=636 S=58671     Ack=1690915976
Seq=760014219 Len=0 Win=24820
         client -> cypher        TCP D=636 S=58671     Ack=1690915976
Seq=760014219 Len=139 Win=24820
       cypher -> client          TCP D=58671 S=636     Ack=760014358
Seq=1690915976 Len=0 Win=24820
       cypher -> client          TCP D=58670 S=636     Ack=759953386
Seq=3752707755 Len=0 Win=24820
         client -> cypher        TCP D=636 S=58670 Fin Ack=3752707755
Seq=759953386 Len=23 Win=24820
```

All the LDAP connections from the client to the server are on port 636 and utilizing TLS/SSL encryption. You can also verify this by looking at the access logs for the server:

```
# cd /usr/iplanet/servers/slapd-`hostname`/logs
# grep 192.168.0.101 access
…
[21/Aug/2003:14:34:46 -0700] conn=683668 fd=64 slot=64 SSL connection from
192.168.1.101 to 192.168.1.20
[21/Aug/2003:14:35:08 -0700] conn=683700 fd=64 slot=64 SSL connection from
192.168.1.101 to 192.168.1.20
[21/Aug/2003:14:35:16 -0700] conn=683701 fd=64 slot=64 SSL connection from
192.168.1.101 to 192.168.1.20
```

192.168.1.101 is the IP address of the client and 192.168.1.20 is the IP address of the LDAP server.

8.2 Encrypted Passwords and Password Enumeration

The user's passwords are encrypted in the directory using the "crypt"[40] function. Users are not able to list their own crypted password and neither are other users. The only users that can read the crypted password fields are the Directory Manager and the Replication Manager. They are special accounts that have full access to the directories. You can verify the permissions, or ACIs, are setup correctly by trying the following commands:

```
[smcgee@client smcgee]$ ldapaddent -d shadow
smcgee:*::::
test:*::::

[smcgee@client smcgee]$ ldapaddent -d passwd
smcgee:*:100:100:Scott McGee:/home/smcgee:/bin/bash:
test:*:602:602:Test User:/home/test:/bin/sh:

[smcgee@client smcgee]$ getent passwd
root:x:0:1:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x Nobody:/:
sshd:x:22:22:sshd privsep:/var/empty:/bin/false
smcgee::100:100:Scott McGee:/home/smcgee:/bin/bash
test::602:602:Test User:/home/test:/bin/sh

[smcgee@client smcgee]$ ldapsearch -h cypher -b dc=shomo,dc=com \
"uid=smcgee" uid gecos userPassword

uid=smcgee,ou=people,dc=shomo,dc=com
uid=smcgee
gecos=Scott McGee
```

The password field in the shadow database, in the password database and the userPassword field are not accessible. However, if you search as the Directory Manager, you can retrieve the userPassword field:

[40] See the crypt man pages.

```
[smcgee@client smcgee]$ ldapsearch -h cypher -b dc=shomo,dc=com \
-D "cn=Directory Manager" "uid=smcgee" uid gecos userPassword

Bind Password:
uid=smcgee,ou=people,dc=shomo,dc=com
uid=smcgee
gecos=Scott McGee
userpassword={crypt}TEGk9ds2ki8s
```

If the ‘read’ ACI is present for the proxyagent user, all users will be able to enumerate the crypted password field for all users, similar to NIS:

```
[smcgee@client2 smcgee]$ ldapaddent -d passwd
smcgee:TEGk9ds2ki8s:100:100:Scott McGee:/home/smcgee:/bin/bash:
test:Oi02e72k38sb:602:602:Test User:/home/test:/bin/sh:
```

8.3 Logging into the Server as Root

When “PermitRootLogin no” is set in sshd_config, root cannot directly login to the server. A local user must login and then su to root or use sudo.

```
[smcgee@client1 smcgee]$ ssh -l root cypher
root@cypher's password:
Permission denied, please try again.
root@cypher's password:
Permission denied, please try again.
root@cypher's password:
Received disconnect: 2: Too many authentication failures for root
```

8.4 Password Expiration, Lockouts and Password Resets

A normal login with a password that will expire in the time allotted in Section 2.7 will display the “Your password will expire in xx days.” message:

```
[smcgee@client1 smcgee]$ ssh client2
smcgee@client2's password:
Your password will expire in 8 days.
Last login: Thu Aug 21 15:17:42 2003 from client1.shomo.com

WARNING:
To protect the system from unauthorized use and to ensure that the system is
functioning properly, activities on this system are monitored and recorded
and subject to audit. Use of this system is expressed consent to such
monitoring and recording. Any unauthorized access or use of this Automated
Information System is prohibited and could be subject to criminal and civil
penalties.

Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
[smcgee@client2 smcgee]$
```

A password that has been reset by the administrator will force the user to set a new password upon login:

```
$ id
uid=602(test) gid=602 (test)
$ ssh client2
test@client2's password:
Warning: Your password has expired, please change it now.
passwd: Changing password for test
Enter existing login password:
New Password:
Re-enter new Password:
passwd: password successfully changed for test
Last login: Tue Aug 19 15:02:30 2003 from client1.shomo.com

WARNING:
To protect the system from unauthorized use and to ensure that the system is
functioning properly, activities on this system are monitored and recorded
and subject to audit. Use of this system is expressed consent to such
monitoring and recording. Any unauthorized access or use of this Automated
Information System is prohibited and could be subject to criminal and civil
penalties.

Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002
$
```

An account that has been locked or inactivated will respond as follows:

```
$ id
uid=602(test) gid=602 (test)
$ ssh client2
test@client2's password:
Connection to client2 closed by remote host.
Connection to client2 closed.
$
```

8.5 Normal Functioning of the Server

You can verify the normal functioning of the Sun ONE Directory Server by logging in to an LDAP client as a normal user. The user should be placed in their correct home directory, have the correct user ID and group ID, and be able to change their password. They should also be able to resolve hostnames to IP addresses and the reverse.

```
Sun Microsystems Inc.   SunOS 5.8       Generic Patch   December 2002

[smcgee@client2 smcgee]$ id
uid=100(smcgee) gid=100(users)
[smcgee@client2 smcgee]$ pwd
/home/smcgee
[smcgee@client smcgee]$ getent hosts client1
192.168.1.101    client1.shomo.com
[smcgee@client2 smcgee]$ passwd
passwd: Changing password for smcgee
Enter existing login password:
New Password:
Re-enter new Password:
passwd: password successfully changed for smcgee
[smcgee@client2 smcgee]$
```

8.6 Verify Open Ports

Run an nmap[41] scan against the server to verify the open ports. The ports that should be open are 22, 389, 636, and 15,000 (if the Administrative Server is running):

```
[root@client root]# nmap -sT -O -p 1-65535 -v cypher

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host cypher (192.168.1.20) appears to be up ... good.
Initiating Connect() Scan against cypher (192.168.1.20)
Adding open port 22/tcp
Adding open port 389/tcp
Adding open port 15000/tcp
Adding open port 636/tcp
The Connect() Scan took 2090 seconds to scan 65535 ports.
For OSScan assuming that port 22 is open and port 1 is closed and neither are
firewalled
Interesting ports on cypher (192.168.1.20):
(The 65531 ports scanned but not shown below are in state: closed)
Port       State       Service
22/tcp     open        ssh
389/tcp    open        ldap
636/tcp    open        ldapssl
15000/tcp  open        unknown
```

[41] http://www.insecure.org/nmap/

```
Remote operating system guess: Sun Solaris 8 early acces beta through actual
release
Uptime 60.146 days (since Wed Jun 25 18:16:07 2003)
TCP Sequence Prediction: Class=truly random
                         Difficulty=9999999 (Good luck!)
IPID Sequence Generation: Incremental

Nmap run completed -- 1 IP address (1 host up) scanned in 2094 seconds
```

Where:

-sT is a full tcp connect scan
- O gives an OS fingerprint
- p 1-65535 is the range of ports to scan
- v is verbose output
cypher is the name of the machine to scan

Scanning all 65,535 ports is the only way to be sure to find all the open ones.

9 Appendix

9.1 Solaris 8 Server Jumpstart Profile

```
#  LDAP Server Install
#
#  Designed for Sun ONE DS 5.1 SP2 on a SF V120
#  - 36 Gig HD
#  - 1.5 Gb RAM
#  - 1151A Gig Ethernet PCI Card
#
#  SMcGee  08/14/2003
#  Based on Default profile from
#  RMallory - ASEG
#
#  This file is a standard Sun jumpstart script
#  called from match rules.ok, and dictates filesystem layout,
#  and packages added or deleted from the standard "Core" install.
#
#  05/03 Solaris 8 Release
#  163 packages total install – 285.52 Mbytes
#
#

install_type      initial_install
system_type       standalone
partitioning      explicit

filesys           rootdisk.s0 5120 /            logging
filesys           rootdisk.s1 1024 swap
filesys           rootdisk.s3 1536 /var         logging
filesys           rootdisk.s4 6144 /usr/iplanet logging
filesys           rootdisk.s5 2048 /var/audit   logging
filesys           rootdisk.s6 1024 /opt         logging
filesys           rootdisk.s7 free /export/local/audit logging


