Installing and Administering NIS/LDAP Gateway

Edition 1

HP 9000 Networking

Manufacturing Part Number: J4269-90001

E0999

Legal Notice

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Contents

Contents

Contents

Contents

Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made.

Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service. See your HP sales representative for details.

First Edition: September 1999 (HP-UX Release 10.20)

Table 1 Product Numbers

Description	Number
LDAP-UX Integration (NIS/LDAP Gateway server B.01.00 and LDAP-UX Client Administration Tools B.01.00)	J4269AA

Related Documentation

For additional information, see the following:

- *NIS/LDAP Gateway Release Notes* (J4269-90002) available at http://docs.hp.com/hpux/internet.
- NIS/LDAP Gateway README file available after you install the product at /opt/ldapux/README-ypldapd.
- Client Administration Tools README file available after you install the product at /opt/ldapux/README-client.
- *Installing and Administering NFS Services* discusses NIS available at http://docs.hp.com/hpux/communications.
- *Netscape Directory Server Administrator's Guide* and other titles available at http://docs.hp.com/hpux/internet.
- Manual pages using the *man*(1) command *ypldapd*(8), *ypserv*(1M), *ypfiles*(4) and other related NIS man pages.

1 Overview of NIS/LDAP Gateway

This chapter provides a high level overview of what the NIS/LDAP Gateway product is and how it works.

The NIS/LDAP Gateway is a Network Information Service (NIS) server that uses an LDAP directory as its information source instead of NIS map files. The Gateway accepts NIS client requests for information, gets the information from an LDAP directory, and returns the information to the NIS clients. It effectively replaces your NIS servers and map files with an NIS/LDAP Gateway server and an LDAP directory. Existing NIS clients transparently use an LDAP directory to resolve user, group, host and other information.

Used in conjunction with LDAP server technologies, such as Netscape's Directory Server, the NIS/LDAP Gateway can consolidate credentials and allow a single password per user to be shared among multiple platforms and applications.

The hierarchical and distributed nature of LDAP is substantially more scalable than the flat, single domain policy of NIS. The NIS/LDAP Gateway allows your organization to leverage the scalability and distributed nature of LDAP directory services, while maintaining an existing NIS infrastructure.

NOTE

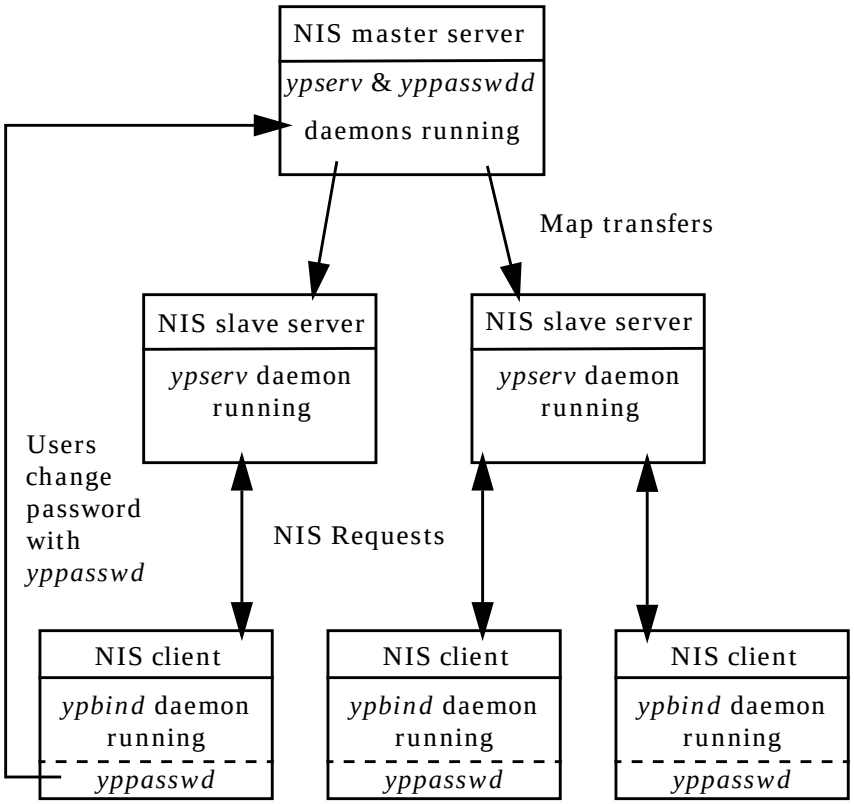
The NIS/LDAP Gateway does not include an LDAP directory server. You can obtain the single-server Netscape Directory Server 4.x for HP-UX - Lite Edition from http://www.software.hp.com, or the fully functioning directory server from your local HP sales office. Other directories that support LDAP can also be used with this product.

Comparing NIS and NIS/LDAP Gateway

This section describes the NIS/LDAP Gateway environment, compares it to NIS, and gives an overview of the steps for migrating to the NIS/LDAP Gateway.

The following diagram shows a typical NIS environment:

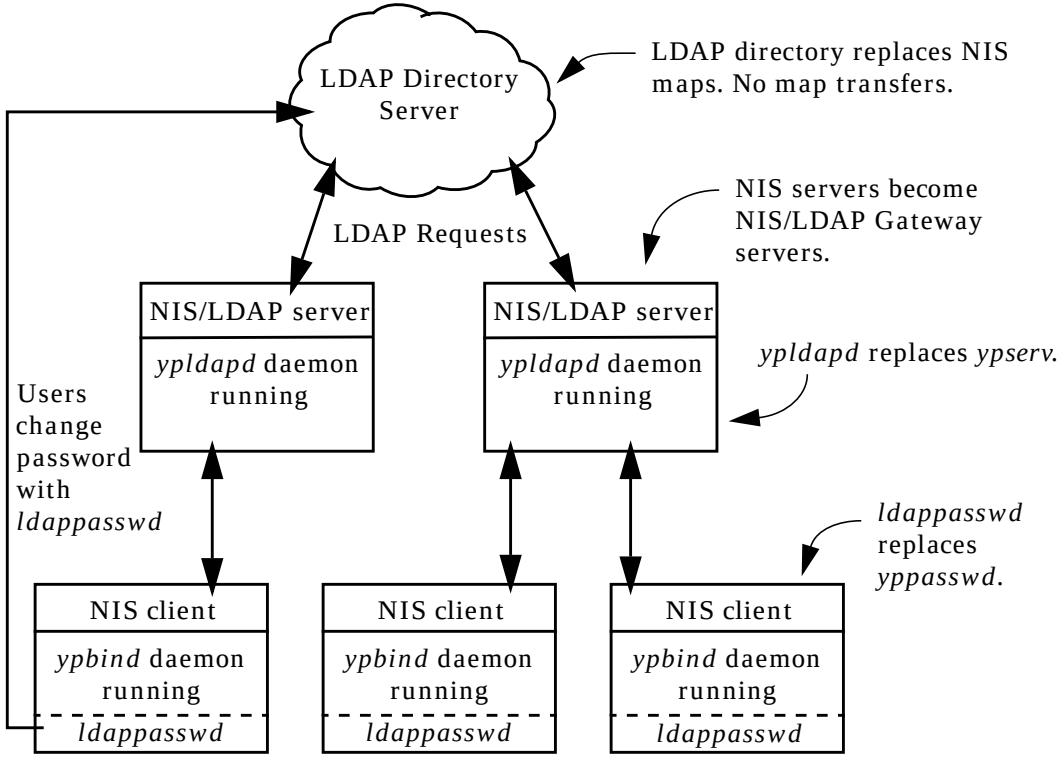
Figure 1-1 Typical NIS Environment



In this NIS environment, the master map files reside on the NIS master server. Copies of these map files are periodically transferred to the NIS slave systems. The NIS servers run the ypserv daemon which serves the information requested by clients. NIS clients run the ypbind daemon which establishes a connection to an NIS server, enabling client processes to get information from the NIS server. Users can change their passwords using the yppasswd command.

