Installation Guide

iPlanet Directory Access Router

Release 2.1

806-5633-01
June 2000

Contents

Chapter 1 Installation Instructions for Windows NT 7
Configuring a Machine to Run iDAR 7
Required System Modules 7
Installing Windows NT Server 8
Installing Third-party Utilities 8
Installing Microsoft Utilities 9
Ensure that the System Clock is Correct and Kept Accurate 9
Installing the Package 9
Install Service Packs and Hotfixes 10
Install Windows NT 4.0 Service Pack 6a or Later 10
Install Hotfixes 10
Install TCP ISN Patch 10
Post-installation System Configuration 11
Restrict Network Services 11
Remove NETBIOS 12
Enable Port Filtering 12
Disable IP Routing 13
Disable WINS Client 13
Remove the OS/2 and POSIX Subsystem Keys from the Registry 13
Remove the OS/2 DLLs 14
Stop Unneeded Services 14
Ensure System Will Automatically Reboot on Error 15
Configure User Accounts 15
Encrypt Account Database 16
Event Log Configuration 17
Set Tuning Parameters 17
Configuration 18

Removing the Software 19

Chapter 2 Installation Instructions for Solaris 21
Disk Space Requirements 21
Required System Modules 21
Unpacking the Downloaded File 22
Installing the Package 22
Startup Script 23
Verify System Tuning 24
File Descriptors 24
TCP Tuning 24
Removing the Software 25

Chapter 3 Installation Instructions for Compaq Tru64 UNIX 27
Disk Space Requirements 27
Required System Modules 27
Unpacking the Downloaded File 27
Installing the Package 28
Startup Script 28
Verify System Tuning 29
Virtual Memory Management Changes 29
Threads Changes 30
TCP/IP Generic Changes 30
TCP/IP Multiprocessor Changes 31
Per-user Limits 31
Removing the Software 32

Chapter 4 Installation Instructions for AIX 33
Disk Space Requirements 33
Required System Modules 33
Unpacking the Downloaded File 33
Installing the Package 34
Starting the Server 34
Removing the Software 34

Chapter 5 Installation Instructions for Linux 37
Disk Space Requirements 37
Required System Modules 37
Unpacking the Downloaded File 37
Installing the Package 38
Startup Script 38

Removing the Software 39

Chapter 6 Installation Instructions for HP-UX 11 41
Disk Space Requirements 41
Required System Modules 41
Installing the Package 41
Removing the Software 43

Chapter 1

Installation Instructions for Windows NT

This section describes how to install a copy of the iPlanet Directory Access Router on Windows NT.

Configuring a Machine to Run iDAR

The iPlanet Directory Access Router should be installed on a computer which is isolated from the public 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 run other operating systems. At a minimum, the computer system should have at least 128MB of RAM, 100MB of disk, a Pentium II or later processor, and a 100MBps Ethernet connection.

In addition, this computer must not have installed the Scriptics TCL/Tk environment as it could interfere with operation of iDAR's configuration tools.

Required System Modules

This software can only be installed on a Windows NT 4.0 Server for the Intel platform. It cannot be installed on Windows 95, versions of Windows NT prior to 4.0, or Windows NT for the Alpha, PowerPC or MIPS architectures.

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 will need an UNZIP utility to unpack the proxy server software. There are many commercially licensed, free and shareware tools available, such as PKZIP or Winzip. Please 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 will 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`.

To manage the proxy configuration file, you will need a text editor that is capable of handling large text files (Notepad and Wordpad are not suitable). If you are already familiar with Emacs on UNIX, a port to Windows can be downloaded from `ftp://ftp.cs.washington.edu/pub/ntemacs/`. There are many other shareware and commercial text editors available.

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 iPlanet Directory Access Router.

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

At this point you will need to install Service Pack 4 or later, if not already installed. This is needed for the installation of Microsoft Internet Explorer 5. Service packs can be obtained from `http://www.microsoft.com/windows/servicepacks/`.

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.

Installing the Package

Log in to Windows NT as the administrator user, or as a user with administrator privileges, if you have not done so already.

Install the software by running the `setup.exe` program that was extracted from the `idar21.zip` or `idar21exp.zip` file. This is a standard InstallShield installation script.

