Installation Guide

iPlanet Directory Access Router

Version 5.0

July 2001

THIS DOCUMENTATION IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

CETTE DOCUMENTATION EST FOURNIE “EN L'ÉTAT”, ET TOUTES CONDITIONS EXPRESSES OU IMPLICITES, TOUTES REPRÉSENTATIONS ET TOUTES GARANTIES, Y COMPRIS TOUTE GARANTIE IMPLICITE D'APTITUDE À LA VENTE, OU À UN BUT PARTICULIER OU DE NON CONTREFAÇON SONT EXCLUES, EXCEPTÉ DANS LA MESURE OÙ DE TELLES EXCLUSIONS SERAIENT CONTRAIRES À LA LOI.

Contents

About This Guide

Welcome to iPlanet Directory Access Router (iDAR). This book provides an overview of design and planning decisions you need to make before installing the iDAR, and describes the different installation methods that you can use.

Prerequisite Reading

Before you install iDAR, we recommend that you read the *iPlanet Directory Server Deployment Guide*. The *Deployment Guide* covers key concepts on how to design and plan your directory service.

After you finish planning your directory service, follow the steps in this installation guide to install the iPlanet Directory Access Router and its related software components.

You may also want to review the *iDAR Administrator's Guide*.

Conventions Used In This Guide

This section explains the conventions used in this book.

`Monospaced font`—This typeface is used for any text that appears on the computer screen or text that you should type. It is also used for filenames, functions, and examples.

NOTE	Notes and Cautions mark important information. Make sure you read the information before continuing with a task.

The greater than symbol (>) is used as a separator for successive menu selections. For example, Object > New > User means that you should pull down the Object menu, drag the mouse down to highlight New, and drag the mouse across to the New submenu in which you must select User.

Throughout this book you will see path references of the form:

`/usr/iplanet/servers/idar-`*`serverID/`*`...`

The `/usr/iplanet/servers` directory is the default installation directory. If you have installed iDAR in a different location, you should adapt the path accordingly. *serverID* represents the server identifier you gave the server when you installed it. For example, if you gave the server an identifier of **phonebook**, then the actual path would be:

`/usr/iplanet/servers/idar-phonebook/. . .`

All paths specified in this manual are in UNIX format. If you are using a Windows NT-based directory server, you should assume the NT equivalent file paths whenever UNIX file paths are shown in this guide.

Related Information

iPlanet Directory Access Router Administrator's Guide. Procedures for the day-to-day maintenance of your directory access router. Includes information on command-line configuration and the iDAR Console.

The document set for iPlanet Directory Server contains the following guides:

iPlanet Directory Server Installation Guide. Procedures for installing your Directory Server as well as procedures for migrating your Netscape Directory Server to iPlanet Directory Server.

iPlanet Directory Server Administrator's Guide. Procedures for the day-to-day maintenance of your directory service. Includes information on configuring server-side plug-ins.

iPlanet Directory Server Deployment Guide. Procedures for the day-to-day maintenance of your directory service. Includes information on configuring server-side plug-ins.

iPlanet Directory Server Configuration, Command, and File Reference. Information about using the command-line scripts shipped with Directory Server.

iPlanet Schema Reference. Information about all the schema used in the iPlanet suite of products.

Other useful iPlanet information can be found at the following Internet locations:

- iPlanet release notes and other documentation:
  http://docs.iplanet.com/docs/manuals/
- iPlanet product status:
  http://www.iplanet.com/support/technical_resources/
- iPlanet Professional Services information:
  http://www.iplanet.com/services/pro_serv/index.html
- iPlanet developer information:
  http://developer.iplanet.com/
- iPlanet learning solutions:
  http://www.iplanet.com/learning/index.html
- iPlanet product data sheets:
  http://www.iplanet.com/products/index.html
- iPlanet product technical support
  http://www.iplanet.com/support

Chapter 1

Preparing for Installation

Before you begin installing iPlanet Directory Access Router (iDAR), you should have installed an iPlanet 5.0 or higher configuration directory.

We also recommend that you have an understanding of the various iDAR components and the design and configuration decisions you need to make.

To help you prepare for your iDAR installation, you should be familiar with the concepts contained in the following sections:

- Installation Components (page 12)
- Configuration Decisions (page 12)
- Installation Process Overview (page 17)
- Installation Privileges (page 18)

The *iPlanet Directory Server Deployment Guide* contains basic directory concepts as well as guidelines to help you design and successfully deploy your directory service. Be sure you understand the concepts presented in this manual before proceeding with the installation process.

NOTE iDAR requires that an instance of iPlanet Directory Server 4.13 or later is already installed and accessible on the network.

Installation Components

iDAR contains the following software components:

- **iPlanet Console**—iPlanet Console provides the common user interface for all iPlanet directory-related server products. From it you can perform common server administration functions such as stopping and starting servers, installing new server instances, and managing user and group information. iPlanet Console can be installed as a standalone application on any machine. You can also install it on your network and use it to manage remote servers.

- **iPlanet Administration Server**—iPlanet Administration Server is a common front-end to all iPlanet servers. It receives communications from iPlanet Console and passes those communications on to the appropriate iPlanet server. Your site will have at least one Administration Server for each server root in which you have installed an iPlanet server.

- **iPlanet Directory Access Router (iDAR)**—An LDAP gateway that routes requests from the client to Directory Server. iDAR runs as a daemon process (UNIX system) or service (Windows NT system).

Configuration Decisions

During iDAR installation, you are prompted for basic configuration information. Decide how you are going to configure these basic parameters before you begin the installation process. You are prompted for some or all of following information, depending on the type of installation that you decide to perform:

- Port number (see “Choosing Unique Port Numbers,” on page 13).

- Server root (see “Creating a New Server Root,” on page 13).

- Users and groups to run the server as (see “Deciding the User and Group for Your iDAR (UNIX Only),” on page 14).

- Configuration administrator and password (see “Defining Authentication Entities,” on page 15).

- The location of the configuration and user iDARs (see “Determining the Location of the Configuration Directory,” on page 15).

- The administration domain (see “Determining the Administration Domain,” on page 16).

Choosing Unique Port Numbers

Port numbers can be any number from 1 to 65535. Keep the following in mind when choosing a port number for your iDAR:

- The standard iDAR (LDAP) port number is 389.
- Port 636 is reserved for LDAP over SSL. Therefore, do not use port number 636 for your standard LDAP installation, even if 636 is not already in use. You can also use LDAP over TLS on the standard LDAP port.
- Port numbers between 1 and 1024 have been assigned to various services by the Internet Assigned Numbers Authority. Do not use port numbers below 1024 other than 389 or 636 for directory services as they will conflict with other services.
- On UNIX platforms, iDAR must be run as root if it will listen on either port 389 or 636.
- On Windows NT, the directory service must have administrative privileges if it will use ports 389 or 636.
- Make sure the ports you choose are not already in use. Additionally, if you are using both LDAP and LDAPS communications, make sure the port numbers chosen for these two types of access are not identical.

For information on how to set up LDAP over SSL (LDAPS) for iDAR, check the *iDAR Administrator's Guide*.

Creating a New Server Root

Your server root is the directory where you install your iPlanet servers. The server root must meet the following requirements:

- The server root must be a directory on a local disk drive; you cannot use a networked drive for installation purposes. The file sharing protocols such as AFS, NFS, and SMB do not provide suitable performance for use by iDAR's logging.
- The server root directory must not be the same as the directory from which you are running the `setup` program.

By default, the server root directory is one of the following:

- `/usr/iplanet/servers` (on UNIX systems)
- `c:\iplanet\servers` (on Windows NT systems)

Deciding the User and Group for Your iDAR (UNIX Only)

For security reasons, it is always best to run UNIX-based production servers with normal user privileges. That is, you do not want to run iDAR with root privileges. However, you will have to run iDAR with root privileges if you are using the default directory ports. If iDAR is to be started by Administration Server, Administration Server must run either as root or as the same user as iDAR.

You must therefore decide what user accounts you will use for the following purposes:

- The user and group under which you will run iDAR.

  If you will not be running iDAR as root, it is strongly recommended that you create a user account for all iPlanet servers. You should not use any existing operating system account, and should not use the nobody account. Also you should create a common group for the iDAR files; again, you should not use the nobody group.

- The user and group under which you will run Administration Server.

  For installations that use the default port numbers, this must be root. However, if you use ports over 1024, then you should create a user account for all iPlanet servers, and run Administration Server as this account.

  As a security precaution, when Administration Server is being run as root, it should be shut down when it is not in use.

You should use a common group for all iPlanet servers to ensure that files can be shared between servers when necessary.

Before you can install iDAR and Administration Server, you must make sure that the user and group accounts you will use exist on your system.

Defining Authentication Entities

As you install iDAR and Administration Server, you will be asked for user names and passwords. This list of login and bind entities will differ depending on the type of installation that you are performing:

- Configuration Directory Administrator ID and password.