The following diagram shows what this environment might look like when converted to an NIS/LDAP Gateway environment:

Figure 1-2 NIS/LDAP Gateway Environment



In the NIS/LDAP Gateway environment, four main differences exist:

1. An LDAP directory replaces your NIS master server and NIS maps. Map files and map transfers are no longer needed. LDAP replication uses more efficient updates instead of complete map builds and transfers.
2. All NIS slave servers become NIS/LDAP Gateway servers. The NIS/LDAP Gateway servers run the ypldapd daemon, rather than the ypserv daemon. ypldapd requests information from the LDAP directory and serves the information back to the NIS clients.

3. NIS clients continue to run the ypbind daemon, which establishes a connection to an NIS/LDAP Gateway server, enabling client processes to get information from the LDAP directory.
4. Users change their passwords using the ldappasswd command or an LDAP administration tool such as a web browser rather than the yppasswd command. Users must use an LDAP administration tool such as a web browser to change their personal information instead of *chfn*(1) and *chsh*(1).

Summary of Installing and Configuring

The following summarizes the steps to take when moving to an NIS/LDAP Gateway environment.

- Install and configure an LDAP directory.
- Install and configure the NIS/LDAP Gateway.
- Migrate your NIS map information to your directory.
- Install ldappasswd on your NIS client systems, if desired.
- Stop the NIS server daemon, ypserv, if necessary
- Start the NIS/LDAP Gateway daemon, ypldapd.

These steps, plus verification and testing steps, are described in detail in Chapter 2 , “Installing the NIS/LDAP Gateway,” on page 17.

The NIS/LDAP Gateway Components

The NIS/LDAP Gateway product, comprising the following components, can be found under /opt/ldapux/ypldapd, except where noted.

Table 1-1 NIS/LDAP Gateway Components

Component	Description
ypldapd	The daemon that replaces the ypserv daemon and serves NIS requests from NIS clients.
ypldapd.conf	The NIS/LDAP Gateway configuration file.
namingcontexts.conf	Configuration file that specifies where in the LDAP directory each NIS map is.
init.d	Contains start-up files.
lib	Contains libraries used by ypldapd.
slapd-v2.nis.conf, slapd-v3.nis.conf	The directory schema for posix account and other information (RFC 2307) required by the NIS/LDAP Gateway. LDAP version 2 and version 3.
ypldapd.8	The *ypldapd*(8) man page.

The installation process copies the automatic start-up file to /etc/rc.config.d/ypldapd and the manual start-up file to /sbin/init.d/ypldapd.

Client Administration Tools

The Client Administration Tools listed below can be found under /opt/ldapux.

Table 1-2 Client Administration Tools

Component	Description
ldapdelete	Allows you to delete entries in the directory.
ldapmodify	Allows you to add, delete, modify, or rename directory entries. All operations are specified using LDIF update statements.
ldappasswd	Changes passwords in the directory. Replaces yppasswd.
ldapsearch	Allows you to search the directory. Returns results in LDIF format.
migrate_all_online.sh	Migrates files to LDIF or to an LDAP directory. Uses perl scripts listed below.
migrate_all_nis_online.sh	Migrates NIS maps to LDIF or to an LDAP directory. Uses perl scripts listed below.
migrate_aliases.pl	Migrates /etc/aliases to LDIF.
migrate_base.pl	Creates base DN information.
migrate_common.ph	Routines used by other migration scripts.
migrate_fstab.pl	Migrates /etc/fstab to LDIF.
migrate_group.pl	Migrates /etc/groups to LDIF.
migrate_hosts.pl	Migrates /etc/hosts to LDIF.
migrate_netgroup.pl	Migrates /etc/netgroup to LDIF.
migrate_netgroup_byhost.pl	Migrates netgroup.byhost NIS map to LDIF.
migrate_netgroup_byuser.pl	Migrates netgroup.buyser NIS map to LDIF.

Table 1-2 Client Administration Tools

Component	Description
migrate_networks.pl	Migrates /etc/networks to LDIF.
migrate_passwd.pl	Migrates /etc/passwd to LDIF.
migrate_protocols.pl	Migrates /etc/protocols to LDIF.
migrate_rpc.pl	Migrates /etc/rpc to LDIF.
migrate_services.pl	Migrates /etc/services to LDIF.
perl, version 5	Used by all the migration scripts.
README-client, README-ypldapd	Additional documentation files.
Contributed tools	Unsupported tools in /opt/ldapux/contrib. See the file /opt/ldapux/contrib/bin/README for details.

2 Installing the NIS/LDAP Gateway

This chapter describes the decisions you need to make and the steps you need to take to install and configure the NIS/LDAP Gateway.

Before You Begin

This section lists some things to keep in mind as you plan your installation.

- You must have an LDAP directory. You can obtain the single-server Netscape Directory Server for HP-UX - Lite Edition, from http://www.software.hp.com, or the fully functioning directory server from your local HP sales office. You can view the documentation at http://docs.hp.com/hpux/internet. If you have another directory, consult the documentation for your directory.
- See the *NIS/LDAP Gateway Release Notes* (part number J4269-90002) for additional information.
- Most examples here use the Netscape Directory Server for HP-UX and assume you have some knowledge of this directory and its tools, such as the Directory Console and ldapsearch. If you have another directory, consult your directory's documentation for specific information.
- The following steps assume you want to emulate the NIS environment on HP-UX as closely as possible. You have a lot of flexibility to do things differently. Modify these steps as needed for your environment.
- The examples use a root DN of o=hp.com for illustrative purposes.

Plan Your Installation and Testing

Before beginning your installation, you should plan how you will set up and test your NIS/LDAP Gateway environment before putting it into

production. This will be similar to the process used to set up and test an NIS environment. Consider the following questions:

- How many LDAP directory servers and replicas will you need?

  Each NIS/LDAP Gateway server binds to an LDAP directory server containing your NIS data. Multiple NIS/LDAP Gateway servers can bind to a single directory server or replica server. The answer depends on your environment, the size and configuration of your directory and how many users you have. Depending on these factors, you may have anywhere from ten to over one hundred NIS/LDAP Gateway servers for each LDAP directory server.

- How many NIS/LDAP Gateway servers will you need?

  This also depends on your environment. A rule of thumb might be to have the same number of NIS/LDAP Gateway servers as you have NIS servers currently.

- Where will you get your NIS data from when migrating it to the directory?

  You can get it from the same source files you create your NIS maps from or you can get it from your NIS maps themselves. The key is to use up-to-date information. You will probably need to keep your NIS maps and your directory in sync for a time while testing. One of the contributed tools, ldifdiff, can help you keep your data in sync.

- Where in your directory will you put your NIS data?

  If you are starting with a brand new directory, you will create a new subtree. If you already have a directory, you can place your NIS data in a separate, new subtree of the directory. Or you can merge your NIS data into your existing directory.

- How will you put your NIS data into your directory?

  If you are starting with a brand new directory, the migration scripts can build a new directory subtree for your NIS data.

  If you have an existing directory and you decide to place your NIS data into a new, separate subtree, the migration scripts can build and populate this subtree.

  If you merge your NIS data into an existing directory, the migration scripts can create LDIF files of your NIS data, but you will have to write your own scripts or use other tools to merge the NIS data into your directory.

- How will you test your NIS/LDAP Gateway environment?

  You may want to set up a separate group of systems to test it on. Or you could install the NIS/LDAP Gateway on one of your existing NIS servers or some other system but use a new domain just for testing. Then change one or more existing NIS clients' domains to the new domain for testing. When you have things set up and working correctly, change the NIS/LDAP Gateway domain to your production domain. You can use *ypset*(1M) to force one or more clients to bind to the NIS/LDAP Gateway for testing. If you encounter problems, you can stop the NIS/LDAP Gateway and restart ypserv. You can migrate one NIS server at a time to the NIS/LDAP Gateway, testing each as you go.