# Core Cluster
cluster SUNWCreq

# Misc Tools
package SUNWless        add   # The GNU pager (less)
package SUNWtoo         add   # Programming Tools
package SUNWtoox        add   # Programming Tools (64-bit)

# Freeware compression gzip,bzip
cluster SUNWCfwcmpx     add   #
cluster SUNWCfwcmp      add   #
package SUNWadmap       add   # System administration applications
package SUNWadmc        add   # System administration core libraries
package SUNWadmfw       add   # System & Network Administration Framework
package SUNWscpu        add   # Source Compatibility, (Usr)
package SUNWscpux       add   # Source Compatibility, (Usr) (64 bit)
```

```
# xpg4 Tools (egrep, etc)
package SUNWxcu4        add   # XCU4 Utilities
package SUNWxcu4x       add   # XCU4 Utilities (64-bit)

# Man pages
package SUNWman         add   # On-Line Manual Pages
package SUNWdoc         add   # Documentation Tools

# LDAP Required Packages
package SUNWlldap       add   # LDAP Libraries
package SUNWmfrun       add   # Motif RunTime Kit       *required

# Freeware shells
package SUNWtcsh        add   # Tenex C-shell (tcsh)
package SUNWbash        add   # GNU Bourne-Again shell (bash)
package SUNWzsh         add   # Z shell (zsh)

# Sun LibC
package SUNWlibC        add   # Sun Workshop Compilers Bundled libC
package SUNWlibCx       add   # Sun WorkShop Bundled 64-bit libC
package SUNWlibCf       add   # SunSoft WorkShop Bundled libC (cfront version)
package SUNWscbcp       add   # SPARCompilers Binary Compatibility Libraries

# Terminfo database
package SUNWter         add   # Terminal Information

# System Accounting
package SUNWaccr        add   # System Accounting, (Root)
package SUNWaccu        add   # System Accounting, (Usr)

# NTP
package SUNWntpu        add   # NTP, (Usr)
package SUNWntpr        add   # NTP, (Root)

# Snoop tool
package SUNWfns         add   # Federated Naming System
package SUNWfnsx        add   # Federated Naming System (64-bit)

# Automated Security Enhancement Tool
package SUNWast         add   # Automated Security Enhancement Tools

# Font packages for Directory Console
package SUNWi1of        add   # ISO-8859-1 (Latin-1) Optional Fonts
package SUNWi2rf        add   # X11 ISO-8859-2 required fonts
package SUNWi4rf        add   # X11 ISO-8859-4 required fonts
package SUNWi5rf        add   # X11 ISO-8859-5 required fonts
package SUNWi7rf        add   # X11 ISO-8859-7 required fonts
package SUNWi8rf        add   # X11 iso8859-8 required fonts
package SUNWi9rf        add   # X11 ISO-8859-9 required fonts
package SUNWi13rf       add   # X11 ISO-8859-13 required fonts
package SUNWi15rf       add   # X11 ISO-8859-15 required fonts
package SUNWfdl         add   # Font Downloader
package SUNWxwfnt       add   # X Window System platform required fonts
package SUNWxwcft       add   # X Window System common (not required) fonts
package SUNWxwoft       add   # X Window System optional fonts
package SUNW1251f       add   # Russian 1251 fonts
package SUNWeugrf       add   # X11 sun_eu_greek fonts

# ICE OpenWindows Libs for Directory Console
package SUNWxwice       add   # ICE components
package SUNWxwicx       add   # X Window System ICE library (64-bit)

# X Windows for Directory Console
package SUNWxi18n       add   # X Window System Internationalization Common Package
package SUNWxwplt       add   # X Window System platform software
package SUNWxwplx       add   # X Window System library software (64-bit)
package SUNWxwrtl       add   # X Window System & Graphics Runtime Library Links in
/usr/lib

# GigaSwift Ethernet Adapter Drivers
package SUNWcea         add
package SUNWceax        add
package SUNWcedu        add
```

9.2 Sample SSH Config

Recommended settings that are different than the default:

```
Port 22
Protocol 2
PermitRootLogin no
Subsystem       sftp    /path/to/sftp-server
```

9.3 /etc/pam.conf