  The configuration directory administrator is the person responsible for managing all the iPlanet servers accessible through iPlanet Console. If you log in with this user ID, then you can administer any iPlanet server that you can see in the server topology area of iPlanet Console.

  For security, the configuration directory administrator should not be the same as the directory manager. The default configuration directory administrator ID is `admin`.

Determining the Location of the Configuration Directory

Many iPlanet servers, including iDAR, use an instance of iPlanet Directory Server to store configuration information. This information is stored in the `o=NetscapeRoot` directory tree. Your *configuration directory* is the Directory Server that contains the `o=NetscapeRoot` tree used by your iPlanet servers.

For ease of upgrades, you should use a Directory Server instance that is dedicated to supporting the `o=NetscapeRoot` tree; this instance should perform no other function with regard to managing your enterprise's directory data.

Because the configuration directory normally experiences very little traffic, you can allow its server instance to coexist on a machine with an iDAR instance. However, for very large sites that are installing a large number of iPlanet servers, you may want to dedicate a low-end machine to the configuration directory so as to not hurt the performance of your other production servers.

Also, as with any directory installation, consider replicating the configuration directory to increase availability and reliability. See the *iPlanet Directory Server Deployment Guide* for information on using replication and DNS round robins to increase directory availability.

CAUTION Corrupting the configuration directory tree can result in the necessity of reinstalling all other iPlanet servers that are registered in that configuration directory. Remember the following guidelines when dealing with the configuration directory:

Always back up your configuration directory after you install a new iPlanet server.

Never change the host name or port number used by the configuration directory.

Never directly modify the configuration directory tree. Only the setup program for the various iPlanet servers should ever modify the configuration.

Determining the Administration Domain

The administration domain allows you to logically group iPlanet servers together so that you can more easily distribute server administrative tasks. A common scenario is for two divisions in a company to each want control of their individual iPlanet servers. However, you may still want some centralized control of all the servers in your enterprise. Administration domains allow you to meet these conflicting goals.

Administration domains have the following qualities:

- All servers share the same configuration directory, regardless of the domain to which they belong.
- Servers in two different domains may use two different user directories for authentication and user management.
- The configuration directory administrator has complete access to all installed iPlanet servers, regardless of the domain to which they belong.
- Each administration domain can be configured with an administration domain owner. This owner has complete access to all the servers in the domain but does not have access to the servers in any other administration domain.
- The administration domain owner can grant individual users administrative access on a server by server basis within the domain.

For many installations, you can have just one administration domain. In this case, choose a name that is representative of your organization. For other installations, you may want different domains because of the demands at your site. In the latter case, try to name your administration domains after the organizations that will control the servers in that domain.

For example, if you are an ISP and you have three customers for whom you are installing and managing iPlanet servers, create three administration domains each named after a different customer.

Installation Process Overview

You can use one of several installation processes to install iDAR. Each one guides you through the installation process and ensures that you install the various components in the correct order.

The following sections outline the installation processes available, how to upgrade from an earlier release of iDAR, and how to unpack the software to prepare for installation.

Selecting an Installation Process

You can install iDAR software using one of the three installation methods provided in the `setup` program:

- **Typical Installation**. Use this if you are performing a normal install of iDAR. Typical installation is described in Chapter 3, “Using Typical Installation.”
- **Custom Installation.** In iDAR 5.0, the custom installation process is very similar to the typical installation process. The only difference is that the custom installation process allows finer control over Administration Server configuration and the ability to supress the installation of iDAR’s services on Windows NT installations.
- **Silent Installation**. Use this if you want to script your installation process. This is especially useful for installing multiple consumer servers around your enterprise. Silent install is described in Chapter 4, “Silent Installation.”

Unpacking the Software

If you have obtained iDAR software from the iPlanet web site, you will need to unpack it before beginning installation.

1. Create a new directory for the installation:

   ```
   # mkdir idar5
   ```

   ```
   # cd idar5
   ```

2. Download the product binaries file to the installation directory.

3. On a UNIX system, unpack the product binaries file using the following command:

   ```
   # gzip -dc file_name.tar.gz | tar -xvof -
   ```

   where *file_name* corresponds to the product binaries that you want to unpack.

   On a Windows NT system, unzip the product binaries.

Installation Privileges

On UNIX systems, you must install as root if you choose to run the server on a port below 1024, such as the default LDAP ports: 389, and 636 (LDAP over SSL). If you choose port numbers higher than 1024, you can install using any valid UNIX login.

On Windows NT systems, you must run the installation as administrator.

Chapter 2

Computer System Requirements

Before you can install iPlanet Directory Access Router (iDAR), you must make sure that the systems on which you plan to install the software meet the minimum hardware and operating system requirements.

These requirements are described in detail for each platform in the following sections:

- Supported Platforms (page 19)
- Operating System Requirements (page 20)
- Hardware Requirements (page 20)

Supported Platforms

iDAR is supported on the following platforms:

- Sun Solaris 2.6 for SPARC operating environment
- Sun Solaris 8 for SPARC (32 bit) operating environment
- Microsoft Windows NT 4.0 Server with Service Pack 6a (x86 only)

NOTE For each platform, check the required patches and kernel parameter settings, as described in the sections that follow.

Hardware Requirements

On all platforms, you will need:

- Roughly 300 MB of disk space for a minimal installation.
- 256 MB of RAM.

Operating System Requirements

This section covers the required operating system version, patches, and utilities for each platform.

- Solaris 2.6 and Solaris 8 Operating Systems
- Windows NT 4.0 Server

Solaris 2.6 and Solaris 8 Operating Systems

If you plan to run iDAR on a Solaris operating system, you must ensure that the recommended patch cluster is installed. Solaris patches are identified by two numbers, for example, 106125-10. The first number (106125) identifies the patch itself. The second number identifies the version of the patch, in the example above the patch is version number 10. We recommend installing the latest version of the patch in order to benefit from the latest fixes.

For advice on guarding against potential security threats, see the *Solaris Operating Environment Security Sun Blueprint* at this site:
`http://www.sun.com/blueprints/0100/security.pdf`

Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

current working directory: 200 MB

Required System Modules

iDAR is optimized for systems with the UltraSPARC chipsets.

Use of Solaris 2.6 or 8 with the Sun recommended patches is required.

The Sun patches listed in Table 2-1 or Table 2-2 should be installed on your system before installing this iPlanet product. The command "`showrev -p`" will list the patches which have been installed. If you need to get a patch, see the web page `sunsolve.sun.com` or FTP to `ftp://sunsolve.sun.com/pub/patches`.

You will need to reboot your machine after installing these patches.

In addition to the patches listed here, you may want to install the latest patch cluster for your version of Solaris, which includes additional recommended and security patches. The Sun recommended patch clusters can be obtained from your Solaris support representative, or from `http://sunsolve.sun.com`.

Table 2-1 List of Patches for Solaris 2.6

105181-28:	SunOS 5.6: Kernel update patch
105210-38:	SunOS 5.6: libaio, libc & watchmalloc patch
105216-04:	SunOS 5.6: /usr/sbin/rpcbind patch
105284-41:	Motif 1.2.7: Runtime library patch
105338-27:	CDE 1.2: dtmail patch
105356-18:	SunOS 5.6: /kernel/drv/ssd and /kernel/drv/sd patch
105357-04:	SunOS 5.6: /kernel/drv/ses patch
105375-26:	SunOS 5.6: sf & socal driver patch
105379-06:	SunOS 5.6: /kernel/misc/nfssrv patch
105395-06:	SunOS 5.6: /usr/lib/sendmail patch
105401-34:	SunOS 5.6: libnsl and NIS+ commands patch
105403-04:	SunOS 5.6: ypbind/ypserv patch
105407-01:	SunOS 5.6: /usr/bin/volrmmount patch
105464-02:	OpenWindows 3.6: Multiple xterm fixes
105472-08:	SunOS 5.6: /usr/lib/autofs/automountd patch
105486-04:	SunOS 5.6: /kernel/fs/hsfs patch
105529-11:	SunOS 5.6: /kernel/drv/tcp patch
105552-03:	SunOS 5.6: /usr/sbin/rpc.nisd_resolv patch
105558-04:	CDE 1.2: dtpad patch
105562-03:	SunOS 5.6: chkey and keylogin patch
105566-11:	CDE 1.2: calendar manager patch