NOTE You cannot run an NIS server (ypserv) and an NIS/LDAP Gateway server (ypldapd) simultaneously on the same system.

- How will you communicate with your user community about the change? How will your users change their personal information such as passwords, login shell, and *finger*(1) information?

  You can install ldappasswd on your NIS client systems to replace yppasswd. Or you can create or purchase web-based tools your users can use to update their passwords and other information in the directory. Note that at this release, the HP-UX commands *chsh*(1) and *chfn*(1) do not change information in the directory.

NOTE The *csh*(1) shell and *finger*(1) command request the entire contents of the passwd map for certain operations which may result in a performance bottleneck. For this reason, you may want to restrict use of *csh*(1) and *finger*(1). See "Minimizing Enumeration Requests" on page 31 for more information.

- How will you put your NIS/LDAP Gateway into production after testing?

  One possible way is to convert each NIS server to an NIS/LDAP Gateway server, one server at a time, one subnet at a time. When you are confident that server is working, convert the next NIS server to the NIS/LDAP Gateway. During the transition, you will probably

need to keep your NIS maps and your directory in sync.

Another possible way is to create a new domain and convert each client to the new domain.

Configure Your Directory

This section describes how your directory needs to be configured to work with the NIS/LDAP Gateway. Examples are given for Netscape Directory Server for HP-UX. If you have a different directory, see the documentation for your directory for details on how to configure it as described here.

Step 1. Install the posix schema (RFC 2307) into your directory.

If you have Netscape Directory Server 4.0 for HP-UX or later, the posix schema is already installed.

For other directories, you can install the schema from /opt/ldapux/ypldapd/etc/slapd-v3.nis.conf for version 3 LDAP directories and /opt/ldapux/ypldapd/etc/slapd-v2.nis.conf for version 2 LDAP directories. Depending on the directory you have, include a line like one of the following in your configuration file:

```
include /opt/ldapux/ypldapd/etc/slapd-v3.nis.conf
include /opt/ldapux/ypldapd/etc/slapd-v2.nis.conf
```

For information on the posix schema (RFC 2307), see http://www.ietf.org.

Step 2. Restrict write access to certain passwd attributes of the posix schema.

CAUTION Make sure you restrict access to the attributes listed below. Allowing users to change them could be a security risk

Grant write access of the uidnumber, gidnumber, homedirectory, and uid attributes only to the directory administrator; disallow write access by all other users. Set up access control lists (ACL) so ordinary users cannot change these attributes in their password entry in the directory. With Netscape Directory Server for HP-UX, you can use the Netscape Console

or ldapmodify.

The following access control instruction (ACI) is by default at the top of the directory tree for a 4.x Netscape directory. This ACI allows a user to change any attribute in their password entry:

```
aci: (targetattr = “*”) (version 3.0; acl “Allow self entry modification”;
 allow (write)userdn = “ldap:///self”;)
```

Modify this ACI to the following, which prevents ordinary users from changing their uidnumber, gidnumber, homedirectory, and uid attributes:

```
aci: (targetattr != “uidnumber || gidnumber || homedirectory || uid”) (version
 3.0; acl “Allow self entry modification, except for important posix attributes”;
 allow (write)userdn = “ldap:///self”;)
```

You may want to restrict write access to other attributes in the password entry as well.

Step 3. Restrict write access to certain group attributes of the posix schema.

Grant write access of the cn, memberuid, gidnumber, and userpassword attributes only to the directory administrator; disallow write access by all other users. Set up access control lists (ACL) so ordinary users cannot change these attributes in the posixGroup entry in the directory. With Netscape Directory Server for HP-UX, you can use the Netscape Console or ldapmodify.

For example, the following ACI, placed in the directory at `ou=groups,ou=nis,o=hp.com`, only allows the directory administrator to modify entries below `ou=groups,ou=nis,o=hp.com`:

```
aci: (targetattr = "*")(version 3.0;acl "Disallow modification of group
 entries"; deny (write) (groupdn != "ldap:///ou=Directory Administrators,
 o=hp.com");)
```

Step 4. Grant read access of attributes of the posix schema.

Grant read access of all posix attributes to all users. If you have Netscape Directory Server for HP-UX, you can skip this step since it is the default for a typical installation. If you have another directory, make sure all users have read access to the posix attributes.

Step 5. Establish UNIX crypt as the default encryption.

Netscape's default is SHA (Secure Hash Algorithm) encryption. With the

Netscape Directory Console, you can select the Configuration tab, then select the “Database” object, then the Passwords tab, and change the Password encryption field.

Step 6. Index important entries for better performance.

Since many of your directory requests will be for the attributes listed below, you should index these to improve performance. If you don’t index, your directory may search sequentially causing a performance bottleneck.

Index on the following attributes:

- cn
- objectclass
- memberuid
- uidnumber
- gidnumber
- uid

To index these entries with Netscape Directory Server, use the Console, Configuration tab, Indexes tab, Add Attributes button.

Step 7. Create a proxy user.

Create a proxy user the NIS/LDAP Gateway will use to bind to the directory. With Netscape Directory Server for HP-UX, use the Netscape Console, Users and Groups tab, Create button.

Step 8. Set access permissions for the proxy user.

Give the proxy user (created in step 7 above) read permission for the userpassword attribute in the directory. Since the NIS/LDAP Gateway daemon, ypldapd, will authenticate to the directory as the proxy user, this user needs to be able to read the passwords. The following example ACI gives the proxy user, ypldap_proxy, permission to compare, read, and search user passwords:

```
aci:(target="ldap:///ou=raptor,ou=labteam,o=hp.com")(targetattr="userpassword")
 (version 3.0; acl "ypldapd Proxy userpassword read rights"; allow
 (compare,read,search) userdn = "ldap:///uid=proxy-user,ou=people,o=hp.com"; )
```

Step 9. For larger directories, increase the Look-through limit.

The `Look-through limit` specifies the maximum number of directory entries to examine before aborting the search operation. The default for

Netscape Directory Server 4.x for HP-UX is 5000. If you have a large directory, (greater than 2000 entries, for example), you may want to increase this. This will be less of a problem for indexed entries since the search would examine fewer entries.

To change this limit in Netscape Directory Server using the Directory Console, use the Configuration tab, select the "Database" object, the Performance tab, and edit the `Look-through limit` text box.

Step 10. For larger directories, increase the Size limit.

The `Size limit` determines the maximum number of entries to return to any query before aborting. The default for Netscape Directory Server 4.x for HP-UX is 2000. If you have a large directory, (greater than 2000 entries, for example), you should increase this.

To change this limit in Netscape Directory Server using the Directory Console, use the Configuration tab, select the server name, the Performance tab, and edit the `Size limit` text box.

Install the NIS/LDAP Gateway on Your Server

Use *swinstall*(1M) to install the NIS/LDAP Gateway software and the Client Administration Tools. See the *NIS/LDAP Gateway Release Notes* for any last-minute changes to this procedure. You can install the NIS/LDAP Gateway server and the LDAP-UX Client Administration Tools.

Import NIS Data into Your Directory

The next step is to import your NIS data into your LDAP Directory. How you do this depends on several factors. Here are some considerations when planning this:

- The migration scripts take your NIS information and generate LDIF files. These scripts can then import the LDIF files into your directory,

creating new entries in the directory. This only works if you are starting with an empty directory or creating an entirely new subtree in your directory for your NIS data.

- Your directory architect needs to decide where in your directory to place your NIS information. Here are some possibilities:
  - — Create a separate subtree for NIS data - The migration scripts can import all your NIS data into the separate subtree.
  - — Integrate the NIS information into your directory - The migration scripts may be helpful depending on where you put the NIS data in your directory. You could use them just to generate LDIF, edit the LDIF, then import the LDIF into your directory.

Steps to Importing Your NIS Data into Your Directory

Here are the steps to importing your NIS data into your directory. Modify them as needed depending on your directory.

