

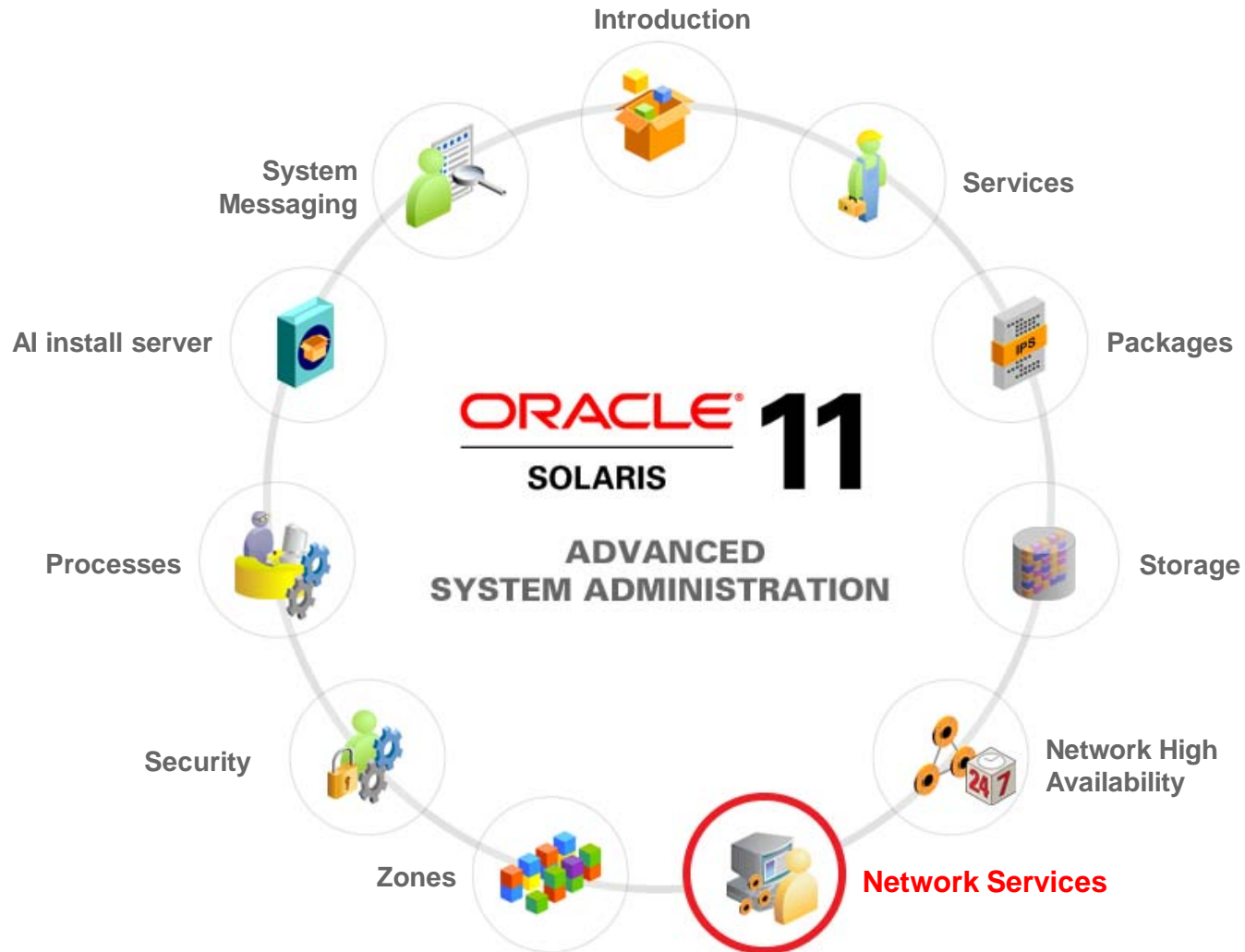
Administering Network Services

Objectives

After completing this lesson, you should be able to configure:

