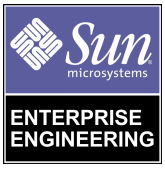
Automating LDAP Client Installations

By Tom Bialaski - Enterprise Engineering

Sun BluePrints™ OnLine - July 2001



http://www.sun.com/blueprints

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 816-1456-10
Revision 01, 05/22/01
Edition: July 2001

Automating LDAP Client Installations

Prior to the release of the Solaris™ 8 Operating Environment (Solaris OE), systems could not be configured with LDAP as a name service at installation time. Now that `sysidtool` has been enhanced to accept LDAP as a name service option, LDAP clients can be configured either through an interactive or hands-off installation. While the procedure for configuring an LDAP client is similar to the NIS and NIS+ procedure, there are some differences you need to be aware of.

This article examines the mechanism that is used to configure a Solaris OE name service client in general, and highlights the differences for configuring a client to use the LDAP name service. This articles also presents an overview of `sysidtool` to familiarize the reader with the mechanics of system configuration. In addition, a description of the information required to configure an LDAP client is provided along with an example showing how that information is entered. Finally, the steps required to set up a JumpStart™ server capable of servicing a hands-off installation of LDAP clients are provided along with example configuration files.

How a Solaris OE Client is Configured

A Solaris OE client is configured by a suite of five programs collectively known as `sysidtool(1M)`. The five programs are:

- `/usr/sbin/sysidnet`
- `/usr/sbin/sysidns`
- `/usr/sbin/sysidsys`
- `/usr/sbin/sysidroot`
- `/usr/sbin/sysidpm`

These programs are executed when the following two events occur:

- Solaris OE is installed.
- After the first reboot following the execution of the `sys-unconfig`(1M) command.

TABLE 1 shows what information is obtained from each of the five utilities.

TABLE 1 `sysidtool` Information

Command	Information Obtained
`sysidnet`	host name, IP address, console type, locale
`sysidns`	name service, IP subnet mask, domain name, host name and IP address of name server(s), LDAP client profile
`sysidsys`	time zone, data, time
`sysidroot`	root password
`sysidpm`	power management
`sysidconfig`	controls use of `sysidcfg`(4)

This information can be obtained from either of the following sources:

- The system console (interactively)
- A name service
- A `sysidcfg` file

The first two sources are used to obtain the information during system installation or following a reboot after the `sys-unconfig` command is run. The third source is used for automatic hands-off installation. During installation, `sysidtool` attempts to find an NIS+ server on the local subnet where the system installation is taking place. If no NIS+ server is found, then a search is performed for a NIS server. If either a NIS+ or NIS server is located, configuration data is extracted from its NIS maps or NIS+ tables. If neither is found, `sysidtool` prompts the user for the required information.

During a hands-off installation, `sysidtool` searches for a file called `sysidcfg` whose location is specified in `/etc/bootparams`. Information contained in the `sysidcfg` file can be used instead of obtaining the data from a name service. An example of a `sysidcfg` file is provided later in this article.

Information Required to Configure an LDAP Client

A Solaris OE LDAP client requires much of the same configuration information that a NIS+ or NIS client does. This common information includes:

- Host name
- IP address
- Netmask
- Root password
- Locale
- Time Zone

Beside this information, an LDAP client requires three additional pieces of information. These are:

- The name of the domain it belongs to (equivalent to a NIS+ or NIS domain name).
- The IP address of an LDAP server that serves that domain and contains LDAP client profiles set up for the client.
- The name of the LDAP client profile to download.

The domain name is similar to the NIS domain name except that it is present in an entry on an LDAP directory server instead of a NIS server configuration file. Unlike the NIS domain name, the LDAP domain name is not case sensitive. LDAP client profiles are entries that are created on an LDAP server configured to support Solaris OE native LDAP clients. The LDAP profile server does not have to be the same LDAP server (or servers), that the LDAP client will ultimately access for name service data, but it is a common practice to use the same server.

Refer to the Sun BluePrints™ book, *Solaris and LDAP Naming Services* (ISBN #0-13-030678-9 which is available through www.sun.com/books, amazon.com, fatbrain.com, and Barnes and Noble bookstores) for directions on how to set up an LDAP server to support native LDAP clients. Additionally, a previous Sun BluePrints OnLine article, *Running Multiple Naming Services on a Solaris™ Client* (published May 2001), explains how a Solaris OE native LDAP client works.