Step 1. Determine which of your NIS maps you will migrate to your directory. **`ypwhich -m`** gives a list of maps and their master server. The maps are typically in `/var/yp/<`*`domainname`*`>`. On your client systems, the file /etc/nsswitch.conf determines which NIS files the client is using.

Step 2. Decide which migration method and scripts you will use. See “NIS to LDAP Migration Scripts” on page 41 for a complete description of the scripts, what they do, and how to use them. Modify the migration scripts, if needed.

Step 3. Back up your directory, if needed.

Step 4. Run the migration scripts.

Step 5. If the method you used above did not already do so, import the LDIF file into your directory.

Configure the NIS/LDAP Gateway

Use the following steps to configure your NIS/LDAP Gateway to work with your directory server and your NIS domain.

Step 1. Edit the configuration file, /opt/ldapux/ypldapd/etc/ypldapd.conf, and set the appropriate values. Use the comments in the file as a guide. See also "Configuration Parameters" on page 45 for details on all the parameters. Provide values at least for the following:

ypdomain	The NIS domain name.
binddn	The directory user the NIS/LDAP Gateway will bind to the directory as. You created a proxy user for this purpose in step 7 under "Create a proxy user," on page 22.
bindcred	The password for the proxy user.
basedn	The Distinguished Name in your directory where the NIS/LDAP Gateway should begin all searches.

CAUTION The file ypldapd.conf contains the proxy user's password and could represent a security risk. Restricting the permissions on this file reduces this risk.

For testing, you can set ypdomain to a new domain, then set the domain name of your test clients to that domain. When you finish testing, set it to your production domain.

After you modify the configuration file, you can copy it to your other NIS/LDAP Gateway servers.

Step 2. Verify that the proxy user can read passwords from your directory.

The following command

```
ldapsearch -D "uid=proxy-user,ou=people,o=hp.com" -h servername -w passwd -b
o=hp.com uid=username
```

binds to the directory as the proxy user and reads the entry for the user ***username***. Change this example to use your proxy user, server, base DN, and user.

You should get output with a line like the following:

```
userpassword={crypt}d92lFl8SMksl2k24
```

If you don't, your proxy user may not be configured properly. Make sure

you have access permissions set correctly for the proxy user. See “Troubleshooting” on page 33 for more information.

Step 3. If you want the NIS/LDAP Gateway to automatically restart after rebooting your system, edit the file /etc/rc.config.d/ypldapd and set YPLDAPD=1.

If you do this, you should also edit /etc/rc.config.d/namesvrs and set NIS_MASTER_SERVER=0 and NIS_SLAVE_SERVER=0 so the NIS server does not automatically restart after rebooting.

Start the NIS/LDAP Gateway Server Daemon

Step 1. If the NIS daemon is running on the same system as your NIS/LDAP Gateway server, stop the NIS daemon:

```
/sbin/init.d/nis.server stop
```

Step 2. Start the NIS/LDAP Gateway daemon. If YPLDAPD=0 in the file /etc/rc.config.d/ypldapd, use the following command:

```
/opt/ldapux/ypldapd/sbin/ypldapd
```

If YPLDAPD=1 in the file /etc/rc.config.d/ypldapd, use the following command:

```
/sbin/init.d/ypldapd start
```

To test all servers on a subnet, repeat the above steps for each NIS server on the local subnet.

Test the NIS/LDAP Gateway

This section describes some simple ways you can test the installation and configuration of your NIS/LDAP Gateway. You may need to do more elaborate and detailed testing, especially if you have a large environment.

The following procedure assumes you have created a new NIS domain called `test-ldap` for testing purposes. Modify these commands as needed for your environment.

Step 1. On an NIS client system, log in as root and change the domain by editing the file /etc/rc.config.d/namesvrs. Change the line containing NIS_DOMAIN to:

```
NIS_DOMAIN=test-ldap
```

Step 2. On the same NIS client system logged in as root, restart the NIS client process:

```
/sbin/init.d/nis.client stop
/sbin/init.d/nis.client start
```

Step 3. Use the *ll*(1) command to examine any files and make sure the owner and group of each file are accurate:

```
ll /tmp
```

If any owner or group shows up as a number instead of a user or group name, respectively, the NIS/LDAP Gateway is not functioning properly.

Step 4. Create a new file and change the file's owner to another user:

```
cd /tmp
touch file
chown newuser file
ll file
```

where ***newuser*** is the name of a different user. The final *ll*(1) command should display the file owned by the new user.

Step 5. Log in to the client system as an ordinary user, that is, a non-root user, in the directory and not in /etc/passwd. If this fails, see “Troubleshooting” on page 33.

Step 6. Once you've logged in as an ordinary user, check to see if your NIS/LDAP Gateway is serving the NIS client by giving the following command on the client system:

```
domainname
```

Step 7. Display one of your maps with a command like the following:

```
ypcat group | more
```

Step 8. Repeat steps 3 and 4 above logged in as an ordinary user.

Put the NIS/LDAP Gateway into Production

This section describes how you can put the NIS/LDAP Gateway into production in your environment, after you've completed all the verification and testing you need, determined how you will administer your directory, and informed your user community about the change. You can stop each NIS server and start the NIS/LDAP Gateway server, one system at a time, completing each subnet one at a time. Modify these commands as needed for your environment.

Step 1. If you decide to use ldappasswd, install it on the appropriate systems.

Step 2. Install the NIS/LDAP Gateway on an NIS server.

Step 3. Copy the ypldapd.conf file from another NIS/LDAP Gateway server. Modify it, if necessary, for example if you have multiple directory servers to distribute the load among or to set the domain to your production domain. See "Configuration Parameters" on page 45 for details.

Step 4. Stop the NIS server daemon on your NIS server system. Log in to the server as root and enter the following command:

```
/sbin/init.d/nis.server stop
```

Step 5. Edit the file /etc/rc.config.d/namesvrs and change NIS_MASTER_SERVER=0 and NIS_SLAVE_SERVER=0.

Step 6. If you want the NIS/LDAP Gateway to restart automatically after rebooting, edit the file /etc/rc.config.d/ypldapd and set YPLDAPD=1.

Step 7. Start the NIS/LDAP Gateway server. If YPLDAPD=0 in the file /etc/rc.config.d/ypldapd, use the following command:

```
/opt/ldapux/ypldapd/sbin/ypldapd
```

If YPLDAPD=1 in the file /etc/rc.config.d/ypldapd, use the following command:

```
/sbin/init.d/ypldapd start
```

Step 8. Repeat steps 2 through 7 above for each NIS server on a subnet. See "Test the NIS/LDAP Gateway" on page 26 for suggestions on testing. If you encounter any problems, see "Troubleshooting" on page 33.

3 Administering the NIS/LDAP Gateway

This chapter describes how to administer the NIS/LDAP Gateway to keep it running smoothly and expand it as your computing environment expands. It describes the following topics:

Starting and Stopping the NIS/LDAP Gateway

How you start and stop the NIS/LDAP Gateway depends on whether automatic restarting is enabled in the file /etc/rc.config.d/ypldapd. See “Enabling Automatic Restart” on page 30 for more information.

Start the NIS/LDAP Gateway, logged in as root, with a command like one of the following.

If automatic restart is enabled (YPLDAPD=1 in /etc/rc.config.d/ypldapd), use the following command:

```
/sbin/init.d/ypldapd start
```

If automatic restart is disabled (YPLDAPD=0 in /etc/rc.config.d/ypldapd), use the following command:

```
/opt/ldapux/ypldapd/sbin/ypldapd
```

Stop the NIS/LDAP Gateway, logged in as root, with a command like one of the following.