Table 2-1 List of Patches for Solaris 2.6 *(Continued)*

105568-23:	SunOS 5.6: /usr/lib/libthread.so.1 patch
105580-18:	SunOS 5.6: /kernel/drv/glm patch
105591-09:	SunOS 5.6: Shared library patch for C++
105615-08:	SunOS 5.6: /usr/lib/nfs/mountd patch
105633-57:	OpenWindows 3.6: Xsun patch
105642-08:	SunOS 5.6: prtdiag patch
105665-03:	SunOS 5.6: /usr/bin/login patch
105667-03:	SunOS 5.6: /usr/bin/rdist patch
105669-10:	CDE 1.2: libDtSvc Patch
105703-27:	CDE 1.2: dtlogin patch
105720-14:	SunOS 5.6: /kernel/fs/nfs patch
105722-07:	SunOS 5.6: /usr/lib/fs/ufs/ufsdump and ufsrestore patch
105741-09:	SunOS 5.6: /kernel/drv/ecpp patch
105755-10:	SunOS 5.6: libresolv, in.named, named-xfer, nslookup, nstest patch
105780-05:	SunOS 5.6: /kernel/fs/fifofs patch
105786-14:	SunOS 5.6: /kernel/drv/ip driver patch
105792-06:	SunOS 5.6: /usr/sbin/tar patch
105800-07:	SunOS 5.6: /usr/bin/admintool, y2000 patch
105802-15:	OpenWindows 3.6: ToolTalk patch
105837-03:	CDE 1.2: dtappgather Patch, including SDE 1.0 installations
105847-09:	SunOS 5.6: /kernel/drv/st.conf and /kernel/drv/st patch
106027-09:	CDE 1.2 / SDE 1.0: dtsession patch
106040-16:	SunOS 5.6: X Input & Output Method patch
106049-02:	SunOS 5.6: /usr/sbin/in.telnetd patch
106112-06:	CDE 1.2: dtfile patch
106123-05:	SunOS 5.6: sgml patch
106125-11:	SunOS 5.6: Patch for patchadd and patchrm
106193-06:	SunOS 5.6: Patch for Taiwan timezone
106222-01:	OpenWindows 3.6: filemgr (ff.core) fixes
106226-01:	SunOS 5.6: /usr/sbin/format patch

Table 2-1 List of Patches for Solaris 2.6 *(Continued)*

106235-08:	SunOS 5.6: lp patch
106242-02:	CDE 1.2: libDtHelp.so.1 fixes
106257-05:	SunOS 5.6: /usr/lib/libpam.so.1 patch
106271-06:	SunOS 5.6: /usr/lib/security/pam_unix.so.1 patch
106285-03:	SunOS 5.6: /kernel/sys/msgsys patch
106292-11:	SunOS 5.6: pkgadd/pkginstall & related utilities
106301-03:	SunOS 5.6: /usr/sbin/in.ftpd patch
106361-11:	SunOS 5.6: csh/jsh/ksh/rksh/rsh/sh patch
106409-01:	SunOS 5.6: Fixes the Traditional Chinese TrueType fonts
106415-04:	OpenWindows 3.6: xdm patch
106429-02:	SunOS 5.6: /kernel/drv/mm patch
106437-03:	CDE 1.2: Print Manager Patch
106439-07:	SunOS 5.6: /usr/sbin/syslogd patch
106448-01:	SunOS 5.6: /usr/sbin/ping patch
106468-04:	SunOS 5.6: /usr/bin/cu and usr/bin/uustat patch
106495-01:	SunOS 5.6: truss & truss support library patch
106522-04:	SunOS 5.6: /usr/bin/ftp patch
106569-01:	SunOS 5.6: libauth.a & libauth.so.1 patch
106592-03:	SunOS 5.6: /usr/lib/nfs/statd patch
106625-11:	SunOS 5.6: libsec.a, libsec.so.1 and /kernel/fs/ufs patch
106639-05:	SunOS 5.6: /kernel/strmod/rpcmod patch
106648-01:	OpenWindows 3.6: libce suid/sgid security fix
106649-01:	OpenWindows 3.6: libdeskset patch
106650-04:	OpenWindows 3.6: mailtool attachment security patch
106828-01:	SunOS 5.6: /usr/bin/date patch
106834-02:	SunOS 5.6: cp/ln/mv patch
106882-02:	SunOS 5.6: /usr/lib/nfs/nfsd patch
107336-01:	OpenWindows 3.6: KCMS configure tool has a security vulnerability
107434-01:	CDE 1.2: Spell checking occasionally kills mail
107490-01:	SunOS 5.6: savecore doesn't work if swap slice is over 2G

Table 2-1 List of Patches for Solaris 2.6 *(Continued)*

107565-02:	SunOS 5.6: /usr/sbin/in.tftpd patch
107618-02:	SunOS 5.6: patch /usr/sbin/vold
107733-09:	SunOS 5.6: Linker patch
107758-01:	SunOS 5.6: Pax incorrectly change mode of symlink target file
107766-01:	SunOS 5.6: ASET cklist reports unchanged 6month older files as new
107774-01:	SunOS 5.6: inetd denial-of-service attack
107991-02:	SunOS 5.6: /usr/sbin/static/rcp patch
108091-03:	SunOS 5.6: ssJDK1.2.1_03 fails with fatal error in ISO8859-01 Locales
108199-01:	CDE 1.2: dtspcd Patch
108201-01:	CDE 1.2: dtaction Patch
108307-02:	SunOS 5.6: keyserv fixes
108333-02:	SunOS 5.6: jserver buffer overflow
108346-03:	SunOS 5.6: patch usr/sbin/rpc.nispasswdd
108468-02:	SunOS 5.6: ldterm streams module fixes
108492-01:	SunOS 5.6: Snoop may be exploited to gain root access
108499-01:	SunOS 5.6: ASET sets the gid on /tmp, /var/tmp when setting med high
108660-01:	SunOS 5.6: Patch for sadmind
108804-02:	SunOS 5.6: /usr/bin/tip patch
108890-01:	SunOS 5.6: patch /usr/lib/netsvc/yp/ypxfrd
108893-01:	SunOS 5.6: patch /usr/lib/netsvc/yp/rpc.ypupdated
108895-01:	SunOS 5.6: patch /usr/sbin/rpc.bootparamd
109266-01:	SunOS 5.6: security: /bin/mail has buffer overflow
109339-02:	SunOS 5.6: nscd's size grows -0TTL values not implemented
109388-01:	SunOS 5.6: patch /usr/vmsys/bin/chkperm
109719-01:	SunOS 5.6: arp should lose set-gid bid
110990-01:	SunOS 5.6: Patch for ttymon
111029-01:	SunOS 5.6: /kernel/sys/semsys patch
111109-01:	SunOS 5.6: Patch to /usr/bin/nawk
111240-01:	SunOS 5.6: Patch to /usr/bin/finger
111560-01:	SunOS 5.6: dmesg security problem

Table 2-1 List of Patches for Solaris 2.6 *(Continued)*

111664-01:	SunOS 5.6: bzip patch

Patches 106409-01 and 108091-03 are not included in the Sun Recommended Patch cluster but can be obtained from the J2SE 1.2.2 Localized JRE patch set.

Table 2-2 List of Patches for Solaris 8

108528-09:	SunOS 5.8: kernel update patch
108652-35:	X11 6.4.1 Xsun patch
108725-05:	SunOS 5.8: st driver patch
108827-10:	SunOS 5.8: libthread patch
108869-06:	SunOS 5.8: snmpdx/mibiisa/libssasnmp/snmplib patch
108875-09:	SunOS 5.8: c2audit patch
108968-05:	SunOS 5.8: vol/vold/rmmount patch
108974-11:	SunOS 5.8: dada, uata, dad, sd and scsi drivers patch
108975-04:	SunOS 5.8: /usr/bin/rmformat and /usr/sbin/format patch
108977-01:	SunOS 5.8: libsmedia patch
108985-03:	SunOS 5.8: /usr/sbin/in.rshd patch
108987-04:	SunOS 5.8: Patch for patchadd and patchrm
108989-02:	SunOS 5.8: /usr/kernel/sys/acctctl and /usr/kernel/sys/exacctsys patch
108991-13:	SunOS 5.8: /usr/lib/libc.so.1 patch
108993-03:	SunOS 5.8: nss and ldap patch
109091-04:	SunOS 5.8: /usr/lib/fs/ufs/ufsrestore patch
109137-01:	SunOS 5.8: /usr/sadm/install/bin/pkginstall patch
109181-03:	SunOS 5.8: /kernel/fs/cachefs patch
109277-01:	SunOS 5.8: /usr/bin/iostat patch
109279-13:	SunOS 5.8: /kernel/drv/ip patch
109318-12:	SunOS 5.8: suninstall patch
109320-03:	SunOS 5.8: LP patch
109322-07:	SunOS 5.8: libnsl patch
109324-02:	SunOS 5.8: sh/jsh/rsh/pfsh patch