The only option is the directory in which to install the software. The default pathname is `[Program Files]\iPlanet\Directory Access Router`. This directory should be on a local drive, and should not already exist.

After the program files are installed, the script will prompt that iDAR is to be installed as a service.

Install Service Packs and Hotfixes

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

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.

Install TCP ISN Patch

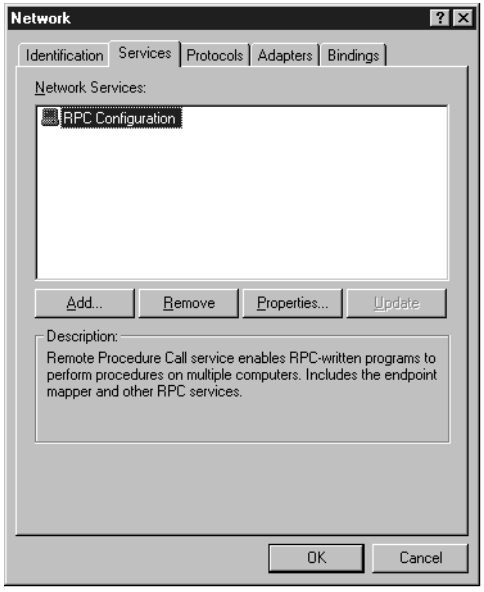
If you will be authenticating users through the proxy, then TCP connection hijacking is a vulnerability. Microsoft has released a patch to improve the serial numbers, `q243835i.exe`. For more information please see `http://www.microsoft.com/security/bulletins/ms99-046.asp`

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

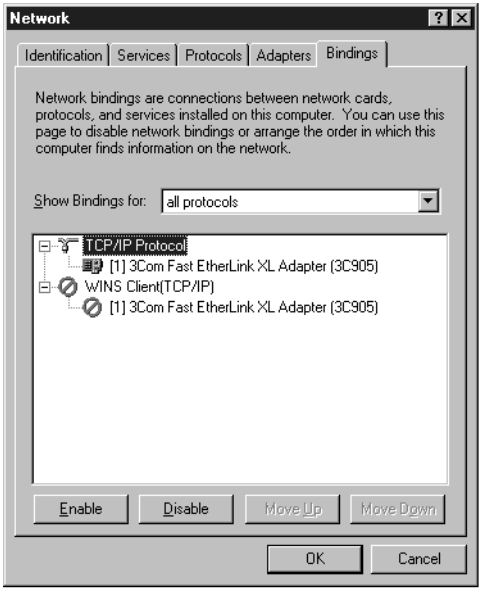
Network file sharing is not required by iDAR and should be disabled. Go to the Control Panel and double click the Network icon. Remove the "`Workstation`", "`Computer Browser`", "`NetBIOS Interface`", "`Remote Access Service`" and "`Server`" services from Network "`Services`" tab. Leave "`RPC Configuration`".



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

Remove NETBIOS

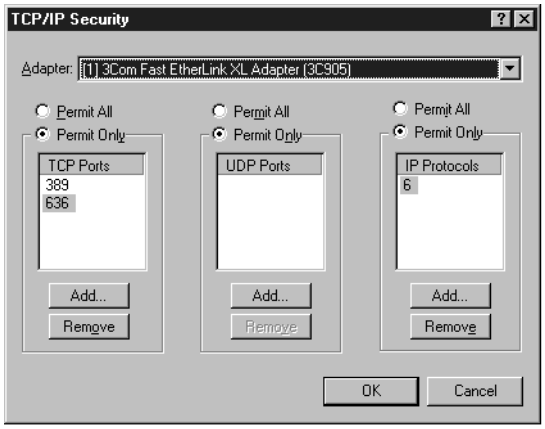
The iDAR only uses TCP/IP and does not require any Microsoft network services. On the "`Bindings`" tab, select "`All protocols`". Disable the WINS Client. This unbinds NETBIOS from TCP/IP.



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.