If automatic restart is enabled (YPLDAPD=1 in /etc/rc.config.d/ypldapd), use the following command:

```
/sbin/init.d/ypldapd stop
```

If automatic restart is disabled (YPLDAPD=0 in /etc/rc.config.d/ypldapd), use one of the following commands:

```
kill $(cat /var/run/ypldapd.pid) # default pid file location
kill pid
```

where *pid* is the process identifier of the ypldapd daemon. You can find this from the pidfile parameter in /opt/ldapux/ypldapd/etc/ypldapd.conf, (The default pidfile is /var/run/ypldapd.pid.) or by a command like the following:

```
ps -ef | grep ypldapd
```

See “The ypldapd Command” on page 37 or the *ypldapd*(8) man page for more information.

Enabling Automatic Restart

If you want the NIS/LDAP Gateway to restart automatically after rebooting the system, edit the file /etc/rc.config.d/ypldapd and set YPLDAPD=1. To disable automatic restarting, set YPLDAPD=0.

See also “Starting and Stopping the NIS/LDAP Gateway” on page 29.

Adding a Client System

Adding an NIS/LDAP Gateway client is essentially the same as adding an NIS client except for ldappasswd or whatever means you give your users for changing their password and other personal information.

For more information, see “To Change Passwords” on page 59 and “To Change Personal Information” on page 59 and “The ldappasswd Command” on page 38.

For NIS information see “To Enable NIS Client Capability” in *Installing and Administering NFS Services* available at http://docs.hp.com/hpux/communications.

Improving Performance

This section lists some ways you can improve the performance of your NIS/LDAP Gateway server.

Minimizing Enumeration Requests

Enumeration requests are directory queries that request all of a map. For example, the command **`ypcat passwd`** is an enumeration request because it requests all of the passwd map. An **`ll`** command would not be an enumeration request since it only requests specific pieces of information from maps.

Certain HP-UX operations enumerate a map from the NIS/LDAP Gateway server. For example, *csh*(1) requests the entire group map at login. *finger*(1) requests the entire passwd map whenever it runs. Applications written with the *getpwent*(3C) family of routines can enumerate a map. If these maps are large, these enumeration requests could cause other NIS/LDAP Gateway client requests to block waiting for the enumeration request to complete. For example, a user doing a simple *ll*(1) command could see a delay in response if another user is logging in with *csh*(1) or using the *finger*(1) command. If the delay is long enough, the request may time out and the client may try to rebind to another server. To minimize these situations, you may want to restrict use of the above mentioned commands.

You can also improve performance of enumeration requests by preloading maps as described in “Preloading the Cache with NIS Maps” on page 32.

Using Additional Processes to Handle Enumeration Requests

One way to reduce the impact of enumeration requests is to allow ypldapd to fork separate processes to handle them thus avoiding tying up ypldapd for the duration of the enumeration requests. Do this by setting the maxchildren parameter. This parameter specifies the maximum number of processes ypldapd will fork when doing enumeration requests. See also “Maximum Number of Processes” on page 54.

Caching

This section discusses how the NIS/LDAP Gateway caches data from the directory and how you can control aspects of caching to improve performance.

Enabling Caching

The NIS/LDAP Gateway server can cache data from the directory to reduce the load on the directory and improve overall performance of NIS operations. You enable caching by setting the caching parameter in the ypldapd.conf file to on. See “Enable or Disable Caching” on page 53 for more information.

Preloading the Cache with NIS Maps

You can configure ypldapd to preload certain NIS maps into the cache. Preloading ensures the cache is always kept current with these maps. This is particularly beneficial for the passwd map and the group map as these are often the largest and most enumerated maps. However, the more maps you preload, the longer the NIS/LDAP Gateway takes to start up.

Use the preload_cache parameter in ypldapd.conf. For example, the following command specifies preloading of the passwd.byname map and group.byname map:

```
preload_cache passwd.byname group.byname
```

For information on the preload_cache parameter see “Preload Maps into the Cache” on page 54.

NOTE For best overall performance, you should turn *off* ypall_caching by setting the ypall_caching parameter to “no” in the file ypldapd.conf and use preloaded maps instead. See “Preload Maps into the Cache” on page 54 for more information.

Setting the Frequency of Cache Refreshing

You can specify how often the cache is refreshed with the cache_dump_interval parameter as described in “Cache Lifetime” on page 53. All preloaded maps will be refreshed periodically, as specified by cache_dump_interval. Maps not preloaded will be flushed, not

refreshed. Future client requests will refill the cache.

The cache_dump_value you use depends on how often you want the cache to be updated, how often information in your directory changes, and how large your preloaded maps are. The larger the cache_dump_interval, the less frequently the preloaded maps in the cache will be updated. The smaller the cache_dump_interval, the more frequently the preloaded maps in the cache will be updated. If you or another user updates the directory, the preloaded maps will not reflect the change until the cache is refreshed. ldappasswd, however, is a special case. When a user changes their password, ldappasswd marks that password entry in the cache as stale.

One strategy is to set the cache_dump_interval to 60 if your maps are greater than 1 megabyte. This will refresh the cache once an hour. If your maps are smaller then 1 megabyte, set the cache_dump_interval to something less than an hour. The more maps you preload, the larger your cache_dump_interval should be.

Forcing a Refresh of the Cache

You can use the following command to force a refresh of the preloaded maps in the cache:

```
kill -s SIGALRM $( cat /var/run/ypldapd.pid )
```

This assumes the file /var/run/ypldapd.pid contains the process identifier of the ypldapd daemon. You configure this with the pidfile parameter in the configuration file as described under “PID File” on page 56.

Troubleshooting

This section lists problems you may encounter, how to troubleshoot and solve them.

Log Files

You can check log files to see if any unusual incidents have occurred with the NIS/LDAP Gateway or your directory. The NIS/LDAP Gateway logs important events and errors to the file /var/adm/syslog/syslog.log. The Netscape Directory Server for HP-UX logs information to files in the logs

directory under /var/opt/netscape/server4/slapd-<*serverID*> where slapd-<*serverID*> is the name of your directory server.

User Cannot Log on to Client System

If a user cannot log in to a client system, perform the following checks.

- Make sure the NIS/LDAP Gateway daemon, ypldapd, is running. Use the following command:

  ps -ef | grep ypldapd

  If it is not running, restart it as described in “Starting and Stopping the NIS/LDAP Gateway” on page 29.

- Make sure the NIS daemon, ypserv, is not running. Use the following command:

  ps -ef | grep ypserv

  If it is running, stop it with a command like the following:

  /sbin/init.d/nis.server stop

- Make sure ypldapd can authenticate to the directory. If you are using a proxy user (determined by the `binddn` parameter in the file /opt/ldapux/ypldap/etc/ypldapd.conf), try searching for one of your user's information in the directory with a command like the following:

ldapsearch -D "uid=proxy-user,ou=people,o=hp.com" -h *servername* -w *passwd* -b “o=hp.com” uid=*username*

  using the name of your directory server, proxy user, user name, and password.

  You should get output with a line like the following:

  `userpassword={crypt}d92lFl8SMksl2k24`

  If you don't, your proxy user may not be configured properly. Make sure you have access permissions set correctly for the proxy user. See “Configure Your Directory” on page 20 for details on configuring the proxy user.

  You can also try binding to the directory as the directory administrator and reading the user's information.

- Use the Netscape Directory Console to authenticate to the directory as the directory administrator. Check the ACLs for the proxy user. Make sure the proxy user can view the userpassword attribute and

all the attributes listed below. If not, change the ACI to allow this. Make sure all users can read their own information. If they cannot, change the ACI to allow this.

Make sure all users have the following attributes and can read them:

— posixaccount
— loginshell
— uidnumber
— uid
— gidnumber
— memberuid
— homedirectory

- Make sure UNIX crypt is the default encryption. Verify in Netscape with a command like the following:

ldapsearch -b "o=hp.com" -D "*AdminDN*" -w "*AdminPw*" uid=*username*

where *AdminDN* is the directory administrator's relative distinguished name, *AdminPw* is the administrator's password, and *username* is the name of a user in the directory. The user must be an inetorgperson or posixaccount.