```
#
#
# PAM configuration[42]
#
# Scott McGee
#
# /etc/pam.conf
# chown root:sys /etc/pam.conf
# chmod 644 /etc/pam.conf
#
# This pam.conf provides the account management features in the
# Directory Server including password expiration, account lockout etc.
# Currently, .rhosts authentication is broken.  This pam.conf provides
# .rhosts authentication but without account management features.  This
# means that a user with a locked or expired account could still log in
# using rsh/rlogin with .rhosts.  As of this document, it has been
# assigned bug id #4909247.
#
# Authentication management
#
#
login       auth requisite          pam_authtok_get.so.1
login       auth required           pam_dhkeys.so.1
login       auth required           pam_dial_auth.so.1
login       auth binding            pam_unix_auth.so.1 server_policy
login       auth required           pam_ldap.so.1
#
rlogin      auth sufficient         pam_rhosts_auth.so.1
rlogin      auth requisite          pam_authtok_get.so.1
rlogin      auth required           pam_dhkeys.so.1
rlogin      auth binding            pam_unix_auth.so.1 server_policy
rlogin      auth required           pam_ldap.so.1
#
dtlogin     auth requisite          pam_authtok_get.so.1
dtlogin     auth required           pam_dhkeys.so.1
dtlogin     auth binding            pam_unix_auth.so.1 server_policy
dtlogin     auth required           pam_ldap.so.1
#
dtsession   auth requisite          pam_authtok_get.so.1
dtsession   auth required           pam_dhkeys.so.1
dtsession   auth binding            pam_unix_auth.so.1 server_policy
dtsession   auth required           pam_ldap.so.1
#
rsh         auth sufficient         pam_rhosts_auth.so.1
rsh         auth binding            pam_unix_auth.so.1 server_policy
rsh         auth required           pam_ldap.so.1
#
other       auth required           pam_authtok_get.so.1
other       auth required           pam_dhkeys.so.1
other       auth binding            pam_unix_auth.so.1 server_policy
other       auth required           pam_ldap.so.1
```

[42] Based on pam.conf in “Solaris 8 Enhanced LDAP Naming Services Feature Patch Documentation”

```
#
passwd      auth binding            pam_passwd_auth.so.1 server_policy
passwd      auth required           pam_ldap.so.1
#
# Account management
#
login       account requisite       pam_roles.so.1
login       account required        pam_projects.so.1
login       account binding         pam_unix_account.so.1 server_policy
login       account required        pam_ldap.so.1
#
dtlogin     account requisite       pam_roles.so.1
dtlogin     account required        pam_projects.so.1
dtlogin     account binding         pam_unix_account.so.1 server_policy
dtlogin     account required        pam_ldap.so.1
#
cron        account required        pam_projects.so.1
cron        account binding         pam_unix_account.so.1 server_policy
cron        account required        pam_ldap.so.1
#
rlogin      account requisite       pam_roles.so.1
rlogin      account required        pam_projects.so.1
rlogin      account sufficient      pam_unix_account.so.1
rlogin      account required        pam_ldap.so.1
#
other       account requisite       pam_roles.so.1
other       account required        pam_projects.so.1
other       account sufficient      pam_unix_account.so.1
other       account required        pam_ldap.so.1 try_first_pass
#
# Session management
#
other       session required        pam_unix_session.so.1
#
# Password management
#
other       password required       pam_dhkeys.so.1
other       password requisite      pam_authtok_get.so.1
other       password requisite      pam_authtok_check.so.1
other       password required       pam_authtok_store.so.1 server_policy
#
# Support for Solaris PPP (sppp)
ppp         auth requisite          pam_authtok_get.so.1
ppp         auth required           pam_dhkeys.so.1
ppp         auth required           pam_dial_auth.so.1
ppp         auth binding            pam_unix_auth.so.1 server_policy
ppp         auth required           pam_dial_auth.so.1
ppp         auth required           pam_ldap.so.1
#
ppp         account requisite       pam_roles.so.1
ppp         account required        pam_projects.so.1
ppp         account required        pam_unix_account.so.1
#
ppp         session required        pam_unix_session.so.1
#
```

9.4 Schema for Basic Solaris LDAP Maps

Hosts:

```
cn=cypher + iphostnumber=192.168.1.20,ou=Hosts,dc=shomo,dc=com
objectClass : ipHost
objectClass : device
objectClass : top
cn : cypher
ipHostNumber : 192.168.1.20
```

Users:

```
uid=smcgee,ou=people,dc=shomo,dc=com
objectClass : posixAccount
objectClass : shadowAccount
objectClass : account
objectClass : top
uid : smcgee
cn : smcgee
uidNumber : 101
gidNumber : 100
gecos : Scott McGee
homeDirectory : /home/smcgee
loginShell : /bin/csh
userPassword : {crypt}eg235Fd
```

Groups:

```
cn=users,ou=group,dc=shomo,dc=com
objectClass : posixGroup
objectClass : top
cn : users
gidNumber : 100
memberUid : smcgee
memberUid : root
```

Automounts:

```
automountKey=smcgee,automountMapName=auto_home,dc=shomo,dc=com
objectClass: automount
objectClass: top
automountKey: smcgee
automountInformation: fileserver:/export/home/smcgee
```

Netgroups:

```
cn=users,ou=netgroup,dc=shomo,dc=com
objectClass nisNetgroup
objectClass top
```

```
        cn users
        nisNetgroupTriple (,smcgee,)
        nisNetgroupTriple (,test,)
```

Client Profiles:

```
        cn=ssl,ou=profile,dc=shomo,dc=com
        objectClass: DUAConfigProfile
        objectClass: top
        cn: ssl
        preferredServerList=192.168.1.20
        defaultServerList: 192.168.1.20,192.168.1.25
        defaultSearchBase: dc=shomo,dc=com
        authenticationMethod: tls:simple
        followReferrals: FALSE
        defaultSearchScope: one
        searchTimeLimit: 30
        profileTTL: 43200
        credentialLevel: proxy
        bindTimeLimit: 2
        serviceAuthenticationMethod: pam_ldap:tls:simple
        serviceAuthenticationMethod: keyserv:tls:simple
        serviceAuthenticationMethod: passwd-cmd:tls:simple
```

9.5 Example Sun ONE DS 5.1 Init script

```
#!/bin/sh
#
# Modified /usr/iplanet/servers/slapd-`hostname`/restart-slapd
# for iPlanet DS 5.1 init script
#
# Place in /etc/init.d/directory
# chown root:sys /etc/init.d/directory; chmod 755 /etc/init.d/directory
# ln –s /etc/init.d/directory /etc/rc3.d/S60directory
#
# Scott McGee
#

unset LD_LIBRARY_PATH

case $1 in
'stop')
        /usr/iplanet/servers/slapd-`hostname`/stop-slapd
        /usr/iplanet/servers/stop-admin
        ;;

'start')
        /usr/iplanet/servers/slapd-`hostname`/start-slapd
        /usr/iplanet/servers/start-admin
        ;;

'restart')
        /usr/iplanet/servers/slapd-`hostname`/restart-slapd
        /usr/iplanet/servers/restart-admin
        ;;
*)
        echo "Usage: $0 { start | stop | restart }"
        exit 1
        ;;
esac
```

9.6 /etc/nsswitch.conf

```
#
# /etc/nsswitch.conf
#
passwd:     files ldap
group:      files ldap

# consult /etc "files" only if ldap is down.
hosts:      ldap  files
ipnodes:    files

networks:   files
protocols:  files
rpc:        files
ethers:     files
netmasks:   files
bootparams: files
publickey:  files

netgroup:   ldap
automount:  files ldap
aliases:    files ldap

# for efficient getservbyname() avoid ldap
services:   files
sendmailvars:   files

# role-based access control
auth_attr: files ldap
exec_attr: files ldap
prof_attr: files ldap
user_attr: files ldap

# audit
audit_user: files ldap
project:    files ldap
```

9.7 LDAP Error Codes

Defined in section [43]4.1.10 of RFC 2251:[44]

```
Meaning                         Hex   Dec
------------------------------  ----  ---
LDAP CONNECTION SUCCESSFUL      0x00    0
LDAP OPERATIONS ERROR           0x01    1
LDAP PROTOCOL ERROR             0x02    2
LDAP TIMELIMIT EXCEEDED         0x03    3
LDAP SIZELIMIT EXCEEDED         0x04    4
LDAP COMPARE FALSE              0x05    5
LDAP COMPARE TRUE               0x06    6
LDAP STRONG AUTH NOT SUPPORTED  0x07    7
LDAP STRONG AUTH REQUIRED       0x08    8
LDAP PARTIAL RESULTS            0x09    9
LDAP REFERRAL RECEIVED          0x0a   10
LDAP ADMINLIMIT EXCEEDED        0x0b   11