Select the TCP/IP protocol window. On the "TCP/IP" protocol window, select "Advanced" and enable security. On the TCP/IP filtering window, permit only TCP ports 389 and 636, 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



Please 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

iDAR does not require these 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`

Please note that 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 the "`Os2LibPath`" item 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 values for "`Posix`" and "`OS/2`" from this key:

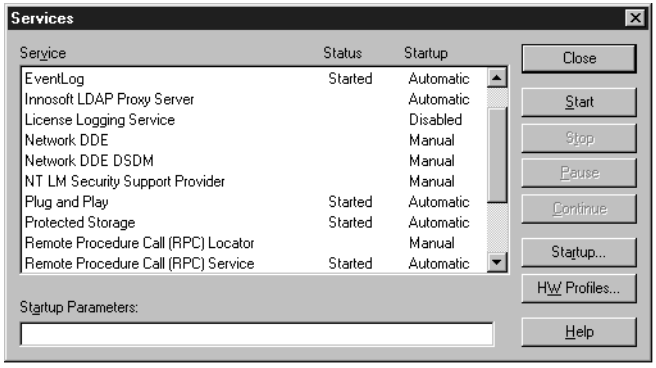
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\SubSystems`

Remove the OS/2 DLLs

All files in the `%SystemRoot%\system32\os2` directory and all subdirectories should be deleted.

Stop Unneeded Services

In the Control Panel "`Services`" page, stop and disable any running services except for "`EventLog`", "`Innosoft LDAP Proxy Server`", "`NT LM Security Support Provider`", "`Plug and Play`", "`Protected Storage`" and "`Remote Procedure Call (RPC) Service`". Services which are listed as "`Manual`" start do not need to be disabled.

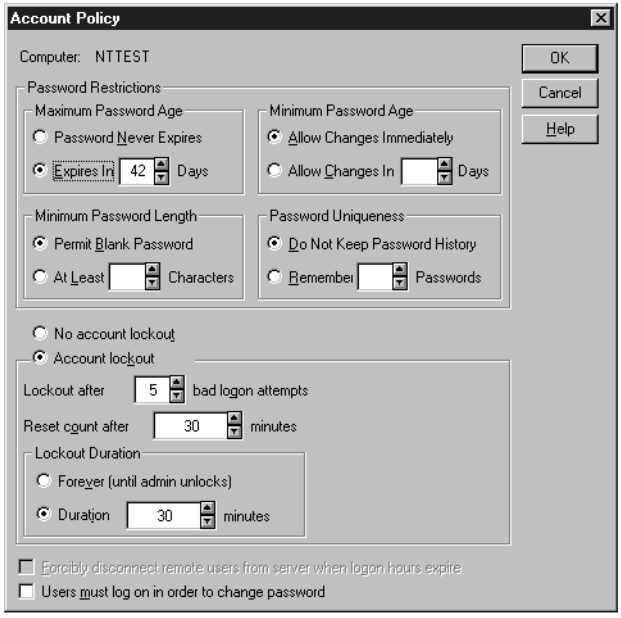


Ensure System Will Automatically Reboot on Error

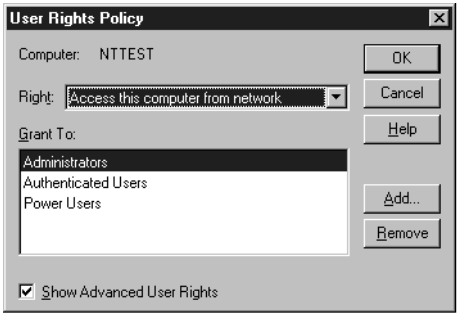
In the Control Panel "`System`" element, Under the "`Startup/Shutdown`" tab, set the show list time to `0` seconds, and ensure that automatic reboot is enabled.

Configure User Accounts

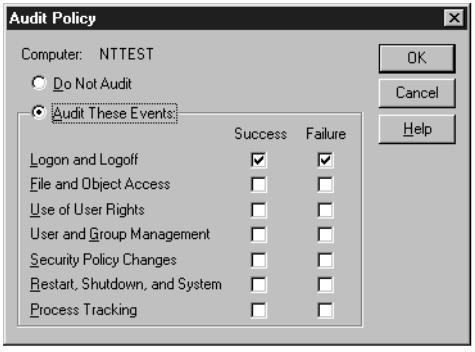
Launch User Manager for Domains. On the Account Policies window, allow accounts to be locked out.



On the User Rights Policy list item “`Access this computer from the network`,” remove “`Everyone`” and add “`Authenticated Users`”.



On the Audit Policy window, enable auditing for Success and Failed Logon and Logoff events.