The output should show something like the following:

```
userPassword: {crypt}3Adkd9D2s9234sf
```

If it shows either of the following:

```
userPassword: {sha}3Adkd9D2s9234sf
userPassword: mypass123
```

change it to use `crypt` encryption. `sha` indicates secure hash algorithm encryption and no bracketed text indicates a clear text password.

You can also check the default encryption in the Directory Console. Select the Configuration tab, then select the "Database" object, then the Passwords tab, and check the Password encryption field.

- Make sure that hidden passwords are disabled. The `hide_passwords` parameter in ypldapd.conf should be set to no.
- Try restarting the client with a command like the following:

```
/sbin/init.d/nis.client stop
/sbin/init.d/nis.client start
```

4 Command and Tool Reference

This chapter describes all the commands and tools associated with the NIS/LDAP Gateway:

- “The ypldapd Command” on page 37 describes the NIS/LDAP Gateway daemon and command and its parameters.
- “The ldappasswd Command” on page 38 describes the command that changes passwords in your directory.
- “LDAP Directory Tools” on page 40 briefly describes the tools ldapsearch, ldapmodify, and ldapdelete.
- “NIS to LDAP Migration Scripts” on page 41 describes the shell and perl scripts that migrate your NIS data to your LDAP directory.
- “Configuration Parameters” on page 45 describes the various parameters for configuring ypldapd in the file ypldapd.conf.

The ypldapd Command

This section describes the ypldapd command and its parameters. See also the *ypldapd*(1) man page.

ypldapd is the command you use to start the NIS/LDAP Gateway daemon. It is a server process that provides information to any process that makes rpc calls to the NIS client routines. This includes any process that calls the standard UNIX naming service routines, such as *getpwent*(3C), *gethostent*(3C) and so forth, as well as the special tools *ypcat*(1) and *ypmatch*(1) provided as part of the NIS product.

ypldapd emulates the equivalent process ypserv by providing an RPC call-compatible interface. Rather than consulting NIS map files as ypserv does, however, ypldapd gets its data from LDAP directories. Communication to and from ypldapd is by means of RPC calls. Lookup functions are described in *ypclnt*(3N), and are supplied as C-callable functions in /lib/libc.

You can configure ypldapd to cache the information it gets from the LDAP directory to improve performance and reduce network traffic. For more information on caching, see “Improving Performance” on page 31.

Syntax

ypldapd [-v] [-c *configfile*]

where

-v displays the version number of the software. Include this number when reporting problems.

-c *configfile* allows you to specify an alternate configuration file. The default configuration file is /opt/ldapux/ypldapd/etc/ypldapd.conf.

You must execute this command logged in as root. See also "Starting and Stopping the NIS/LDAP Gateway" on page 29.

Examples

The following command starts the NIS/LDAP Gateway daemon:

```
/opt/ldapux/ypldapd/sbin/ypldapd
```

The following command starts the NIS/LDAP Gateway daemon using /tmp/ypldapd.conf as its configuration file:

```
/opt/ldapux/ypldapd/sbin/ypldapd -c /tmp/ypldapd.conf
```

See also "Starting and Stopping the NIS/LDAP Gateway" on page 29.

The ldappasswd Command

This section describes the ldappasswd command and its parameters.

The ldappasswd program, installed in /opt/ldapux/bin, allows users to change their passwords in the directory. Changing a user's password with ldappasswd marks the cache entry for that user as stale, if caching is enabled. ldappasswd assumes an LDAP directory server that supports {crypt} format. (For more information, see *passwd*(1) and *crypt*(3C).)

Syntax

ldappasswd [*options*]

where ***options*** can be any of the following:

-b *basedn*	specifies ***basedn*** as the base distinguished name of where to start searching. If ypldapd is running, then this is not required.
-h *host*	specifies ***host*** as the LDAP server name or IP address. If ypldapd is running, then this is not required.
-c	generates an encrypted password on the client. Use this parameter for directories that do not automatically encrypt passwords. The default is to send the new password in plain text to the directory. Netscape Directory Server 4.x for HP-UX supports automatic encryption of passwords.
-v	prints the software version and exits.
-p *port*	specifies ***port*** as the LDAP server TCP port number.
-D *binddn*	specifies ***binddn*** as the bind distinguished name.
-w *passwd*	specifies ***passwd*** as the bind password (for simple authentication).
-l login	specifies ***login*** as the uid of the account to change; defaults to the current user.

If the NIS client is configured to an NIS/LDAP Gateway server, the -b, -h, -p, -D, -w, and -l options are not required. These options are useful for changing a password from a system that is not an NIS client or for changing another user's password.

Examples

The following command changes the password in the directory for the currently logged in user:

```
ldappasswd
```

The following command changes the password in the directory for the user **steves**:

```
ldappasswd -l steves
```

LDAP Directory Tools

This section briefly describes the tools ldapsearch, ldapmodify, and ldapdelete. These tools are described in detail in the *Netscape Directory Server for HP-UX Administrator's Guide* available at http://docs.hp.com/hpux/internet.

Additional tools are available in the directory /opt/ldapux/contrib/bin, however these tools are unsupported. See the file /opt/ldapux/contrib/bin/README for more information.

ldapsearch

You use the ldapsearch command-line utility to locate and retrieve LDAP directory entries. This utility opens a connection to the specified server using the specified distinguished name and password, and locates entries based on the specified search filter. Search results are returned in LDIF format. For details, see the *Netscape Directory Server for HP-UX Administrator's Guide* available at http://docs.hp.com/hpux/internet.

ldapmodify

You use the ldapmodify command-line utility to modify entries in an existing LDAP directory. ldapmodify opens a connection to the specified server using the distinguished name and password you supply, and modifies the entries based on the LDIF update statements contained in a specified file. Because ldapmodify uses LDIF update statements, ldapmodify can do everything ldapdelete can do. For details, see the *Netscape Directory Server for HP-UX Administrator's Guide* available at http://docs.hp.com/hpux/internet.

ldapdelete

You use the delete command-line utility to delete entries from an existing LDAP directory. ldapdelete opens a connection to the specified server using the distinguished name and password you provide, and deletes the entry or entries. For details, see the *Netscape Directory Server for HP-UX Administrator's Guide* available at http://docs.hp.com/hpux/internet.

NIS to LDAP Migration Scripts

This section describes the shell and perl scripts that can migrate your NIS data either from source files or NIS maps to your LDAP directory. These scripts are found in /opt/ldapux/migrate. The two shell scripts `migrate_all_online.sh` and `migrate_all_nis_online.sh` migrate all your NIS maps, while the perl scripts `migrate_aliases.pl`, `migrate_group.pl`, `migrate_hosts.pl`, and so forth, migrate individual NIS maps. The shell scripts call the perl scripts.

The migration scripts require perl, version 5 or later, which is installed with the NIS/LDAP Gateway in /opt/ldapux/contrib/bin/perl.

Naming Context

The naming context specifies where in your directory your NIS data will be, under the base DN. For example, if your base DN is "ou=NIS,o=hp.com," the passwd map would be at "ou=People,ou=NIS,o=hp.com". Table 4-1 shows the default naming context. The default will work in most cases.

Table 4-1 Default Naming Context

Map Name	Location in the Directory Tree
passwd	ou=People
group	ou=Groups
aliases	ou=mailGroups
fstab	ou=Mounts
netgroup.byuser	nisMapName=netgroup.byuser
netgroup.byhost	nisMapName=ngetgroup.byhost
netgroup	ou=Netgroups
hosts	ou=Devices
networks	ou=tcpIp
protocols	ou=tcpIp

Table 4-1 Default Naming Context

Map Name	Location in the Directory Tree
rpc	ou=tcpIp
services	ou=tcpIp

If you change the default naming context, modify the file migrate_common.ph and change it to reflect your naming context. You must also change the file /opt/ldapux/ypldapd/etc/namingcontexts.conf. See also “Naming Context Mappings” on page 47.