LDAP NO SUCH ATTRIBUTE          0x10   16
LDAP UNDEFINED TYPE             0x11   17
LDAP INAPPROPRIATE MATCHING     0x12   18
LDAP CONSTRAINT VIOLATION       0x13   19
LDAP TYPE OR VALUE EXISTS       0x14   20
LDAP INVALID SYNTAX             0x15   21

LDAP NO SUCH OBJECT             0x20   32
LDAP ALIAS PROBLEM              0x21   33
LDAP INVALID DN SYNTAX          0x22   34
LDAP IS LEAF                    0x23   35
LDAP ALIAS DEREF PROBLEM        0x24   36

NAME ERROR(n)   ((n & 0xf0) == 0x20)   37

LDAP INAPPROPRIATE AUTH         0x30   48
LDAP INVALID CREDENTIALS        0x31   49
LDAP INSUFFICIENT ACCESS        0x32   50
LDAP BUSY                       0x33   51
LDAP UNAVAILABLE                0x34   52
LDAP UNWILLING TO PERFORM       0x35   53
LDAP LOOP DETECT                0x36   54

LDAP NAMING VIOLATION           0x40   64
LDAP OBJECT CLASS VIOLATION     0x41   65
LDAP NOT ALLOWED ON NONLEAF     0x42   66
LDAP NOT ALLOWED ON RDN         0x43   67
LDAP ALREADY EXISTS             0x44   68
LDAP NO OBJECT CLASS MODS       0x45   69
LDAP RESULTS TOO LARGE          0x46   70

LDAP OTHER                      0x50   80
LDAP SERVER DOWN                0x51   81
```

[43] http://jwm3.com/labs/ldaperror/
[44] http://www.faqs.org/rfc/rfc2251.txt

LDAP LOCAL ERROR	0x52	82
LDAP ENCODING ERROR	0x53	83
LDAP DECODING ERROR	0x54	84
LDAP TIMEOUT	0x55	85
LDAP AUTH UNKNOWN	0x56	86
LDAP FILTER ERROR	0x57	87
LDAP USER CANCELLED	0x58	88
LDAP PARAM ERROR	0x59	89
LDAP NO MEMORY	0x5a	90
LDAP CONNECT ERROR	0x5b	91

9.8 Sample Checklist for Configuring an LDAP Server

- € Install the Sun ONE Directory Server 5.1 Service Pack 2
  - Change directory to /opt/DS51
  - gunzip –c directory-5.1sp2-us.sparc-sun-solaris2.8.tar.gz | tar xvf –
  - Run "./setup" and install as appropriate to the local domain environment
    - Changing the domain will require re-import of all directory information from flat files. As such, it is not advised.
  - Run /opt/DS51/fix_iplanet.sh to correct schema, Console font errors and install a directory init script
- € Run /usr/lib/ldap/idsconfig to convert schema
  - Choose crypt password storage
  - Other Profile information doesn't matter as it will be overwritten
  - Run vlvindex script to index directory
- € Populate the Directory
  - Convert server to a client of itself
  - Collect NIS, files or NIS+ data
  - Use ldapaddent to populate the directory
  - Setup account security settings
- € Encryption
  - Set Certificate Database password in Console
  - Create certificate request with FQDN of server as CN
  - Sign certificate request with "openssl"
  - Install certificate and CA certificate with "certutil"
  - Create server "pin" file in /usr/iplanet/servers/alias with certificate database password
  - Chmod "pin" file read-only to root.
  - Turn on encryption in Console and restart server
- € Replication
  - Create Replication Manager user
  - Set passwordExpirationTime to 20380119031407Z
  - Turn on Multi-Master Replication
  - Setup Replication agreement on existing server and initialize one V120 as client
- € Verify contents of the server
  - /usr/bin/ldapsearch commands
- € Add the server IP addresses, FQDNs, and aliases to the /etc/inet/hosts file on each client.

9.9 Example ldapadd Wrapper Script

```
#!/bin/sh
#
# ldap_adduser
#
# Shell wrapper for ldapadd for adding a new
# user, setting the password and automount dir
#
# This is a rough example without a lot of error
# checking.  To be used as an example.
#
# Scott McGee
# 4/28/03
#
#


# Set the location variables:

SERVER=""         # Insert LDAP Servername
DOMAIN=""         # Insert base DN, like dc=shomo,dc=com
HOMESERVER=""     # Insert NFS server