- Network File System (NFS)
- A Domain Name System (DNS) client
- A Lightweight Directory Access Protocol (LDAP) client

Job Workflow



Agenda

- Configuring the Network File System (NFS)
- Configuring a Domain Name System (DNS) client
- Configuring a Lightweight Directory Access Protocol (LDAP) client

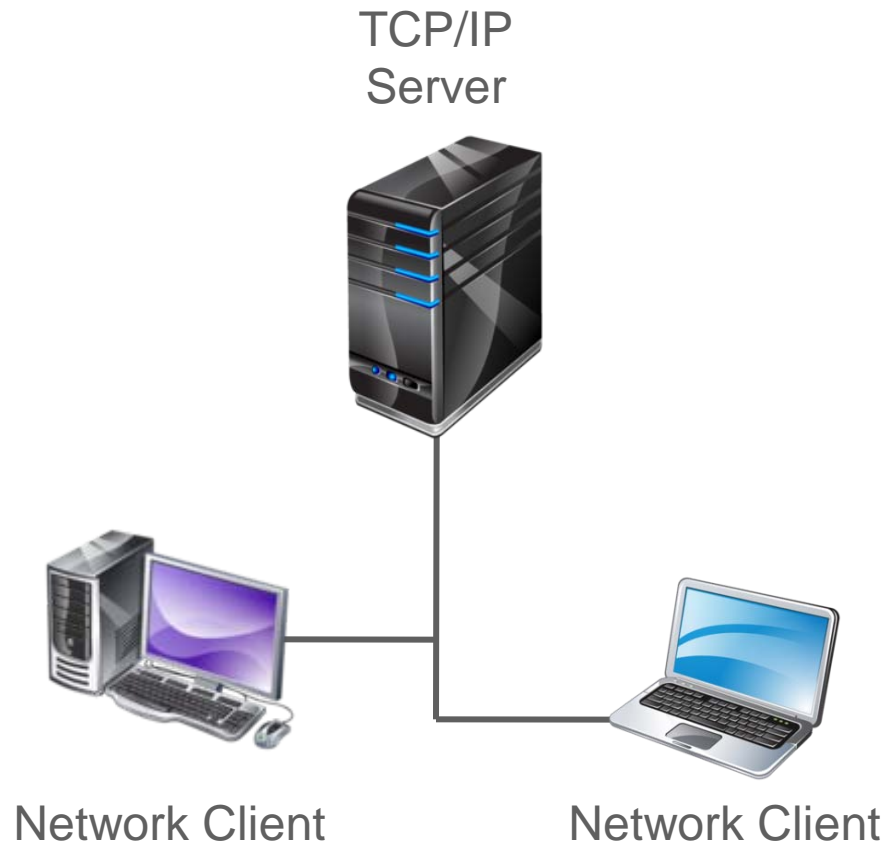
Importance of Network Services

Network services are required to ensure the following:

- Computers of different architectures that run different operating systems are able to share file systems across a network.
- You can look up IP addresses for:
 - Internet host names
 - Host names for IP addresses that are distributed across the network
- You have a directory structure that:
 - Includes details of various resources and identities
 - Can be accessed across networks

Configuring Network Services

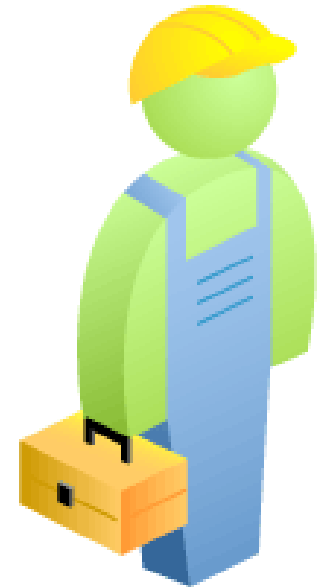
- RARP/ARP
- TFTP
- NFS
- Name service
 - NIS, LDAP, DNS