Note – Installation of an LDAP client through `sysidtool` requires that an `ipHost` entry containing the host name and IP address of the client be created on the LDAP server specified in the LDAP client profile. The name service configuration will fail if a host entry matching the client's host name cannot be found on the LDAP server.

The following two examples show the dialogue that takes place when LDAP is specified as the name service during an interactive installation. For brevity, only the portion that pertains to name service configuration is shown.

EXAMPLE 1 Interactive Installation of a Solaris OE Native LDAP Client Dialogue

```
Available name services:

1. NIS+
2. NIS
3. DNS
4. LDAP
5. None

Please enter the number corresponding to the type of name service
you would like [2]: 4

Please specify the domain where this system resides. Make sure you
enter the name correctly including capitalization and punctuation.

Enter this system's domain name [Boston.East.Sun.COM]:bpsrus.com

Please enter the name of the LDAP profile being used to configure
this system as an LDAP client. You must also enter the IP address
of the server that contains the profile.

Enter the name of the profile [default]: myprofile
Enter the address of the profile server []: 128.0.0.7
```

Note – The default domain name that is displayed is obtained from a NIS or NIS+ server. This domain name is only displayed if one is found on the subnet that the client is attached to. A search for LDAP servers on the subnet is not performed, so a domain name cannot be determined by examining one.

EXAMPLE 2 Interactive Installation of a Solaris OE Native LDAP Client Output

```
You have entered the following values:

Host Name:                ldapclient
IP Address:               128.0.0.10
System part of a subnet:  Yes
Netmask:                  255.255.255.0
Enable IPv6:              No
Name Service:             LDAP
Domain Name:              bpsrus.com
Profile Name:             myprofile
Profile Server Address:   128.0.0.7
Time Zone:                Eastern
Power Management: Turn Power Management Off
Do not ask about Power Management at reboot.
```

Post Installation Issues

1. After the client reboots, you will notice a console message similar to the following:

```
NIS domainname is bpsrus.com
```

This message is misleading, because it implies you are running NIS. The domain name refers to the `nisdomain` attribute set on the LDAP server that the client is binding to. Unlike a NIS client, there is no `ypbind` process running on a native LDAP client.

2. For user authentication, `pam_unix` is the only authentication method specified in the `/etc/pam.conf` file. If you want to authenticate users using `pam_ldap`, additional lines need to be added to the `pam.conf` file. The previous Sun BluePrints OnLine article, *Running Multiple Naming Services on a Solaris™ Client* (published May 2001), describes how to do this.

3. Unless your LDAP server is populated with `rpc` map data, you will get errors when the system boots. To eliminate these errors, edit the following line in the `/etc/nsswitch.conf` file.

```
#rpc:        ldap [NOTFOUND=return] files
rpc:        files ldap
```

The next section walks you through a complete hands-off installation.

Hands-off Installation of an LDAP Client

This section describes how to use a JumpStart server to automatically install native LDAP clients. This procedure assumes you already have an LDAP server configured to support native LDAP clients. Before attempting an automatic installation, you should make sure an interactive client installation works with the LDAP server you have configured.

Pre-configuring LDAP as the Name Service

Unlike the NIS and NIS+ name services, `sysidtool` cannot use LDAP as a name service to obtain configuration information. Instead, the only option for a hands-off installation is the creation of a `sysidcfg` file for the client that is read by the JumpStart installation utilities.

The following syntax is used to specify LDAP as a name service in a `sysidcfg` file:

```
name_service=LDAP
{domain_name=domain_name
profile=profile_name
profile_server=ip_address}
```

An example of this section looks like the following:

```
name_service=LDAP
{domain_name=bpsrus.com
profile=myprofile
profile_server=128.0.0.7}
```

Note – The variable `profile_server` refers to the LDAP directory server that contains the LDAP profile specified with the `profile` variable. Do not confuse this terminology with the JumpStart profiles or profile servers.