# Usage statement if no username entered on the command line

while [ $# -lt 1 ]
do
        echo "\nUsage: "
        echo "   ldap_adduser <username>\n"
        exit 0
done

USER=$1

# Read in the info:

echo "Please enter the Home Directory (ex: /home/smcgee): \c"
      read homedir
echo "Please enter the User id number: \c"
      read uidnumber
echo "Please enter the Group id number: \c"
      read gidnumber
echo "Please enter a comment: \c"
      read comment
echo "Please enter a default shell: \c"
      read shell

echo "\nThis is what will be added to the LDAP database: \n
dn: uid=$USER,ou=people,$DOMAIN
objectClass: posixAccount
objectClass: shadowAccount
objectClass: account
objectClass: top
uid: $USER
```

```
cn: $USER
uidNumber: $uidnumber
gidNumber: $gidnumber
gecos: $comment
homeDirectory: $homedir
loginShell: $shell"

echo "\nIf this is correct, enter 'y' for yes: \c"
      read correct
if [ $correct = "y" ]; then
      # Create the ldif statement and send it to ldapadd
      echo \
      "dn: uid=$USER,ou=people,$DOMAIN
objectClass: posixAccount
objectClass: shadowAccount
objectClass: account
objectClass: top
uid: $USER
cn: $USER
uidNumber: $uidnumber
gidNumber: $gidnumber
gecos: $comment
homeDirectory: $homedir
loginShell: $shell" | \
      /bin/ldapadd -h $SERVER -D "cn=Directory Manager"

else
      echo "Bailing out.  Try again.\n"
      exit 1
fi


echo "\nDo you want to add an auto_home entry for $USER?\n"
echo "Directory will be set to $HOMESERVER:/export/home/$USER\n"
echo "Enter 'y' for yes, anything else for no: \c"
      read yesno2
if [ $yesno2 = "y" ]; then
      echo \
      "dn: automountKey=$USER,automountMapName=auto_home,$DOMAIN
objectClass: automount
objectClass: top
automountKey: $USER
automountInformation: $HOMESERVER:/export/home/$USER" | \
      /bin/ldapadd -h $SERVER -D "cn=Directory Manager"

# Print out commands to create the user’s home directory
            echo ""
            echo "Run this to create the Home Directory on $HOMESERVER"
            echo "mkdir /export/home/$USER"
            echo "cp /etc/skel/local.cshrc /export/home/$USER/.cshrc"
            echo "cp /etc/skel/local.login /export/home/$USER/.login"
            echo "cp /etc/skel/local.profile /export/home/$USER/.profile"
            echo "chown -R $uidnumber /export/home/$USER"
            echo ""

else
      echo "Not adding auto_home directory."
```

```
fi


echo "Do you want to set a password for $USER? "
echo "Enter 'y' for yes, anything else for no: \c"
      read yesno

if [ $yesno = "y" ]; then
      # Turn off echo while we ask for the new password:
      trap 'stty echo; exit' 0 1 2 3 15
      echo "Please enter $USER's new password: \c"
            stty -echo
            read password
      echo "\nPlease confirm $USER's new password: \c"
            read password2
            stty echo
      echo ""
      if [ $password = $password2 ]; then
            echo "Enter the Directory Manager's password:"
            # Create the ldif statement and send it to ldapmodify
            echo "dn: uid=$USER,ou=people,$DOMAIN
changetype: modify
replace: userPassword
userPassword: $password" | \
            /bin/ldapmodify -h $SERVER -D "cn=Directory Manager"
      else
            echo "New passwords don't match.\n"
            exit 0
      fi


else
      echo "Skipping setting the default password."
fi

echo "Done.\n"