Migrating All Your Files

The two shell scripts `migrate_all_online.sh` and `migrate_all_nis_online.sh` migrate all your NIS maps either to LDIF or into your directory. The `migrate_all_online.sh` shell script gets NIS information from the appropriate source files, such as /etc/passwd, /etc/group, /etc/hosts, and so forth. The `migrate_all_nis_online.sh` script gets NIS information from your NIS maps using the *ypcat*(1) command. The scripts take no parameters but prompt you for needed information. They also prompt you for whether to leave the output as LDIF or to add the entries to your directory. These scripts call the perl scripts described under “Migrating Individual Files” on page 43. You may need to modify these scripts to work in your environment.

NOTE

The scripts use ldapmodify to add entries to your directory. If you are starting with an empty directory, it may be faster for you to use `ldif2db` or `ns-slapd ldif2db` with the LDIF file. See the *Netscape Directory Server Administrator's Guide* for details on `ldif2db` and `ns-slapd`.

If any entry in the migrated LDIF file is already in your directory, the script will stop at that point. The entries previous to the duplicate will be in the directory. To continue, you can edit the LDIF files to remove the entries already added up to the duplicate, resolve the duplicate, then continue adding the remaining entries. Alternatively you can remove the entries from the directory that were already added, resolve the duplicate, then re-add all the entries from the LDIF file.

Migrating Individual Files

The following perl scripts migrate each of your NIS source files in /etc to LDIF. These scripts are called by the shell scripts described under “Migrating All Your Files” on page 42. The perl scripts get NIS information from the input source file and output LDIF.

Environment Variables

When using the perl scripts to migrate individual files, you need to set the following environment variable:

LDAP_BASEDN The base distinguished name where you want your data.

For example, the following command sets the base DN to “o=hp.com”:

```
export LDAP_BASEDN="o=hp.com"
```

General Syntax for Perl Migration Scripts

All the perl migration scripts use the following general syntax:

scriptname inputfile **[*outputfile*]**

where

scriptname is the name of the particular script you are using. The scripts are listed below.

inputfile is the name of the appropriate NIS source file corresponding to the script you are using.

outputfile is optional and is the name of the file where the LDIF is written. stdout is the default output.

Migration Scripts

The migration scripts are:

- `migrate_aliases.pl` migrates aliases in /etc/aliases to LDIF information, conforming to the RFC 822 MailGroup schema.
- `migrate_base.pl` creates base DN information.
- `migrate_fstab.pl` migrates file system information in /etc/fstab.
- `migrate_group.pl` migrates groups in /etc/group.
- `migrate_hosts.pl` migrates hosts in /etc/hosts.

- `migrate_netgroup.pl` migrates netgroups in /etc/netgroup.
- `migrate_netgroup_byhost.pl` migrates the netgroup.byhost map. This script must be run as root because it calls /usr/sbin/revnetgroup.
- `migrate_netgroup_byuser.pl` migrates the netgroup.byuser map. This script must be run as root because it calls /usr/sbin/revnetgroup.
- `migrate_networks.pl` migrates networks in /etc/networks.
- `migrate_passwd.pl` migrates users in /etc/passwd.
- `migrate_protocols.pl` migrates protocols in /etc/protocols.
- `migrate_rpc.pl` migrates RPCs in /etc/rpc.
- `migrate_services.pl` migrates services in /etc/services.
- `migrate_common.ph` is a set of routines and configuration information all the perl scripts use.

Examples

The following are some examples using the migration scripts.

The following command converts all NIS files in /etc to LDIF:

```
$ migrate_all_online.sh
```

The following commands convert /etc/passwd into LDIF and output it to stdout:

```
$ export LDAP_BASEDN="dc=aceindustry,dc=com"
$ migrate_passwd.pl /etc/passwd

dn: uid=jbloggs,ou=People,dc=aceindustry,dc=com
uid: jbloggs
cn: Joe Bloggs
objectclass: top
objectclass: posixAccount
objectclass: account
userPassword: {crypt}daCXgaxahRNkg
loginShell: /bin/ksh
uidNumber: 20
gidNumber: 20
homeDirectory: /home/jbloggs
gecos: Joe Bloggs,42U-C3,555-1212
```

The following commands convert /etc/group into LDIF and place the result in /tmp/group.ldif:

```
$ export LDAP_BASEDN="o=hp.com"
$ migrate_group.pl /etc/group /tmp/group.ldif

dn: cn=mira.aceindustry.com,ou=Groups,o=hp.com
objectclass: posixGroup
objectclass: top
ipHostNumber: 10.1.70.5
cn: mira
cn: www.hp.com
cn: mira.hp.com
userPassword: {crypt}*
gidNumber: 325
```

The following command migrates /etc/hosts:

```
migrate_hosts.pl /etc/hosts
```

Configuration Parameters

You can change the NIS/LDAP Gateway's run-time configuration parameters in the file /opt/ldapux/ypldapd/etc/ypldapd.conf. This section describes these parameters in detail.

NOTE

Because the configuration file contains a password, you should protect it by making the file only accessible by root. Use a command like the following:

```
chmod 600 ypldapd.conf
```

Changing Configuration Parameter Values

You can change configuration parameter values by editing the /opt/ldapux/ypldapd/etc/ypldapd.conf file. Each entry in the file consists of a key word, followed by white space, followed by the value for that parameter. Any line starting with a pound sign or hash symbol (#) is treated as a comment and ignored.

NIS Domain to Serve

Specifies the NIS domain that the NIS/LDAP Gateway serves. See *domainname*(1) for more information.

Required.

Syntax

ypdomain *domain-name*

where *domain-name* is the domain name ypldapd is to serve.

Example

ypdomain dev-team

LDAP Server Name

Specifies the host name of your LDAP server. The host's IP address must be resolvable without consulting NIS (through NIS or /etc/hosts) or specified in dotted decimal notation, to avoid reentrancy problems. It is suggested you use a DNS name (and configure /etc/nsswitch.conf to perform host lookups in DNS before NIS) or an IP address.

Required.

Syntax

ldaphost *server-name*

where *server-name* is a host name or IP address.

Example

ldaphost nis-ldap

ldaphost 15.0.96.234

LDAP Protocol Version

Specifies the version of the LDAP protocol your directory server is using.

Optional.

Default Value

2

Valid Range

2 | 3

Syntax

ldapversion *integer*

Example

ldapversion 3

Search Base DN

Specifies the Distinguished Name in your directory where the NIS/LDAP Gateway should begin all searches.

Required.

Syntax

basedn *DN*

Example

basedn o=hp.com

basedn dc=aceindustry, dc=com

Naming Context Mappings

Specifies the file containing name mappings from NIS names to distinguished names in your directory. The default mappings are in the file /opt/ldapux/ypldapd/etc/namingcontexts.conf. The default mappings will work in most cases. Edit this file if you put your NIS data in other than the default places. See also “Naming Context” on page 41.

Optional.

Default Value

namingcontexts namingcontexts.conf

where namingcontexts.conf is found in /opt/ldapux/ypldapd/etc/.

Syntax

namingcontexts *filename*

Example

namingcontexts namingcontexts.conf

Bind DN

Specifies the distinguished name of the proxy user the NIS/LDAP Gateway uses to bind to the directory.

Optional.

Default value

The default is to bind anonymously.

Syntax

binddn *DN*

Example

binddn cn=Directory Manager

binddn cn=proxyuser, ou=people, o=hp.com

Bind DN Password

Specifies the credentials or password of the proxy user the NIS/LDAP Gateway uses to bind to the directory. See “Bind DN” above.

Optional, but required if using a proxy user.

NOTE

You should protect this password in your configuration file by making the file ypldapd.conf only accessible by root with a command like the following:

```
chmod 600 ypldapd.conf
```

Syntax

bindcred *credential*

Example

bindcred ldap1234

LDAP Port

Specifies the TCP port number for the NIS/LDAP Gateway to connect to your LDAP directory server.