Table 2-2 List of Patches for Solaris 8 *(Continued)*

109326-05:	SunOS 5.8: libresolv.so.2, in.named patch
109470-02:	CDE 1.4: Actions Patch
109587-03:	SunOS 5.8: libspmistore patch
109742-04:	SunOS 5.8: /kernel/drv/icmp patch
109783-01:	SunOS 5.8: /usr/lib/nfs/nfsd patch
109805-03:	SunOS 5.8: pam_krb5.so.1 patch
109898-02:	SunOS 5.8: /kernel/drv/arp patch
109951-01:	SunOS 5.8: jserver buffer overflow
110075-01:	SunOS 5.8: /kernel/drv/devinfo and /kernel/drv/sparcv9/devinfo patch
110283-03:	SunOS 5.8: mkfs and newfs patch
110286-02:	OpenWindows 3.6.2: Tooltalk patch
110322-01:	SunOS 5.8: /usr/lib/netsvc/yp/ypbind patch
110383-01:	SunOS 5.8: libnvpair patch
110387-03:	SunOS 5.8: ufssnapshots support, ufsdump patch
110453-01:	SunOS 5.8: admintool patch
110458-02:	SunOS 5.8: libcurses patch
110662-02:	SunOS 5.8: ksh patch
110700-01:	SunOS 5.8: automount patch
110898-02:	SunOS 5.8: csh/pfcsh patch
110901-01:	SunOS 5.8: /kernel/drv/sgen and /kernel/drv/sparcv9/sgen patch
110934-01:	SunOS 5.8: pkgtrans, pkgadd, pkgchk and libpkg.a patch
110939-01:	SunOS 5.8: /usr/lib/acct/closewtmp patch
110943-01:	SunOS 5.8: /usr/bin/tcsh patch
110945-01:	SunOS 5.8: /usr/sbin/syslogd patch
110951-01:	SunOS 5.8: /usr/sbin/tar and /usr/sbin/static/tar patch
111071-01:	SunOS 5.8: cu patch
111111-01:	SunOS 5.8: nawk line length limit corrupts patch dependency checking
111232-01:	SunOS 5.8: patch in.fingerd
111234-01:	SunOS 5.8: patch finger
111293-03:	SunOS 5.8: /usr/lib/libdevinfo.so.1 patch

Table 2-2 List of Patches for Solaris 8 *(Continued)*

111325-01:	SunOS 5.8: /usr/lib/saf/ttymon patch
111327-02:	SunOS 5.8: libsocket patch
111363-01:	SunOS 5.8: /usr/sbin/installf patch
111548-01:	SunOS 5.8: catman, man, whatis, apropos and makewhatis patch
111570-01:	SunOS 5.8: uucp patch

This release of iPlanet Directory Server is not supported on Solaris 2.5.1 or earlier, Solaris 7, or any version of Solaris x86.

This release of iPlanet Directory Server may be used on a 64 bit Solaris 8 environment, but will run as a 32 bit process, and is limited to 3.7 GB of process memory.

Verify System Tuning

Deployment of a service based on iPlanet directory products will require system tuning to achieve optimal performance. Basic Solaris tuning guidelines are available from several books, including *Sun Performance and Tuning: Java and the Internet* (ISBN 0-13-095249-4). Advanced tuning information is available in the *Solaris Tunable Parameters Reference Manual* (806-4015) which can be obtained from this site: `http://docs.sun.com/ab2/coll.707.1/`

The program `idsktune`, which is available in your installation at `<server-root>/shared/bin/idsktune`, analyzes the Solaris kernel tuning parameters and reports any changes that should be made to improve performance. This program does not modify the system.

File Descriptors

The system-wide maximum file descriptor table size setting will limit the number of concurrent connections that can be established to iDAR. The governing parameter, `rlim_fd_max`, is set in the `/etc/system` file. By default if this parameter is not present the maximum is 1024. It can be raised to 4096 by adding to `/etc/system` a line

```
set rlim_fd_max=4096
```

and rebooting the system. This parameter should not be raised above 4096 without first consulting your Sun Solaris support representative as it may affect the stability of the system.

TCP Tuning

The TCP/IP implementation in a Solaris kernel is by default not correctly tuned for Internet or Intranet services. The following /dev/tcp tuning parameters should be inspected, and if necessary changed to fit the network topology of the installation environment.

The tcp_time_wait_interval in Solaris 8 and tcp_close_wait_interval in Solaris 2.6 specify the number of milliseconds that a TCP connection will be held in the kernel's table after it has been closed. If its value is above 30000 (30 seconds) and the directory is being used in a LAN, MAN or under a single network administration, it should be reduced by adding a line similar to the following to the /etc/init.d/inetinit file:

```
ndd -set /dev/tcp tcp_close_wait_interval 30000
```

The tcp_conn_req_max_q0 and tcp_conn_req_max_q parameters control the maximum backlog of connections that the kernel will accept on behalf of the iDAR process. If the directory is expected to be used by a large number of client hosts simultaneously, these values should be raised to at least 1024 by adding a line similar to the following to the /etc/init.d/inetinit file:

```
ndd -set /dev/tcp tcp_conn_req_max_q0 1024
ndd -set /dev/tcp tcp_conn_req_max_q 1024
```

The tcp_keepalive_interval specifies the interval in seconds between keepalive packets sent by Solaris for each open TCP connection. This can be used to remove connections to clients that have become disconnected from the network. The ids-proxy-con-timeout attribute on the ids-proxy-sch-NetworkGroup objectclass, with a value in seconds, can also be used for this purpose, as it will time out idle connections. For more information, see Chapter 16, “Groups Configuration” in the *iDAR Administrator’s Guide*.

The tcp_rexmit_interval_initial value should be inspected when performing server performance testing on a LAN or high speed MAN or WAN. For operations on the wide area Internet, its value need not be changed.

The tcp_smallest_anon_port controls the number of simultaneous connections that can be made to the server. When rlim_fd_max has been increased to above 4096, this value should be decreased, by adding a line similar to the following to the /etc/init.d/inetinit file:

```
ndd -set /dev/tcp tcp_smallest_anon_port 8192
```

The tcp_slow_start_initial parameter should be inspected if clients will predominately be using the Windows TCP/IP stack.

The tcp_ip_abort_cinterval controls how long in milliseconds iDAR should wait for an LDAP server to respond when establishing a new connection. This value should normally be reduced by adding a line similar to the following to the /etc/init.d/inetinit file:

```
ndd -set /dev/tcp tcp_ip_abort_cinterval 10000
```

In some environments, it may also be necessary to change the tcp_ip_abort_interval and tcp_strong_iss tuning parameters.

Windows NT 4.0 Server

This section describes how to prepare your system for installation of iDAR on Windows NT.

Configuring a Machine to Run iPlanet Directory Access Router

iDAR should be installed on a computer that is isolated from the Internet by a network-level firewall. This is necessary to protect the NT operating system from IP-based attacks.

No other network functions should be provided by this computer. The computer should not be dual-booting or running other operating systems. At a minimum, the computer system should have at least 256 MB of RAM, 300 MB of disk, a Pentium II or later processor, and a 100Mbps ethernet connection.

Disk Space Requirements

Ensure that you have sufficient disk space before downloading the software.

Download drive: 100 MB
Installation drive: 200 MB

Required System Modules

Windows NT Server Service Pack 6a is required. iDAR is not supported on Windows NT 3.5.1 or earlier releases, or Windows NT for the Alpha architecture. Neither is it supported on Windows NT Workstation, because this form of the operating system is not suitable for scalable Internet or Intranet server deployments. Windows NT Workstation is limited in its allowable setting for connection backlog. Windows NT Server allows a connection backlog setting of more than 10, which is necessary for TCP/IP servers under heavy load.

Installing Windows NT Server

During the installation of Windows NT, please observe the following:

- If there is already an operating system present on the computer, choose to perform a fresh install rather than an upgrade.
- Format the drives with NTFS rather than FAT, as NTFS allows access controls to be set on files and directories.
- Specify that the computer will be a stand-alone server and will not be a member of any existing domain or workgroup. This will reduce dependencies on the network security services.
- Choose an administrator password of at least 9 characters. Use punctuation or other non-alphabetic characters in the first 7 characters.
- Do not install Internet Information Server.
- Specify only TCP/IP as network protocol, and do not install any other network services.

Installing Third-Party Utilities

You need an UNZIP utility to unpack the iDAR software. There are many commercially licensed, free and shareware tools available, such as PKZIP or Winzip. Note that shareware unregistered versions of PKZIP 2.70 maintain a TCP/IP connection to an Internet advertising service, and so may not be suitable for installation on this system.

You need to install Adobe Acrobat Reader to read the documentation. It can be downloaded from `ftp://ftp.adobe.com/pub/adobe/acrobatreader/win/4.x`.

Install Windows Service Packs and Hotfixes

Windows NT Service Packs include key fixes that are necessary to maintain the security and reliability of the operating system. The hotfix series contains important changes for problems that were found after the service pack was released. Windows NT Server Service Pack 6a is required.

Install Windows NT 4.0 Service Pack 6a or Later

It can be obtained from `http://www.microsoft.com/windows/servicepacks/`. The system will reboot after the service pack is installed.