The following is a sample of a complete `sysidcfg` file for a group of LDAP clients.

```
system_locale=en_US
timezone=US/Eastern
terminal=sun-cmd
timeserver=localhost
name_service=LDAP
{domain_name=bpsrus.com
profile=myprofile
profile_server=128.0.0.7}
root_password=m4QPOWNY
```

▼ JumpStart Server Procedure

This procedure assumes you have already set up a JumpStart boot, install, and profile server. Refer to the Sun BluePrints article, *Building a JumpStart™ Infrastructure* (published April 2001), if you are unfamiliar with the mechanics for setting up a JumpStart environment.

1. Install the Solaris 8 OE Update 3 (1/01) image on the JumpStart install server.
2. Add the client's host name, IP address, and Ethernet address to the `/etc/hosts` and `/etc/ethers` files on the JumpStart boot server, or to the name service the boot server is using.

Note – The JumpStart boot server that supports LDAP clients can use LDAP as a name service. However, a `sysidcfg` file must still be created because the LDAP client cannot access an LDAP server until it is fully installed.

---

3. Create a `sysidcfg` file specifying LDAP as the name service. A `sysidcfg` file can be shared among several clients. However, if you want to specify different root password or LDAP profile, you need to create separate `sysidcfg` files.

Note – Only one `sysidcfg` file can appear in a directory. If you want to set different configuration parameters for different clients, a separate directory needs to be created for each client or group of clients.

---

4. Run the `add_install_client` command specifying the `-c` and the `-p` options For example:

```
# ./add_install_client -c jumpserv:/jumpstart -p jumpserv:/
jumpstart/ldapclient1/sysidcfg ldapclient1 sun4u
```

5. On the client, run the boot command from the prom monitor prompt.

```
ok> boot net - install
```

To make additional modification, such as specifying `pam_ldap` authentication and changing the default database search path in the `nsswitch.conf` file, you need to add a JumpStart server finish script. For example, the following script replaces the system default `pam.conf` and `nsswitch.conf` files with pre-configured ones.

```
cp /a/etc/pam.conf /a/etc/pam.conf.orig
cp ${SI_CONFIG_DIR}/ldapfiles/pam.conf /a/etc/pam.conf
cp /a/etc/nsswitch.conf /a/etc/nsswitch.conf.orig
cp ${SI_CONFIG_DIR}/ldapfiles/nsswitch.conf /a/etc/nsswitch.conf
```

This example assumes you have a directory named `ldapfiles` on the JumpStart server and have pre-configured the `pam.conf` and `nsswitch.conf` files.

JumpStart Server Considerations

To support LDAP client installations, the Solaris OE version running on the JumpStart server is not important. The server can be running NIS, NIS+, LDAP, or no name service. When choosing whether or not to store JumpStart server related information in a name service, the main consideration is whether the data will be shared among multiple JumpStart servers. In this case, all servers would be running the same name service and belong to the same domain.

Conclusion

Prior to Solaris 8 OE, Update 3, the only way you could configure a native LDAP client was to install the client specifying another name service, or no name service, then convert it to an LDAP client after it was installed. Now you have a choice of configuring the client at installation time, either interactively or hands off, using JumpStart technology. However, as described in this article, there are limitations.

Three key points to remember when configuring native LDAP clients are:

- You must use the LDAP profile method to initialize clients.
- Naming service information must be supplied to the client either interactively or through a `sysidcfg` file if using JumpStart software.
- The hostname of the client must appear in the LDAP directory.

For a more in depth discussion on the mechanics of JumpStart software, watch for the Sun BluePrints book, *JumpStart™ Technology: Effective Use in the Solaris™ Operating Environment*, (ISBN #0-13-062154-4 which will be available through www.sun.com/books,amazon.com, fatbrain.com, and Barnes and Noble bookstores) coming out this summer.

Acknowledgements

I would like to thank Michael Haines of Sun Professional Services for lending his LDAP expertise to help create this article and verify its accuracy.

Author's Bio: Tom Bialaski

Tom Bialaski is currently a Senior Staff Engineer with the Enterprise Engineering group at Sun Microsystems, and is the author of "Solaris Guide for Windows NT Administrators," and co-author of "Solaris and LDAP: Naming Services." Tom has 20 years of experience with the UNIX® operating system and has been a Sun Engineer since 1984.