Optional.

Default

389

Syntax

ldapport *integer*

Example

ldapport 6249

LDAP Search Scope

Specifies how deep the NIS/LDAP Gateway should go when searching your directory.

Optional.

Default

sub

Valid Range

sub | one | base

where:

- sub means the NIS/LDAP Gateway is to search the base DN and all of its descendants; that is, the entire subtree.

- one means search only the immediate children of the base DN; that is, one level down.
- base means search only the base DN. This value should not be used as it is too restrictive, effectively preventing searching below the base DN.

Syntax

scope *level*

Example

scope one

LDAP Alias Dereference Policy

Specifies how the NIS/LDAP Gateway should handle aliases when searching your LDAP directory server.

Optional.

NOTE Netscape Directory Server for HP-UX implements referrals instead of alias dereferencing. See the *Netscape Directory Server Deployment Guide* for details on referrals.

Default

deref never

Valid Range

never | find | search | always

where:

- never means the NIS/LDAP Gateway should never dereference aliases.
- find means dereference only when finding an alias.
- search means dereference only when searching.
- always means dereference always.

Syntax

deref *level*

Example

deref never

Fall Through to NIS

Specifies whether the NIS/LDAP Gateway should search an NIS domain if the requested information is not found in the LDAP directory.

Optional.

Default

extended on

Valid Range

on | off

Syntax

extended *Boolean*

Example

extended off

Parent NIS Domain

Specifies the NIS domain to fall through to if the needed information is not found in the directory. Maps not supported by the NIS/LDAP Gateway and maps already fulfilled by the directory will be supplemented by binding to the specified NIS parentdomain.

Optional.

Syntax

parentdomain *domainname*

Example

parentdomain nisusers

Fall Through to DNS

Specifies whether the NIS/LDAP Gateway should search a DNS server if the requested host information is not found in the LDAP directory.

Optional.

Default

dns_lookups on

Valid Range

on | off

Syntax

dns_lookups *Boolean*

Example

dns_lookups off

Search Time Limit

Specifies how long, in seconds, the NIS/LDAP Gateway should search the directory before aborting the search operation.

Optional.

Default

The default is no timeout.

Valid Range

0 to 2^{32} (0 means no time limit on searches.)

Syntax

timelimit *integer*

Example

timelimit 6000

Enable or Disable Caching

Specifies whether the NIS/LDAP Gateway should cache information from the directory. See “Caching” on page 32 for more information.

Optional.

Default

caching on

Valid Range

on | off

Syntax

caching *Boolean*

Example

caching off

Cache Lifetime

Specifies how often, in minutes, the NIS/LDAP Gateway should refresh the preloaded maps in the cache and flush all other maps from the cache. See “Setting the Frequency of Cache Refreshing” on page 32 for more information.

Optional.

Default

cache_dump_interval 15

Valid Range

0 to 2^{32} (0 means never refresh the cache.)

Syntax

cache_dump_interval *integer*

Example

cache_dump_interval 30

Preload Maps into the Cache

Specifies what maps, if any, should be preloaded into the cache. Caching must be enabled with the caching parameter as described in “Enable or Disable Caching” on page 53. See also “Caching” on page 32.

Optional.

Default

No maps preloaded into the cache.

Syntax

preload_cache *mapname* [*mapname2* [... *mapnameN*]]

Recommended

preload_cache group.byname

Example

preload_cache passwd group hosts

Maximum Number of Processes

Specifies the maximum number of processes to fork for enumeration requests. See “Minimizing Enumeration Requests” on page 31 for more information.

Optional.

Default

maxchildren 0

Recommended

5 or greater

Syntax

maxchildren *integer*

Example

maxchildren 10

Use Caching for Enumeration Requests

Specifies whether enumeration requests use caching. Filling the cache on an enumeration request can tie up the NIS/LDAP Gateway daemon for a long time, delaying service of other NIS requests, causing clients to fail or rebind to another server.

NOTE You should preload maps instead of caching enumeration requests. See “Preload Maps into the Cache” on page 54. See also “Minimizing Enumeration Requests” on page 31 for more information.

Optional.

Default

ypall_caching off

Valid Range

on | off

Recommended

ypall_caching off

Syntax

ypall_caching *Boolean*

Example

ypall_caching off

NIS Master Host Name

Specifies the NIS domain the **ypwhich** command should return. By default, **ypwhich** returns the name of the local host.

Optional.

Syntax

ypmaster *hostname*

Example

ypmaster nisserver

PID File

Specifies the file in which to write the process identifier (PID) for the NIS/LDAP Gateway daemon, ypldapd. If you don't specify a full path, the file is placed in the root directory, /.

Optional.

Default

pidfile /var/run/ypldapd.pid

Recommended

pidfile /var/run/ypldapd.pid

Syntax

pidfile *filename*

Example

pidfile /tmp/ypldapd.pid

Enable or Disable Shadow Passwords

NOTE Shadow passwords are not supported in this release.

You must set this parameter to no or you will not be able to log in.

Default

hide_passwords no

Valid Range

yes | no

Syntax

hide_passwords *Boolean*

Example

hide_passwords no

5 User Tasks

This chapter describes the following tasks your users will need to do:

- “To Change Passwords” on page 59
- “To Change Personal Information” on page 59, such as login shell, phone number and location

To Change Passwords

On HP-UX, users change their passwords with the *passwd*(1) command which changes /etc/passwd or the NIS maps or the *yppasswd*(1) command which changes the NIS maps. With users' passwords in the directory, they must use a different method of changing their password.

Users change their password with the ldappasswd command. This command is similar to the yppasswd command. It changes a user's password in the LDAP directory. For details on this command, see “The ldappasswd Command” on page 38.

You can make ldappasswd available to your users by installing it on all your client systems or putting it on a central system accessible to your users.

Alternatively, your users can use a simple LDAP gateway through a web browser connected to the directory to change their password. The advantage to this method is that they can also change their other personal information as described below.

To Change Personal Information

On HP-UX, users change their personal information (or gecos information) such as full name, phone number, and location with the *chfn*(1) command which changes /etc/passwd or the NIS maps. HP-UX users change their login shell with the *chsh*(1) command, which also changes /etc/passwd or the NIS maps. With this personal information in

the directory, they must use a different method to change it.

If you have Netscape Directory Server for HP-UX, you can use the Netscape Console or the ldapmodify command to change personal information. Or you can use a simple LDAP gateway through a web browser to display and change this information.

Glossary

See also the Glossary in the *Netscape Directory Server for HP-UX Administrator's Guide* available at http://docs.hp.com/hpux/internet.

Access Control Instruction A specification controlling access to entries in a directory.

Access Control List One or more ACIs.

ACI *See Access Control Instruction*

ACL *See Access Control List.*

IETF Internet Engineering Task Force; the organization that defines the LDAP specification. See http://www.ietf.org.

LDAP *See Lightweight Directory Access Protocol*

LDIF *See LDAP Data Interchange Format*

LDAP Data Interchange Format (LDIF) The format used to represent directory server entries in text form.

ldappasswd A command to change a user's password in the LDAP directory.

Lightweight Directory Access Protocol (LDAP) A standard, extensible set of conventions specifying communication between clients and servers across TCP/IP network connections. *See also SLAPD.*

Network Information Service (NIS) A distributed database system providing centralized management of common configuration files, such as /etc/passwd and /etc/hosts.

NIS *See Network Information Service*

RFC Request for Comments; a document and process of standardization from the IETF.

RFC 2307 The IETF specification for using LDAP as a Network Information Service; required by the NIS/LDAP Gateway. See http://www.ietf.org/rfc/rfc2307.txt.

SLAPD The University of Michigan's stand-alone implementation of LDAP, without the need for an X.500 directory.

ypldapd The NIS/LDAP Gateway daemon. It replaces the NIS ypserv daemon by accepting NIS client requests and getting the requested

information from an LDAP directory rather than from NIS maps.

Index