Install Hotfixes

Download and install any Windows NT 4.0 Hotfixes that are for the service pack that is installed on the system, such as `post-sp6a` for Service Pack 6a. They can be obtained from `ftp://ftp.microsoft.com/bussys/winnt/winnt-public/fixes/usa/nt40/`. It will probably be necessary to reboot the system after each hotfix is installed.

Installing Microsoft Utilities

The following additional utilities are recommended to improve the security of the Windows NT Operating System. They are not required for the operation of the iDAR.

If you have the Resource Kit CD-ROM produced by Microsoft Press, then copy the utility ‘`passprop.exe`’ from the Windows NT Server Resource Kit onto the system. The utility is located on the CD in the `i386\netadmin` directory. You will need this later to enable Administrator account lockout.

You will need to install Microsoft Internet Explorer 5 or later, as this is needed by the Security Configuration Manager.

The Microsoft Security Configuration Manager is located on the Service Pack 4 CD-ROM, or can be downloaded from `ftp://ftp.microsoft.com/bussys/winnt/winnt-public/tools/scm/`. This tool is described in Microsoft Knowledge Base article Q195227.

Ensure That the System Clock is Correct and Kept Accurate

So that date and time stamps in log files can be correlated with those of other computer systems, the system clock should be kept reasonably in sync. As the NET TIME command requires NetBIOS, which will be disabled during post-installation system configuration, either a TCP/IP based NTP client should be installed (such as the shareware program Tardis), or a time radio receiver attached. See `http://www.ntp.org/` for more information on NTP clients for Windows NT.

Install TCP ISN Patch

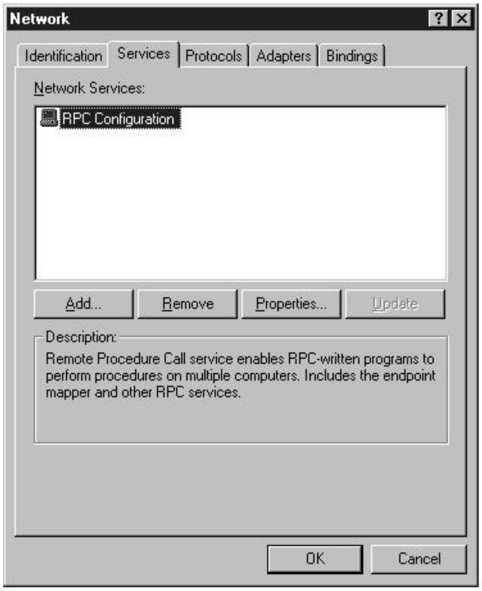
If you will be authenticating users to the directory, then TCP connection hijacking is a vulnerability. Microsoft has released a patch to improve the serial numbers, `q243835i.exe`. For more information please see `http://www.microsoft.com/security/bulletins/ms99-046.asp`

Additional Post-Installation System Configuration

The Windows environment will require tuning to provide optimum performance for iDAR in an operational environment. Consult the Windows system administrator’s documentation or support channel for information on NT tuning for multi-threaded internet services. The following sections provide some guidelines.

Restrict Network Services

Network file sharing is not required by iDAR and should be disabled. Go to the Control Panel and open the Network icon. Remove the Workstation, Computer Browser, NetBIOS Interface, Remote Access Service and Server Services from Network Services tab. Leave RPC Configuration.



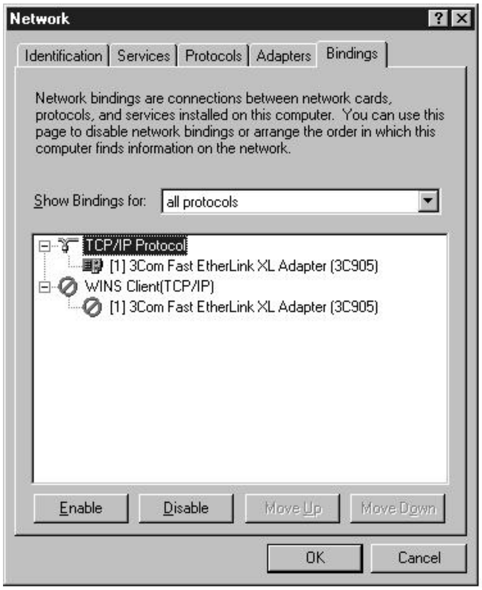
Network Services:
RPC Configuration

Description:
Remote Procedure Call service enables RPC-written programs to perform procedures on multiple computers. Includes the endpoint mapper and other RPC services.

From then on, each time the Network Control Panel is used, Windows NT will prompt to install Windows NT Networking. Always answer No to the prompt.

Remove NETBIOS

The iDAR uses only TCP/IP and does not require any Microsoft network services. On the Bindings tab of the Network window, select All Protocols. Disable the WINS Client. This unbinds NETBIOS from TCP/IP.



Network bindings are connections between network cards, protocols, and services installed on this computer. You can use this page to disable network bindings or arrange the order in which this computer finds information on the network.

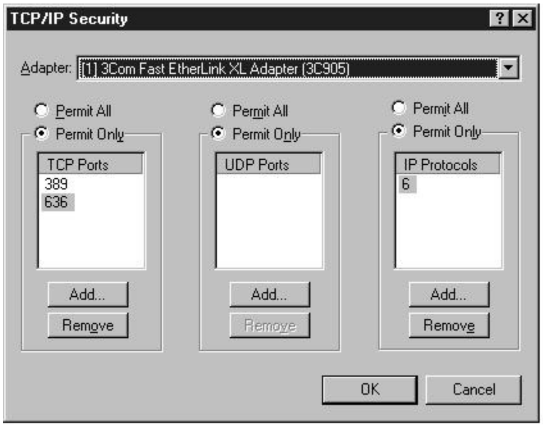
Show Bindings for: all protocols

- TCP/IP Protocol
  - [1] 3Com Fast EtherLink XL Adapter (3C905)
- WINS Client(TCP/IP)
  - [1] 3Com Fast EtherLink XL Adapter (3C905)

Enable Port Filtering

The RPC services are not removed, as it may be necessary for Microsoft software to make RPC connections on the loopback interface. However, the RPC ports must not be accessible to other systems.

Open the Network window; select the Protocols tab, then select TCP/IP and click Properties...; select Advanced and Enable Security. On the TCP/IP Filtering window, permit only TCP ports 389 and 636 and the administration port number, permit no UDP ports, and permit only IP protocol 6 (TCP). If you have multiple interfaces, it may be necessary to repeat this for each interface.



TCP/IP Security

Adapter: [1] 3Com Fast EtherLink XL Adapter (3C905)

○ Permit All
● Permit Only

TCP Ports
389
636

○ Permit All
● Permit Only

UDP Ports

○ Permit All
● Permit Only

IP Protocols
6

Note that after this change has been made, the Microsoft command-line FTP client will no longer operate. This is because the Microsoft client requires the FTP server to establish a connection in the reverse direction, and all non-LDAP ports are blocked.

Disable IP Routing

On the TCP/IP protocol window, disable IP Routing.

Disable WINS Client

On the Devices window of the Control Panel, disable the WINS Client.

Remove the OS/2 and POSIX Subsystem Keys From the Registry

iPlanet Directory Access Router does not require OS/2 and POSIX subsystems. Remove them by performing the following registry actions with regedit.

Delete all subkeys of:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OS/2 Subsystem for NT
```

There is another key under CurrentControlSet\Control named SessionManager, without a space in its name. Do not alter anything below that key.

Delete the value of Os2LibPath in this key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment
```

Change the value of the Optional item in the following key to the two bytes “`00 00`”:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
```

Delete the Posix and OS/2values from the following key:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems
```

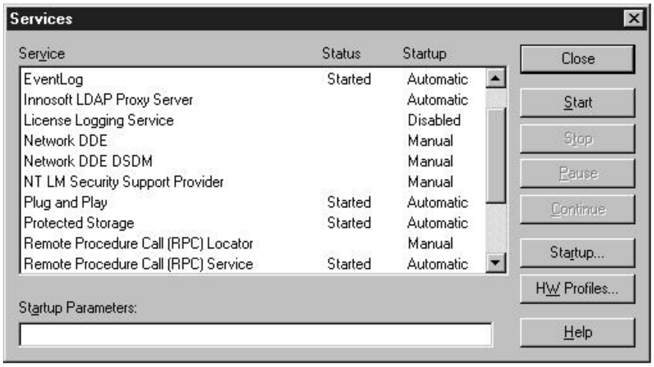
Remove the OS/2 DLLs

Delete all files in the `%SystemRoot%\system32\os2` directory and all subdirectories.

Stop Unneeded Services

Open the Control Panel, and the Services panel. Stop and disable any running services except for the following: EventLog, iPlanet Directory Server, iPlanet Administration Server, NT LM Security Support Provider, Plug and Play, Protected Storage, Remote Procedure Call (RPC) Service, and SNMP.

Services that are listed as Manual start do not need to be disabled.