Network File System: Overview

The Network File System (NFS):

- Allows access to file systems over the network
- Enables any system to access any other system's file systems
- Has the following advantages:
 - Accesses the same data
 - Reduces storage costs
 - Provides data consistency and reliability
 - Provides transparency
 - Reduces administration overhead
 - Provides heterogeneous environments
 - Enables automatic file sharing



Configuring NFS

This section covers the following topics:

- Configuring the NFS server
- Checking the NFS services status
- Configuring the NFS client
- Selecting a different version of NFS on a server
- Enabling the automount service
- Displaying NFS server and client statistics

Configuring the NFS Server

1. Create a ZFS file system for the files you want to share.
2. To share the file system:
 - a. Set the ZFS `share` property.
 - b. Set the ZFS `share.nfs` property to `on`.
3. Use the `share` command to verify what is being shared.

```
# zfs create rpool/export/home/docs
# zfs set share=name=docs,path=/export/home/docs,prot=nfs \
rpool/export/home/docs
name=docs,path=/export/home/docs,prot=nfs
# zfs set share.nfs=on rpool/export/home/docs
# zfs set compression=on rpool/export/home/docs
# share
docs      /export/home/docs  nfssec=sys,rw
```

Checking the NFS Services Status

To check the status of the NFS services, use `svcs -a | grep nfs`.

```
# svcs -a | grep nfs
disabled      7:01:37  svc:/network/nfs/cbd:default
disabled      7:01:37  svc:/network/nfs/client:default
online        7:01:37  svc:/network/nfs/fedfs-client:default
online        7:01:37  svc:/network/nfs/mapid:default
online        16:31:11  svc:/network/nfs/status:default
online        16:31:12  svc:/network/nfs/nlockmgr:default
online        16:31:15  svc:/network/nfs/rquota:default
online        16:31:17  svc:/network/nfs/server:default
```

Configuring the NFS Client

1. Run `dfshares server` to verify that you can view the shared resource.
2. Create a directory to use as the mount point.
3. Run `mount -F nfs -o ro server:resource /directory` to specify the resource to be mounted.
4. Verify that the files in the shared resource can be shared.

```
# dfshares server1
RESOURCE                                SERVER    ACCESS    TRANSPORT
server1:/export/home/docs              server1    -          -
# mkdir /docs
# mount -F nfs -o ro server1:/export/home/docs /docs
# cd /docs
server1:/docs# ls
assetlist
```

Selecting a Different Version of NFS on a Server

To select a different version of NFS on a server or client, use the `sharectl set` command.

Example:

To set a server or client to provide only NFS version 3:

Server:

```
# sharectl set -p server_versmax=3 nfs
# sharectl set -p server_versmin=3 nfs
```

Client:

```
# sharectl set -p client_versmax=3 nfs
# sharectl set -p client_versmin=3 nfs
```

Enabling the Automount

To enable or disable the automount service, use the `svcadm` command.

Enable service:

```
# svcadm enable autofs
```

Mount file system:

```
# cd /net/server1/export/share/local
```

Disable service:

```
# svcadm disable autofs
```

Displaying NFS Server and Client Statistics

To display statistics about the NFS service on the client or server, use the `nfsstat` command.

```
# nfsstat -c
Client rpc:
Connection oriented:
calls      badcalls  badxids   timeouts  newcreds  badverfs  timers
1595799    1511      59        297       0         0         0
cantconn   nomem     interrupts
1198       0         7
Connectionless:
calls      badcalls  badxids   timeouts  newcreds  badverfs  timers
1595799    1511      59        297       0         0         0
. . . . .
Client nfs:
calls      badcalls  clgets    cltoomany
1640097    3112     1640097   0
. . . . .
Client nfs_acl:
Version 2: (3105 calls)
null       getacl    setacl     getattr   access    getxattrdir
0 0%       0 0 %     0 0%      3105 100% 0 0%      0 0%
```