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

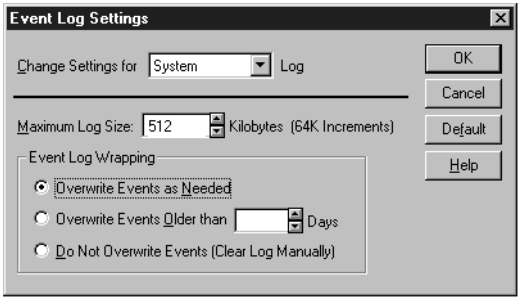
If you have copied the ‘`passprop`’ utility from the NT Server Resource Kit, it can be used to allow lockout of the administrator’s account by running it on the command line as `passprop /adminlockout`

Encrypt Account Database

Protect the SAM database by running the program “`syskey`”. This encrypts the Administrator’s password so that registry-extracting hacker tools cannot use it.

Event Log Configuration

Launch the Event Viewer and set the log overwrite intervals.



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, latency overhead is reduced 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
```

Set the value of `MaxFreeTcbs` to 0xFA0.

This example increases the TCB timewait table to 4,000 entries from the default of 2,000. Now that overhead time introduced by TCP is lowered for iDAR, you must adjust the corresponding hash table which is where the TCBs are stored. This is done by adding by adding the following registry value:

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

Set 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 iDAR is experiencing memory bottlenecks and more memory cannot be allotted to the server, lower the above values.

On a multiprocessor system, you may want to try 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 find the request urgent enough (a high enough interrupt level), it will defer 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 increase.

When an interrupt is sent to a particular CPU and it gets 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 from happening, set the following registry value:

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

Set 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.

Configuration

You will need to construct iDAR's `tailor.txt` and `tailor.ldif` files. This process is described in the iPlanet Directory Access Router Administrator's Guide.

Removing the Software

Should it be necessary to delete iDAR software from the machine, there are two steps that must be followed:

The first step is to stop the service, if it is currently running, using the "`Services`" icon on the Control Panel. If the service is running, the software will not be deinstalled properly. Select the item "`iPlanet Directory Access Router`," and if the status is "`Started`," click the "`Stop`" button.

Second, the "`Uninstall`" item on the "`iPlanet Directory Access Router`" Program menu should be run. This will cause the service and all program files to be deleted from the disk.

Chapter 2

Installation Instructions for Solaris

This section describes how to install a copy of the iPlanet Directory Access Router for Solaris.

Disk Space Requirements

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

current working directory: 60 MB
partition containing `/var`: 30 MB
partition containing `/opt`: 30 MB

Required System Modules

iDAR is optimized for systems with the UltraSPARC, Pentium Pro, Pentium II, or Pentium III chipsets.

Use of Solaris 2.6 or 7 with the Sun recommended patches is required.

The following Sun patches 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.

- Solaris 2.6 SPARC: 105181-19, 105210-27 and 105568-16 are required. In addition, 105401-25, 107733-5, 105633-34, 105669-10, 105786-11, 106125-9, 106040-12, 105755-7, 106439-5 and 106495-1 are recommended.

- Solaris 2.6 x86: 105182-16 and 105491-5 are required. In addition, 106126-6, 105211-18, 105787-6 are recommended.

- Solaris 7 SPARC: 106980-5 and 106541-9 are required. In addition, 107078-8, 107544-3, 107171-5, 106793-3 are recommended.

- Solaris 7 x86: 106981-5 and 106542-7 are required.

Unpacking the Downloaded File

Uncompress and untar the file. These file names may contain `.export` if outside the US and Canada.

```
zcat iDAR-2.1.sspc.tar.Z | tar xpf - (if Solaris SPARC)
zcat iDAR-2.1.sx86.tar.Z | tar xpf - (if Solaris x86)
```

You should have the following files in this directory:

```
iDAR.pkg
iDAR-2.1.sspc.tar.Z (if Solaris SPARC)
iDAR-2.1.sx86.tar.Z (if Solaris x86)
```

At this point you should move the compressed tar file, "`iDAR-2.1.*.tar.Z`", to your backup media, in case you ever need to restore the operating system and packages on it.

Installing the Package

Log in as the super-user, if you have not done so already.

Install the software on this system by running the `pkgadd` command:

```
pkgadd -d iDAR.pkg
```

This program will prompt you with the following list of packages, of which there will be only one. The platform name in parenthesis will be "`i86pc`" for Solaris Intel, "`sun4u`" for SPARC.

The following packages are available:

```
1 iDAR iPlanet Directory Access Router(i86pc) 2.1
```

```
Select package(s) you wish to process (or 'all' to process all
packages). (default: all) [?,??,q]:
```

Enter `1`. iDAR is by default installed under the directory `/opt`, as `/opt/iDAR`. However any directory can be the base directory, and `pkgadd` will automatically create a symbolic link for `/opt/iDAR`.

Answer `y` to the next question of whether scripts may be executed as the super-user. This will allow `pkgadd` to ensure that the system has the correct patches installed.

The final output message should be:

```
Installation of <iDAR> was successful.
```

If `pkgadd` reports any problems, check to make sure that the `/opt` or other installation directory is writable and contains sufficient disk space. If the package installation was only partially successful, the damaged installation may be removed with the command `pkgrm iDAR`.

Otherwise, when the installation is successful, you may delete the file `iDAR.pkg` from your working directory.

Startup Script

The `pkgadd` command will install a startup script which will cause iDAR to be run the next time the system is rebooted. At this point you may wish to edit this file `/etc/init.d/S93iDAR` to set options. iDAR can be started manually, if it is not already running, with the command:

```
sh /etc/init.d/S93iDAR start
```

If you do not wish to have the iDAR start automatically when the machine boots, then the `/etc/rc2.d/S93iDAR` file may be deleted.

Note that renaming this file to be called something else in this directory will not prevent it from being used, for when UNIX starts it will attempt to run all the appropriate files in this directory. For this same reason be sure when editing this file that any temporary or backup files (such as `S93iDAR~`) are deleted, otherwise they will confuse the operating system.

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) and Solaris Performance Administration* (ISBN 0-07-011768-3). Advanced tuning information is available from the Web site: `http://www.rvs.uni-hannover.de/people/voeckler/tune/EN/tune.html`.

The program `/opt/iDAR/sbin/idsktune` analyzes the Solaris kernel tuning parameters and reports any changes that should be made to improve performance. This program does not itself 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 7 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. Please see the iDAR Administrator's Guide for more details.

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.

Removing the Software

The software may be deleted from the system by running the command (as root)

```
pkgrm iDAR
```

Note: If you have placed a file (or anything else) in the installation directory following a pkgadd -d iDAR.pkg installation process, the pkgrm iDAR command will NOT complete successfully the first time it is run. This is because the pkgrm process does not know anything about any files other than those installed by the pkgadd process. Since it doesn't recognize any such files, it will not remove them and therefore be unable to remove the install directory.

If you see this failure, DO NOT try and install over the top of it with a `pkgadd` command because the `pkgadd` will fail. Instead, issue the `pkgrm iDAR` command again and you should see a successful completion. You can then go ahead and issue the `pkgadd` command to install a new version of iDAR.

Chapter 3

Installation Instructions for Compaq Tru64 UNIX

This section describes how to install a copy of the iPlanet Directory Access Router for Compaq Tru64 UNIX.

Disk Space Requirements

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

current working directory: 60 MB
partition containing `/opt`: 30 MB

Required System Modules

Use of Compaq Tru64 UNIX 4.0D or later is required, and the 4.0F release is recommended.

More information on Tru64 UNIX patches is available at `http://www.digital.com/java/download/jdk_du/dupatches.html`.

Unpacking the Downloaded File

Uncompress and untar the file. The file name may contain `.export` if outside the US and Canada.

```
zcat iDAR-2.1.osf.tar.Z | tar xpf -
```

You should have the following files in this directory:

```
IDAR210/
```

```
iDAR-2.1.osf.tar.Z
```

At this point you should move the compressed tar file, “iDAR-2.1.osf.tar.Z”, to your backup media, in case you ever need to restore the operating system and packages on it.

Installing the Package

Log in as the super-user, if you have not done so already.

Install the software on this system by running the `setld` command:

```
setld -l IDAR210
```

This program will prompt you with the following list of subsets, of which there will be only one. Enter “1”, then “y”. It will then continue, and the final output message should be:

```
Configuring ”iPlanet Directory Access Router” (IDAR210)
```

If setld reports any problems, check to make sure that the `/opt` directory is writable and contains sufficient disk space. If the package installation was only partially successful, the damaged installation may be removed with the command “`setld -d IDAR210`”.

Otherwise, when the installation is successful, you may delete the directory “`IDAR210`” from your working directory.

Startup Script

The `setld` command will install a startup script which will cause iDAR to be run the next time the system is rebooted. At this point you may wish to edit this file `/sbin/rc3.d/S93iDAR` to set options, as described in the following sections. iDAR can be started manually, if it is not already running, with the command

```
sh /sbin/rc3.d/S93iDAR start
```

If you do not wish to have iDAR start automatically when the machine boots, then the `/sbin/rc3.d/S93iDAR` file may be deleted.

Note that renaming this file to be called something else in this directory will not prevent it from being used, for when UNIX starts it will attempt to run all the appropriate files in this directory. For this same reason be sure when editing this file that any temporary or backup files (such as `S93iDAR~`) are deleted, otherwise they will confuse the operating system.

Verify System Tuning

The program `/opt/iDAR/sbin/idsktune` analyses the Tru64 kernel tuning parameters and reports any changes that should be made to improve system performance. This program does not itself modify the system.

Several kernel tuning parameters will probably need to be set, and these can be changed using `dxkerneltuner`. After making these changes the system will need to be rebooted. Note that these tuning parameters may not be available on versions of Tru64 UNIX prior to 4.0F.

subsystem	parameter	max value
vm	vm-mapentries	400
vm	maxvas	2147483648
vm	vm-vpagemax	262144
proc	max-threads-per-user	8392
tcp	tcp_msl	5
tcp	tcpnodelack	1
inet	sominconn	32767
inet	somaxconn	32767
inet	ipqs	16
inet	tcbhashnum	16

Virtual Memory Management Changes

The `vm` subsystem controls how Tru64 UNIX manages virtual memory allocation requires on behalf of processes.

The vm-mapentries parameter controls the number of memory-mapped files which can be simultaneously opened in a user process. On Solaris, memory-mapped files (mapped from /dev/zero) are used to allocate thread stacks, however this is not be the case on Tru64 UNIX. The default value on Tru64 UNIX is 200, on a production system it should be raised to 400.

The vm-maxvas setting specifies the amount of virtual memory available to each process. On Windows NT and most other UNIX systems this is typically limited to 2GB, however as Tru64 UNIX uses a 64 bit pointer space, vm-maxvas can be raised from a default of 1GB to the sum of physical and swap memory. Should you have 2 or more gigabytes of physical memory, this parameter should be raised to 2147483648.

The vm-vpagemax parameter specifies the number of pages which can be given memory protection attributes. As Tru64 UNIX assigns memory protection to thread stacks, and pages are 8KB in size, this parameter typically needs to be increased. For an operational service, vm-vpagemax should be raised from 16384 to 262144.

Threads Changes

The proc subsystem contains limits on the scheduling resources in Tru64 UNIX.

The max-threads-per-user specifies the maximum number of threads that all the processes running under a single userid may have blocked or runnable at any given time. The superuser is not subject to this limit. If iDAR is not to be run by user root or the ids-proxy-sch-GlobalConfiguration objectclass attribute ids-proxy-con-userid is set, this parameter should be increased to the maximum number of simultaneous connections, plus 100.

TCP/IP Generic Changes

This section lists generic TCP / IP tuning parameters in the tcp and inet subsystems.

The tcp_msl parameter specifies the maximum segment lifetime: the number of seconds that a TCP packet may be lost in the network and show up later than expected. The default for this parameter is 60, which is appropriate for wide area networks such as the Internet. When iDAR is to be accessed on by clients on a local LAN or MAN under a single administration, this parameter may be reduced. A setting too large can result in a large number of connections on the server appearing in the TIME_WAIT state. In a test configuration where all the testing is

being done on a single isolated 100MB full duplex LAN, this parameter can be reduced to 5 seconds. The `tcpnodelack` parameter specifies whether the kernel should disable the Nagle delayed ack algorithm for all clients. In operational environments, this parameter may be set to 1.

The `inet` subsystem parameters `sominconn` and `somaxconn` specify the bounds on the listen backlog: connections which the kernel may accept on behalf of a process. These parameters should be increased to their recommended maximum, 32767.

TCP/IP Multiprocessor Changes

This section lists TCP/IP tuning parameters which should be changed only if the server is a multiprocessor configuration. These changes should not be applied for single processor configurations as they may cause a decrease in performance and system stability.

The `inet` subsystem tuning parameters `ipqs` and `tcbhashnum` can both be raised from 1 to 16. This is intended to decrease contention to kernel tables which must be accessed for each incoming packet.

Per-user Limits

By default a shell on Tru64 UNIX does not permit a process to access all the available address space that has been configured in the kernel. The soft limits provide a tighter set of restrictions that must be manually removed.

iDAR itself removes the file descriptor soft limit when it starts, but other limits must first be removed by hand before running any of the executables.

The commands to remove the soft limits are not standardized across the shells; please consult the on-line manual page for the specific shell being used. The `csh` shell requires the following commands be typed:

```
limit datasize unlimited
limit stacksize unlimited
limit memoryuse unlimited
limit addressspace unlimited
limit descriptors unlimited
```

Removing the Software

The software may be deleted from the system by running the command (as `root`)

```
setld -d IDAR210
```

Chapter 4

Installation Instructions for AIX

This section describes how to install a copy of the iPlanet Directory Access Router for AIX.

Disk Space Requirements

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

current working directory: 60 MB
partition containing `/usr`: 30 MB

Required System Modules

Use of AIX 4.3 or later is required.

Unpacking the Downloaded File

Uncompress and untar the file. This file name may contain a `.export` if outside the US and Canada.

```
zcat iDAR-2.1.aix.tar.Z | tar xpf -
```

You should have the following files in this directory:

```
idar.bff
```

```
iDAR-2.1.aix.tar.Z
```

At this point you should move the compressed tar file, "`iDAR-2.1.*.tar.Z`", to your backup media, in case you ever need to restore the operating system and packages on it.

Installing the Package

Log in as the super-user, if you have not done so already.

Install the software on this system by running the `smit install.latest` command:

```
smit install.latest
```

This program will prompt you for installation of the package. Specify `iDAR.server` as the fileset to install.

If smit reports any problems, check to make sure that the `/opt` directory is writable and contains sufficient disk space. Otherwise, when the installation is successful, you may delete the file "`idar.bff`" from your working directory.

After installing, it will be necessary to reboot the server. On AIX, this can be done with `shutdown -Fr`.

Starting the Server

During the installation, iDAR will be registered as a subsystem in the object repository. Following a reboot (to restart the `srcmstr`), it can be started by `startsrc` or by using `smit`.

It can be started in normal operation mode with the following command:

```
startsrc -s idar
```

and stopped using the command:

```
stopsrc -s idar
```

Removing the Software

Deleting the software is a five step process that must be performed by the root user.

1. Ensure that iDAR is not currently running.
2. Delete the iDAR record from the object repository using `odmdelete -o SRCsubsys -q subsysname=idar`
3. Delete the service using the `smit` command. Choose “Remove Installed Software” under “Software Maintenance and Utilities” and specify `idar` as the SOFTWARE name.
4. Remove the symbolic link `/opt/iDAR` using `rm /opt/iDAR`
5. Reboot the machine using `shutdown -Fr` to restart SRC.

Chapter 5

Installation Instructions for Linux

This section describes how to install a copy of the iPlanet Directory Access Router for Red Hat Linux 6.0 or 6.1 for Intel.

Disk Space Requirements

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

current working directory: 60 MB
partition containing `/opt`: 30 MB

Required System Modules

Red Hat Linux 6.0 or 6.1 for Intel is required. Earlier versions of Red Hat Linux and other distributions are not supported.

Unpacking the Downloaded File

Uncompress and untar the file. This file name may contain a `.export` if outside the US and Canada.

```
gunzip -c iDAR-2.1.rhli.tar.gz | tar xf-
```

You should have the following files in this directory:

```
iDAR-2.1-l.i386.rpm
RELEASE.txt
iDAR-2.1.rhli.tar.gz
```

At this point you should move the compressed tar file, "`iDAR-2.1.*.tar.gz`", to your backup media, in case you ever need to restore the operating system and packages on it.

Installing the Package

Log in as the super-user, if you have not done so already.

Install the software on this system by running the `rpm` command.