exit 0
```

10 Recommended Reading

10.1 Books

Sun Microsystems' iPlanet Directory Server 5.1 Guides
http://docs.sun.com/db/prod/4470#hic

"Solaris and LDAP Naming Services, Deploying LDAP in the Enterprise"
http://www.sun.com/solutions/blueprints/books/LDAP.html

"LDAP System Administration"
http://www.oreilly.com/catalog/ldapsa/

"The SANS Institute - Solaris Security Step by Step"
https://store.sans.org/store_item.php?item=21

10.2 Tools

Sun ONE Directory Server 5.1 Service Pack 2
http://wwws.sun.com/software/download/inter_ecom.html
http://wwws.sun.com/software/download/products/3e5beea5.html

Sun ONE Directory Server Resource Kit 5.1
http://wwws.sun.com/software/download/products/3ed69993.html

Certutil (from Netscape/Mozilla)
http://www.mozilla.org/projects/security/pki/nss/tools/ - Tools
http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html
ftp://ftp.mozilla.org/pub/security/nss/releases/NSS_3_4_1_RTM/SunOS5.8_OPT.OBJ/nss-3.4.1.tar.gz

OpenSSL
http://www.openssl.org/
ftp://ftp.sunfreeware.com/pub/freeware/sparc/8/

OpenSSH
http://www.openssh.org/

Sun Solaris Patches:
http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

YASSP:
http://www.yassp.org/

11 References

Bilaski, Tom and Haines, Michael. "Sun Blueprints Solaris and LDAP Naming Services, Deploying LDAP in the Enterprise". Palo Alto: Sun Microsystems Press - A Prentice Hall Title, 2001. ISBN 0-13-030678-9 http://www.sun.com/solutions/blueprints/books/LDAP.html

Brewis, Mark and Hardisty, Jim. "Directory Traversal in Sun iPlanet Administration Server 5.1", Bugtraq, August 8, 2003. http://www.securityfocus.com/archive/1/332399

Brown, Philip. "Secure LDAP for Solaris (via TLS/SSL)". http://www.bolthole.com/solaris/LDAP.html

Carter, Gerald. "LDAP System Administration – Putting Directories to Work". California: O'Reilly & Associates, Inc, 2003.

"CERT Advisory CA-2001-18 Multiple Vulnerabilities in Several Implementations of the Lightweight Directory Access Protocol (LDAP)". Carnegie Mellon University, December 10, 2001. http://www.cert.org/advisories/CA-2001-18.html

Faust, Sacha. "LDAP Injection, Are Your Web Applications Vulnerable?". SPI Dynamics, Inc, 2003. http://www.spidynamics.com/mktg/LDAP1/index.html

Glosser, David. "Solaris Security: An introduction to Packages, Clusters, Software Groups". 2002. http://www.mgmg-interactive.com/mgmg/packages1.html, http://www.mgmg-interactive.com/mgmg/packages2.html, http://www.mgmg-interactive.com/mgmg/packages3.html

Howard, Luke. "Pam_ldap Module". http://www.padl.com/OSS/pam_ldap.html

igor@ypass.net. "Solaris Schema". http://sapiens.wustl.edu/~sysmain/info/openldap/schemas/solaris.schema

"iPlanet Directory Server 5.1 Guides". Sun Microsystems. http://docs.sun.com/db/coll/S1_ipDirectoryServer_51

"iPlanet Directory Server 5.1 Administrator's Guide". California: Sun Microsystems, Inc. http://docs.sun.com/db/doc/816-5606-10

"iPlanet Directory Server 5.1 Installation Guide". California: Sun Microsystems, Inc. http://docs.sun.com/db/doc/816-5610-10

"iPlanet Directory Server 5.1 Deployment Guide". California: Sun Microsystems, Inc. http://docs.sun.com/db/doc/816-5609-10

References Continued

Lanza, Jefferey. “Vulnerability Note VU#276944 - iPlanet Directory Server contains multiple vulnerabilities in LDAP handling code”. Carnegie Mellon University, December 12, 2001. http://www.kb.cert.org/vuls/id/276944

Mallory, Rob. Jumpstart configuration. Advanced Systems Engineering Group, San Diego, 2003. ASEG.com.

McGreer, Ian. “Using the Certificate Database Tool”. The Mozilla Organization, December 2002. http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html

Pomeranz, Hal. “Solaris Security Step by Step”. The SANS Institute, 2001. Pages 1-21.

Shand, Adam. “Solaris8LDAP”. April 2003. http://www.spack.org/index.cgi/Solaris8Ldap

Solaris 8 OE Patch 108993-23.README. Sun Microsystems, Inc., August, 2003. http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage

“Solaris 8 Enhanced LDAP Naming Services Feature Patch Documentation”. California: Sun Microsystems, Inc., March 6, 2003. Page 71-90.

“Sun ONE Directory Server 5.2 Release Notes”. California: Sun Microsystems, Inc. http://docs.sun.com/source/816-6703-10/index.html

“Sun ONE / iPlanet / Netscape Directory Server LDAP Error Codes”. JWM3, Inc. May 29, 2003. http://jwm3.com/labs/ldaperror/

Various. “PAM LDAP Mailing List Archives”. http://www.netsys.com/pamldap/

Various. “PROTOS Test-Suite: c06-ldapv3”. University of Oulu, December 2001, http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/ldapv3/.

12 Index