Practice 6-1 Overview: Configuring the NFS

This practice covers the configuration of the following:

- NFS server
- NFS client

Agenda

- Configuring the Network File System (NFS)
- Configuring a Domain Name System (DNS) client
- Configuring a Lightweight Directory Access Protocol (LDAP) client

Domain Name System: Overview

The Domain Name System (DNS) is:

- A hierarchical, distributed database that is implemented on a TCP/IP network
- Primarily used to look up IP addresses for Internet host names and host names for IP addresses
- Used to store other Internet-related host information, such as mail exchange routing information, location data, and available services

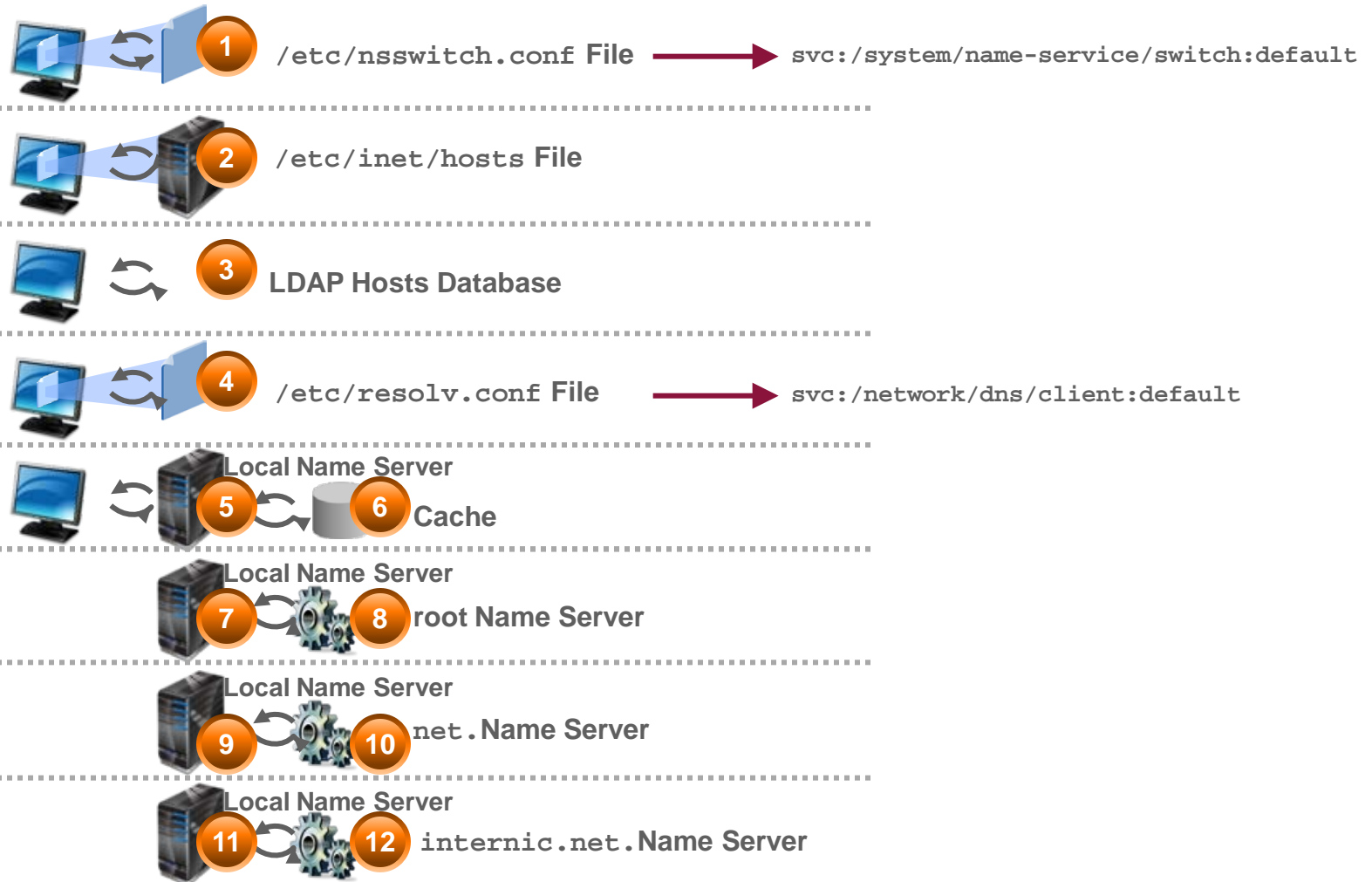
How DNS Works

1. A DNS client requests information about a host name from one or more name servers and then waits for a response.
2. DNS servers respond to requests after looking up one of the following:
 - Information cache that was loaded from file or a third-party database on a DNS master
 - Network from a cooperating DNS slave server
3. If found, the host name is resolved.
4. If there is no response and the server is not responsible for the domain in question, the service recursively requests (if permitted) the host name from other servers and caches that response.

DNS Name Resolution

- *Name resolution* is the process of translating a domain name to an IP address (and vice versa).
- The name resolution process in Oracle Solaris 11 is implemented through SMF services.