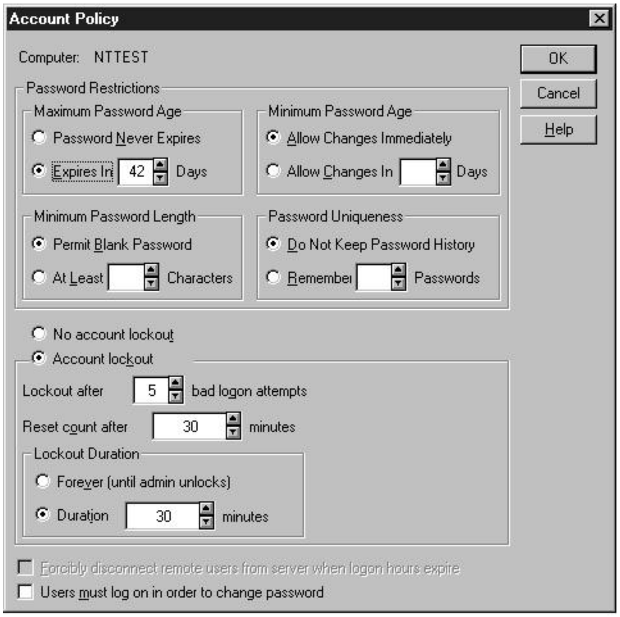
Service	Status	Startup
EventLog	Started	Automatic
Innosoft LDAP Proxy Server		Automatic
License Logging Service		Disabled
Network DDE		Manual
Network DDE DSDM		Manual
NT LM Security Support Provider		Manual
Plug and Play	Started	Automatic
Protected Storage	Started	Automatic
Remote Procedure Call (RPC) Locator		Manual
Remote Procedure Call (RPC) Service	Started	Automatic

Ensure System Will Automatically Reboot on Error

Open the Control Panel System panel. Under the Startup/Shutdown tab, set the show list time to `0` seconds, and select the Automatic reboot checkbox.

Configure User Accounts

Open the Administrative tools. (Start>Programs>Administrative Tools>User Manager.) Under Policies, choose Account... On the Account Policies window, allow accounts to be locked out.



Account Policy

Computer: NTTEST

Password Restrictions

Maximum Password Age
○ Password Never Expires
● Expires In 42 Days

Minimum Password Age
● Allow Changes Immediately
○ Allow Changes In Days

Minimum Password Length
● Permit Blank Password
○ At Least Characters

Password Uniqueness
● Do Not Keep Password History
○ Remember Passwords

○ No account lockout
● Account lockout

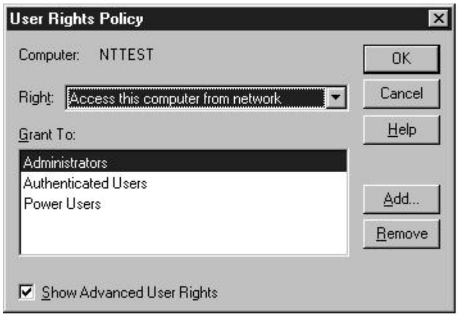
Lockout after 5 bad logon attempts

Reset count after 30 minutes

Lockout Duration
○ Forever (until admin unlocks)
● Duration 30 minutes

□ Forcibly disconnect remote users from server when logon hours expire
□ Users must log on in order to change password

Next, under Policies, choose User Rights... Select Access this computer from the network, remove Everyone and add Authenticated Users.



User Rights Policy

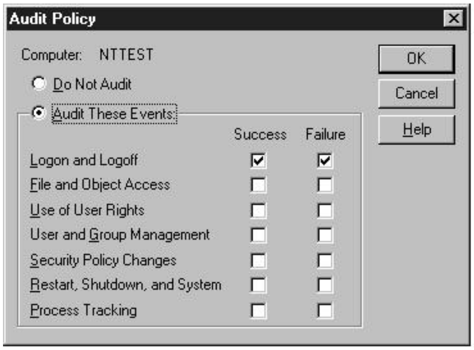
Computer: NTTEST

Right: Access this computer from network

Grant To:
Administrators
Authenticated Users
Power Users

☑ Show Advanced User Rights

Next, under Policies, choose Audit, select Audit These Events, and check the boxes for both Success and Failure for the Logon and Logoff Events.



Audit Policy

Computer: NTTEST

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	☑	☑
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

You may wish also to rename the administrator account to something else, making it harder to guess.

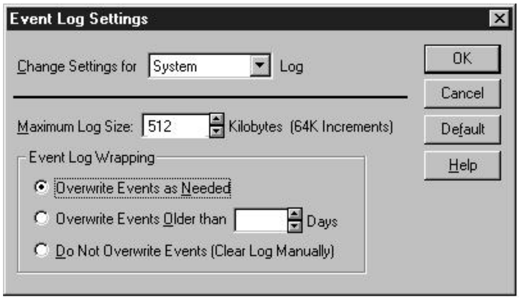
If you have copied the `passprop` utility from the NT Server Resource Kit, it can be used to allow lockout of the administrator's account by running it on the command line as `passprop/adminlockout`.

Encrypt Account Database

Protect the NT user account database, SAM, by running the syskey program. This encrypts the Administrator's password so that registry-extracting hacker tools cannot use it.

Event Log Configuration

Open the Event Viewer (Start>Programs>Administrative Tools>Event Viewer); set the log overwrite intervals (located under Log>Log Settings...) to a value appropriate to your deployment.



Event Log Settings

Change Settings for System Log

Maximum Log Size: 512 Kilobytes (64K Increments)

Event Log Wrapping

● Overwrite Events as Needed

○ Overwrite Events Older than Days

○ Do Not Overwrite Events (Clear Log Manually)

Set Tuning Parameters

The transmission control blocks (TCBs) store data for each TCP connection. A control block is attached to the TCB hash table for each active connection. If there are not enough control blocks available when an LDAP connection arrives at the server via TCP/IP, there is added delay while it waits for additional control blocks to be created. By increasing the TCB timewait table size, you reduce latency overhead by allowing more client connections to be serviced faster. To adjust this value, add to the following registry key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

the `MaxFreeTcbs` value of 0xFA0.

This example increases the TCB timewait table to 4,000 entries from the default of 2,000. Now that the overhead time introduced by TCP has been lowered for iPlanet Directory Access Router, adjust the corresponding hash table that stores the TCBs. Adjust the hash table by adding to the following registry value:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
```

the value of `MaxHashTableSize` to 0x400.

This increases the TCB hash table size from 512 to 1,024, allowing more room for connection information. TCB information is stored in the nonpaged memory pool. If iPlanet Directory Access Router is experiencing memory bottlenecks and more memory cannot be allotted to the server, lower the above values.

On a multiprocessor system, we recommend optimizing the NIC and CPU relationship. Each LDAP request received over the network generates an interrupt to the processor requesting service. If the processor does not consider the request to be sufficiently urgent, (i.e., with a sufficiently high interrupt level), it defers the request. This deferred interrupt request becomes a Deferred Procedure Call (DPC). As more and more requests come into the server, the number of interrupts and DPCs increases.

When an interrupt is sent to a particular CPU and is subsequently deferred, additional server overhead is incurred if this DPC is shipped off to another CPU in the server (if the server is an SMP capable machine). This is NTs default behavior and can be costly from a performance perspective. To stop this transfer from happening, add to the following registry value:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NDIS\Parameters
```

the value of `ProcessorAffinityMask` to 0.

This forces the CPU that handled the interrupt to also handle any associated DPCs. This also insures that the network interface card or cards are not to associated with a specific CPU. This improves the CPUs servicing of interrupts and DPCs generated by the network interface card(s).

Windows NT ships with a variety of transport drivers such as TCP/IP, NBF (NetBEUI), and NWLink. All of these transports export a TDI interface on top and an NDIS (Network Driver Interface Specification) on the bottom. (Windows NT also ships with AppleTalk and DLC, however, these do not have a TDI interface.) If the TCP/IP protocol is first in the bindings list, average connection setup time decreases.

Windows NT can implement the Van Jacobson TCP fast retransmit and recovery algorithm to quickly retransmit missing segments upon the receipt of n ACKS, without waiting for the retransmission timer to expire. To implement the Van Jacobson algorithm, edit:

```
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters
```

Add a value named `TcpMaxDupAcks`, with type `REG_DWORD`, and set the value to the number of ACKs. The range is 1-3, and the default is 2.

Chapter 3

Using Typical Installation

This chapter describes how to perform basic installation activities using the Typical Installation option. Please ignore the Express Installation option.

Using Typical Installation

Most initial installations of iDAR can be performed using the Typical Installation option of the setup program. Typical installation differs slightly depending on whether you are installing on UNIX or Windows NT. The following sections outline the different procedures.

Using Typical Installation on UNIX

To perform a typical installation on UNIX:

1. Log in as root.
2. Create a new directory:

   ```
   # mkdir idar5
   ```

   ```
   # cd idar5
   ```

3. If you have not already done so, download the product binaries file to the installation directory.
4. Unpack the product binaries file using the following command:

   ```
   # gunzip -dc file_name.tar.gz | tar -xvof -
   ```

   where *file_name* corresponds to the product binaries that you want to unpack.