```
rpm -i idar*.rpm
```

If rpm reports any problems, check to make sure that the `/opt` directory is writable and contains sufficient disk space. Otherwise, when the installation is successful, you may delete the rpm file from your working directory.

Startup Script

The `rpm` command will install a startup script which will cause iDAR to be run the next time the system is rebooted. At this point you may wish to edit this file `/etc/rc.d/rc3.d/S93iDAR` to set options, as described in the following sections. The iDAR can be started manually, if it is not already running, with the command

```
sh /etc/rc.d/jbvrc3.d/S93iDAR start
```

If you do not wish to have iDAR start automatically when the machine boots, then the `/etc/rc.d/rc3.d/S93iDAR` file may be deleted.

Note that renaming this file to be called something else in this directory will not prevent it from being used, for when Linux starts it will attempt to run all the appropriate files in this directory. For this same reason be sure when editing this file that any temporary or backup files (such as `S93iDAR~`) are deleted, otherwise they will confuse the operating system.

Removing the Software

The software may be deleted from the system by running the command (as `root`)

```
rpm -e iDAR
```

Chapter 6

Installation Instructions for HP-UX 11

This section describes how to install a copy of the iPlanet Directory Access Router on HP-UX 11.

Disk Space Requirements

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

download drive: 60 MB
installation drive: 30 MB

Required System Modules

HP-UX 11 is required.

Installing the Package

Log in as the super-user, if you have not done so already.

Uncompress and untar the file. If you are outside of the United States, the tar filename may contain an "`.export`" infix.

```
zcat iDAR-2.1.hpux.tar.Z | tar xpf -
```

In addition to `iDAR-2.1.hpux.tar.Z`, you should now have a directory named `iDAR-2.1.hpux` as well.

At this point you should move the compressed tar file `iDAR-2.1.hpux.tar.Z`, to your backup media, in case you ever need to restore the operating system and packages on it. Once archived, you may remove the compressed version via:

```
rm iDAR-2.1.hpux.tar.Z
```

Now register the package with HP-UX by executing the following command:

```
swreg -l depot iDAR-2.1.hpux
```

Note: the path to the `iDAR-2.1.hpux` file should be the complete and absolute path to the directory created in the previous step. The `swreg` command notifies the HP-UX package facility of the availability of the new package. Now execute the following:

```
swinstall
```

The `swinstall` HP-UX command will start an interactive user interface through which you can inspect, verify and direct the installation of the package.

From within the initial dialog box, via the `Source Depot Path` dialog, select the registered `depot` for the `iDAR-2.1.hpux` package.

Once you have signaled your selection, you should be presented with a list of packages ready to be installed. Select the line that possesses iDAR.

Then from the `Action` pull down menu, select `Install (analysis)`. At this point you should be presented with a dialog box that permits the inspection of the package via a set of buttons labeled: `Product Summary`, `Logfile`, `Disk Space`, and `Re-analyze`. These options provide insight into the package's contents and do not require any additional action in your part.

By pressing the `Ok` button, you will advance to an installation confirmation dialog. Press the `Yes` button to proceed. Once the `Install Window's Done` button is no longer dimmed out, then the product has been installed. You are again presented with the opportunity to inspect the `Product Summary` and/or the `Logfile`, but neither option is mandatory.

Selecting the `Done` button at this stage returns you to the `Software Selection` screen. From the `File` pull down menu, select the option to `Exit`.

The last step is to unregister the `depot`. This is accomplished with the same command used to register the `depot` with the exception of an additional parameter, namely `-u` for unregister, i.e.,

```
swreg -l depot -u iDAR-2.1.hpux
```

Once again the path to the `iDAR-2.1.hpux` file should be the complete and absolute path to the directory created in the previous step.

Removing the Software

Removal of the iDAR package is accomplished via the `swremove` program.

While logged in as super-user, execute:

```
swremove
```

Similar in presentation to `swinstall`, `swremove` displays a list of packages that are currently installed on the system. To remove the iDAR package, merely click on the line possessing iDAR and then from the `Actions` pull down list choose `Remove (analysis)`. The system will then present a dialog box through which you can examine the `Product Summary`, `Logfile`, `Re-analyze`. The removal process is initiated via the selection of the `Ok` button followed by answering, in the affirmative, the subsequent confirmation dialog box.