 - The `/etc/resolv.conf` file (which determines the name resolution search list and the address of the DNS servers) is now an SMF service:
`svc:/network/dns/client:default`
 - The `/etc/resolv.conf` file is activated by a reference to the DNS entry in the `/etc/nsswitch.conf` file.
 - The `/etc/nsswitch.conf` file is also an SMF service:
`svc:/system/name-service/switch:default`

Name Resolution Process



Checking the Connection to the DNS Server

To check the connectivity, use `nslookup host_IP_address`.

```
# nslookup 192.168.0.100
Server:      192.168.0.100
Address:     192.168.0.100#53
```

```
100.0.168.192.in-addr.arpaname = s11-server1.mydomain.com
```

Practice 6-2 Overview: Configuring a DNS Client

In this practice, you configure a DNS client.

Note: The DNS server is already set up for you because setup is usually the job of a network administrator.

Agenda

- Configuring the Network File System (NFS)
- Configuring a Domain Name System (DNS) client
- Configuring a Lightweight Directory Access Protocol (LDAP) client

Lightweight Directory Access Protocol: Overview

Lightweight Directory Access Protocol (LDAP):

- Allows access to directory servers for distributed naming and other directory services
- Supports a hierarchical database structure
- Can be used to provide naming services in both UNIX and multiplatform environments

Preparing for LDAP Client Setup

The requirements for an Oracle Solaris client to use LDAP as a naming service are:

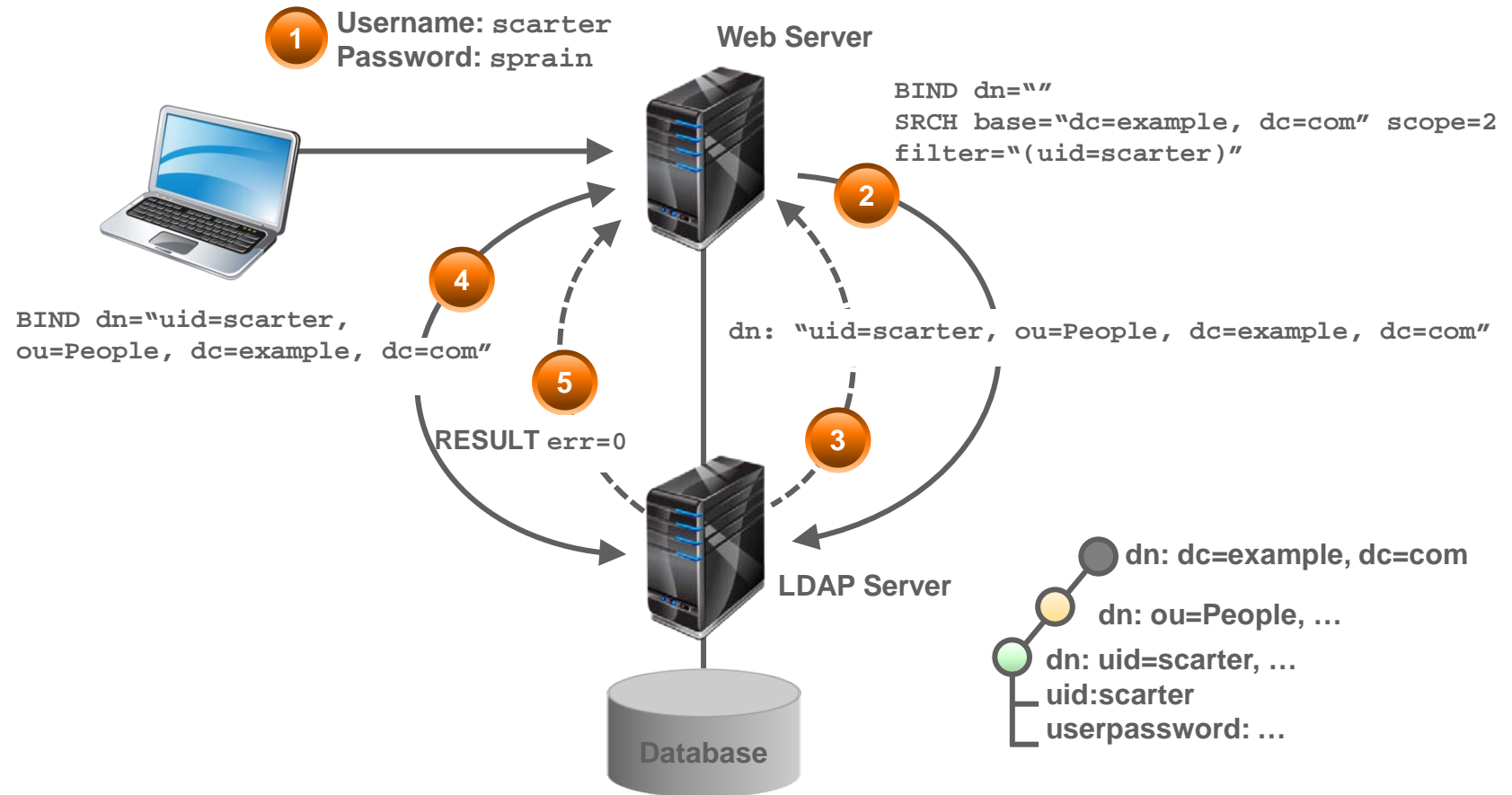
- The client's domain name must be served by the LDAP server.
- The name service switch must point to LDAP for the required services.
- The client must be configured with all the parameters that define its behavior.
- `ldap_cachemgr` must be running on the client.
- At least one server for which a client is configured must be running.

LDAP and the SMF

SMF manages the LDAP client service.

SMF Feature	LDAP Client Service
<code>svcadm</code>	Used to enable, disable, or restart the LDAP client service
<code>svc:/network/ldap/client</code>	The fault management resource identifier (FMRI) for the LDAP client service
<code>network/nis/domain</code>	During the configuration process, this service is also enabled to supply the domain name to be used by the <code>network/ldap/client</code> service
<code>svcs</code>	Used to query the status of the LDAP client and the <code>ldap_cachemgr</code> daemon

How LDAP Works



Practice 6-3 Overview: Configuring an LDAP Client

In this practice, you configure an LDAP client.

Note: The LDAP server is already set up for you because setup is usually the job of a network administrator.

Summary

In this lesson, you should have learned how to configure:

- Network File System (NFS)
- A Domain Name System (DNS) client
- A Lightweight Directory Access Protocol (LDAP) client