5. Run the setup program. You can find it in the directory where you untarred binary files. Issue the following command from the installation directory:

   ```
   ./setup
   ```

6. The setup program asks if you would like to proceed with the setup. Press Enter to respond with the default (the default for this prompt is Yes) or press n if you would like to exit the setup program.

   If you want to log in as root or super user (su), you will need to exit the setup program.

7. Next, the setup program asks you if you agree to the license terms. Press "y" to agree with the license terms.

8. When you are asked what you would like to install, press Enter to select the default, iPlanet Servers (this is item 1).

9. When you are asked what type of installation you would like to perform, press Enter to select the default, Typical Installation.

10. For server root, enter a full path to the location where you want to install your server.

    The location that you enter must be some directory other than the directory from which you are running setup. If the directory that you specify does not exist, setup creates it for you.

    By default, the setup program provides the following path:

    ```
    /usr/iplanet/servers
    ```

    If you want to install the software into this directory tree, press Enter; otherwise, supply your own path.

11. For the Server Products Core Components, iDAR, and Administration Services, press Enter to select the default (all components).

12. Press Enter to select all of the Server Products Core Components.

13. Press Enter to select all of the Administration Services components (iPlanet Administration Server and the Administration Server Console).

14. Press Enter to select all the iDAR components.

15. For the hostname, enter a fully qualified hostname or select the default (which is the local host).

16. The `setup` program then asks you for the System User and the System Group names. Enter the identity under which you want the servers to run.

    For more information on the user and group names that you should use when running iPlanet servers, see “Deciding the User and Group for Your iDAR (UNIX Only),” on page 14.

17. For the configuration directory, select which directory will host your `o=NetscapeRoot` tree in the form: `ldap://host:port`.

    The configuration directory must exist before you can continue this installation.

18. For Administration Domain, enter the domain that you want this server to belong to.

    The name you enter should be a unique string that is descriptive of the organization responsible for administering the domain. For information on administration domains, see “Determining the Administration Domain,” on page 16.

19. For Configuration Directory Administrator ID and password, enter the name and password that you will log in as when you want to authenticate to the console with full privileges.

20. For the administration port number, enter a value that is not in use (for example, you might want to use the value 5000 to indicate a 5.0 iDAR). Be sure to record this value.

21. For the user you want to run Administration Server as, enter `root`. This is the default.

    For information on why you should run Administration Server as root, see “Deciding the User and Group for Your iDAR (UNIX Only),” on page 14.

22. For iDAR port number, enter a value that is not in use. The default is 389.

The server is then unpackaged, minimally configured, and started. You are told what host and port number Administration Server is listening on.

The server is configured to use the following suffixes:

- The suffix that you configured.
- `o=NetscapeRoot`

Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix, or create a new suffix to be used for this purpose. For details on how to create new suffixes for your iDAR, see the *iPlanet Directory Server Administrator's Guide.*

Using Typical Installation on Windows NT

To perform a typical installation on Windows NT:

1. Log in as a user with administrator privileges.
2. If you have not already done so, download the product binaries file to the installation directory.
3. Unzip the product binaries files and run the `setup` program.
4. When you are asked what you would like to install, select the default, iPlanet Servers.
5. When you are asked what type of installation you would like to perform, select the default, Typical.
6. For server installation root, enter a full path to the location where you want to install your server.

   The location that you enter must be some directory other than the directory from which you are running `setup`. If the directory that you specify does not exist, `setup` creates it for you.

7. For configuration directory, select the default if this directory will host your `o=NetscapeRoot` tree. Otherwise, enter the appropriate contact information for the configuration directory.

   If this iDAR instance is not the configuration directory, then the configuration directory must exist and be running before you can continue this installation.

8. For Administration Domain, enter the domain to which you want this server to belong.

   The name that you enter should be a unique string that is descriptive of the organization responsible for administering the domain. For information on administration domains, see "Deciding the User and Group for Your iDAR (UNIX Only)," on page 14.

9. For Configuration Directory Administrator ID and password, enter the name and password that you will log in as when you want to authenticate to the console with full privileges.

10. For administration port number, enter a value that is not in use. Be sure to record this value.

11. For the iDAR port, select the default (389) unless you already have another application using that port.

The server is then unpackaged, minimally configured, and started.

The server is configured to use the following suffixes:

- The suffix that you configured.
- `o=NetscapeRoot`

Do not modify the contents of the directory under the `o=NetscapeRoot` suffix. Either create data under the first suffix, or create a new suffix to be used for this purpose. For details on how to create new suffixes for your iDAR, see the *iPlanet Directory Server Administrator's Guide*.

Chapter 4

Silent Installation

Silent installation allows you to use a file to predefine all the answers that you would normally supply interactively to the setup program. This provides you with the ability to script the installation of your iPlanet Directory Access Routers (iDARs).

This chapter includes the following sections:

- Using Silent Installation (page 47)
- Preparing Silent Installation Files (page 48)
- Installation Directives (page 51)

Using Silent Installation

To use silent installation, you call the setup program with the `-s` and `-f` command line options. That is, to use silent installation:

1. On UNIX machines, log in as `root`. On Windows NT machines, log in with Administrator privileges.
2. Create a new directory:

   ```
   # mkdir idar5
   ```

   ```
   # cd idar5
   ```

3. If you have not already done so, download the product binaries file to the installation directory.
4. On UNIX, unpack the product binaries file using the following command:

   ```
   # gunzip -dc file_name.tar.gz | tar -xvof-
   ```

   where *file_name* corresponds to the product binaries that you want to unpack.

5. On Windows NT, unzip the product binaries.

6. Prepare the file that will contain your installation directives.

7. Run the setup program with the `-s` and `-f` command line options:

   `setup -s -f` *file_name*

   where *file_name* is the name of the file that contains your installation directives.

The next section in this chapter provides some examples of the silent install files. A section describing all of the silent installation directives that you can use when installing iDAR then follows.

Preparing Silent Installation Files

Silent installation is intended for use at sites where many server instances must be created.

This section first describes how to create silent installation files. It then provides examples of using silent installation to support the following common installation scenarios:

- A Typical Installation
- Using an Existing Configuration Directory
- Installing the Stand-Alone iPlanet Console

You find a definition of the individual installation directives in “Installation Directives,” on page 51.

NOTE Any Distinguished Names in the files must be in the UTF-8 character set encoding.

Creating Silent Installation Files

The best way to create a file for use with silent installation is to use the setup program to interactively create a server instance of the type that you want to duplicate around your enterprise.

To do this run `setup` with the `-k` flag. The `setup` program will create the following file: `<ServerRoot>/setup/install.inf`

This file contains all the directives that you would use with silent installation to create the server instance. You can then use this file to create other server instances of that type.

You will have to make some modifications to this file before you use it on other machines. Specifically, ensure that you:

- Set the `FullMachineName` directive to a value that is appropriate for the machine on which iDAR will be installed, if it's not to be the local machine. In most circumstances, it is best not to use this directive because `FullMachineName` will then default to the local host name. However, if you use custom installation to generate your initial server instance, then this directive will appear in the `install.inf` file.

- Set the `ServerIPAddress` directive appropriate for the local machine. The same usage rules apply for `ServerIPAddress` as for `FullMachineName`. Specifically, try to not include ServerIPAddress in your `install.inf` file unless you absolutely have to (as may be necessary for multi-homed systems).

- Verify the installation path on the `ServerRoot` directive. If you are installing on both Windows NT and UNIX machines, make sure the appropriate path delimiter is used. Add or remove the Windows NT drive letter designation as is appropriate for the host you are installing on.

- If you create your `install.inf` file on a Windows NT machine, then the `SuiteSpotUserID` and `SuiteSpotGroup` directives are both set to `nobody`. If you subsequently use this file on a UNIX machine, ensure the user and group specified by these directives are appropriate for the machine. The `SuiteSpotUserID` and `SuiteSpotGroup` directives determine what user and group a server will run under when installed on a UNIX system.

Be sure to protect `install.inf` files since they contain passwords in the clear.

For complete information on the directives you can use in a silent installation file, see “Installation Directives,” on page 51.

A Typical Installation

The following table shows the `install.inf` file that is generated for a typical installation:

```
[General]
FullMachineName=   idarhost.yourdomain.com
ConfigDirectoryLdapURL=ldap://directoryhost.yourdomain.com:389/
SuiteSpotUserID=   nobody
SuitespotGroup=   nobody
ConfigDirectoryAdminID=   admin
ConfigDirectoryAdminPwd=   admin
ServerRoot=   /usr/iplanet/servers
AdminDomain=   yourdomain.com
Components=svrcore,base,admin,idar,idarConsole,idarConsoleInstaller,idarTCL

[admin]
SysUser=   nobody
Port=   5000
ServerIpAddress=
ServerAdminID=   admin
ServerAdminPwd=   admin
Components=   admin,admin-client

[idarConsoleInstaller]
idarListenPort=   10389
Components=   idarConsoleInstaller

[base]
Components=   base,base-client,base-jre

[idar]
Components=   idar

[idarConsole]
Components=   idarConsole

[idarTCL]
Components=   idarTCL
```

Installing the Stand-Alone iPlanet Console

The following is the `install.inf` file that is generated when you install just iPlanet Console:

```
[General]
ServerRoot=   /usr/iplanet/servers
Components=
```

Installation Directives

This section describes the basic format of the file used for silent installation. It then describes the directives that are available for each area of the silent installation file. Specifically, the following sections are provided here:

- Silent Installation File Format
- [General] Installation Directives
- [Base] Installation Directives
- [idarConsoleInstaller] Installation Directives
- [admin] Installation Directives

Silent Installation File Format

When you use silent installation, you provide all the installation information in a file. This file is formatted as follows:

```
[General]
directive=value
directive=value
directive=value
...
[Base]
directive=value
directive=value
directive=value
...
[idar]
directive=value
directive=value
directive=value
...
[admin]
directive=value
directive=value
directive=value
...
[idarTCL]
directive=value
directive=value
directive=value
...
[idarConsole]
directive=value
directive=value
directive=value
...
[idarConsoleInstaller]
directive=value
directive=value
directive=value
...
```

The keywords `[General]`, `[idar]`, `[idarConsole]`, `[idarConsoleInstaller]`, `[idarTCL]`, and `[admin]` are required. They indicate that the directives that follow are meant for a specific aspect of the installation. They must be provided in the file in the order indicated above.

[General] Installation Directives

[General] installation directives specify information of global interest to the iPlanet servers installed at your site. That is, the information you provide here will be common to all your iPlanet servers.

The [General] installation directives are:

Table 4-1 [General] Installation Directives

Directive	Description
`Components`	Specifies components to be installed. The list of available components will differ depending on the iPlanet servers available on your installation media. For stand-alone directory installation, the list of components is: • `srvrcore`—uninstallation binaries • `base`—the base installation package • `admin`—the Administration Server binaries • `idar`—the iDAR binaries • `idarTCL`—the TCL binaries • `idarConsole`—components used by the console to make it iDAR aware • `idarConsoleInstaller`—installation routines to "glue" iDAR's Console to the host platform This directive is required. At a minimum, you should always provide: `components = srvrcore, base, admin`
`ServerRoot`	Specifies the full path to the directory where the iPlanet server binaries are installed. This directive is required.
`FullMachineName`	Specifies the fully qualified domain name of the machine on which you are installing the server. The default is the local host name.
`SuiteSpotUserID`	UNIX only. Specifies the username that iPlanet servers will run as. This parameter does not apply to the user that the Administration Server runs as. See the SysUser directive in Table 4-4 for more information. The default is user `nobody` but this should be changed for most deployments.

Table 4-1 [General] Installation Directives *(Continued)*

Directive	Description
`SuiteSpotGroup`	UNIX only. Specifies the group that iPlanet servers will run as. The default is group `nobody` but this should be changed for most deployments.
`ConfigDirectoryLdapURL`	Specifies the LDAP URL that is used to connect to your configuration directory. LDAP URLs are described in the *iPlanet Directory Server Administrator's Guide*. This directive is required.
`AdminDomain`	Specifies the administration domain under which this server will be registered. See "Deciding the User and Group for Your iDAR (UNIX Only)," on page 14 for more information about administration domains.
`ConfigDirectoryAdminID`	Specifies the user ID of the entry that has administration privileges to the configuration directory. This directive is required.
`ConfigDirectoryAdminPwd`	Specifies the password for the ConfigDirectoryAdminID. This directive is required.
`UserDirectoryLdapURL`	Specifies the LDAP URL that is used to connect to the directory where your user and group data is stored. If this directive is not supplied, the configuration directory is used for this purpose. LDAP URLs are described in the *iPlanet Directory Server Administrator's Guide*.
`UserDirectoryAdminID`	Specifies the user ID of the entry that has administration privileges to the user directory.
`UserDirectoryAdminPwd`	Specifies the password for the UserDirectoryAdminID.

[Base] Installation Directives

There is only one [Base] installation directive and it allows you to determine whether iPlanet Console is installed:

Table 4-2 [Base] Installation Directive

Directive	Description
`Components`	Specifies the base components to be installed. The base components are: • `base`—install the shared libraries used by all Server Consoles. You must install this package if you are also installing some other iPlanet server. • `base-client`—install the Java run time environment used by the Server Consoles. • `base-jre`—causes the Java run time environment to be installed. This directive is required if you are installing an iPlanet server (versus, for example, just iPlanet Console). You must install both packages when you are installing an iPlanet server.

[idarConsoleInstaller] Installation Directives

[idarConsoleInstaller] installation directives specify information of interest only to the iDAR instance that you are currently installing. These directives are described in the following section.

Required [idarConsoleInstaller] Installation Directives

You must provide the following directives when you use silent installation with iDAR:

Table 4-3 Required [idarConsoleInstaller] Installation Directives

Directive	Description
`Components`	Specifies the idarConsoleInstaller components to be installed. The idarConsoleInstaller components are: • `idarConsoleInstaller`—setup utilities. This directive is required. It is recommended that you always install these components any time you install iDAR.

Table 4-3 Required [idarConsoleInstaller] Installation Directives *(Continued)*

Directive	Description
`idarListenPort`	Specifies the port on which iDAR will listen for connections.

[admin] Installation Directives

[admin] installation directives specify information of interest only to your iDAR's Administration Server. That is, this is the installation information required for the Administration Server that is used to manage the iDAR instance that you are currently installing.

The [admin] installation directives are:

Table 4-4 [admin] Installation Directives

Directive	Description
`Components`	Specifies the admin components to be installed. The base components are: • `admin`—install the Administration Server. You must install the Administration Server if you are also installing some other iPlanet server. • `admin-client`—install iPlanet Console. Specify just this component if you are installing iPlanet Console as stand-alone. Do not install this component if you will remotely manage your servers and iPlanet Console will be installed somewhere else on your network.
`SysUser`	UNIX only. Specifies the user that the Administration Server will run as. For default installations that use the default iPlanet port numbers, this user must be root. Root is the default. For information on what users your servers should run as, see "Deciding the User and Group for Your iDAR (UNIX Only)," on page 14
`Port`	Specifies the port that the Administration Server will use. Note that the Administration Server's host name is given by the `FullMachineName` directive. For more information on `FullMachineName`, see Table 4-1 on page 53.

Table 4-4 [admin] Installation Directives *(Continued)*

Directive	Description
`ServerAdminID`	Specifies the administration ID that can be used to access this Administration Server if the configuration directory is not responding. The default is to use the value specified by the `ConfigDirectoryAdminID` directive. See "Defining Authentication Entities," on page 15 for information on this directive.
`ServerAdminPwd`	Specifies the password for ServerAdminID.
`ServerIPAddress`	Specifies the IP address that the Administration Server will listen to. Use this directive if you are installing on a multi-homed system and you do not want to use the first IP address for your Administration Server.

Chapter 5

Post Installation

This chapter describes the post-installation procedures for launching the iPlanet Directory Access Router (iDAR) online help and populating the directory tree.

Launching the Help System

The help system for iDAR is dependent upon iPlanet Administration Server. If you are running iPlanet Directory Access Router Console on a machine remote to Administration Server, you will need to confirm the following:

Client IP address authorized on Administration Server. The machine running iDAR Console needs access to Administration Server. To configure Administration Server to accept the client machine's IP address, do the following in Administration Server:

1. Launch iPlanet Administration Server Console. The console should be running on the same machine as Administration Server.
2. Click the Configuration tab, then click the Network tab.
3. In the Connection Restrictions Settings, select "IP Addresses to Allow" from the pull down menu. Click Edit.
4. Edit the IP Addresses field to the following: *.*.*.*

NOTE This allows all clients access to Administration Server.

5. Restart Administration Server. You can now launch the online help by clicking any of the Help buttons in iDAR's Console.

Proxy authorized on Administration Server. If you use proxies for your HTTP connections on the client machine running iDAR Console, you need to do one of the following:

- Remove proxies on the machine running Directory Server Console. This allows the client machine to access Administration Server directly.

  To remove the proxies on the machine running Directory Server Console, you need to alter the proxy configuration of the browser you will use to run the help. In Netscape Communicator, select Preferences from the Edit menu. Select Advanced then Proxies to access the proxy configuration. In Internet Explorer, select Internet Options from the Tools menu.

- Add the client machine proxy IP address to Administration Server list of acceptable IP addresses.

CAUTION Adding the client machine proxy IP address to Administration Server creates a potential security hole in your system.

Index